IBM Security Identity Governance and Intelligence
Version 5.2.2

Administration Topics

IBM

IBM Security Identity Governance and Intelligence
Version 5.2.2

Administration Topics

Table of contents

Chapter 24. Introduction to Enterprise Connectors 413

Chapter 25. Introduction to Access Optimizer 449

Chapter 26. Introduction to Access Risk Controls for SAP 539

Chapter 27. Introduction to Report Designer 577

Table list

Part 1. Administrators

An administrator can access the Administration Console and define administrator users for a single module or all the Identity Governance and Intelligence modules. Administrators are authorized to perform a selected set of tasks on specific modules.

For more information about the tasks that administrators can do, see Personas and use cases.

Chapter 1. Administration Console

Administration Console is an administration dashboard that provides control over the various management features of Identity Governance and Intelligence.

Logging in to the Administration Console

To log in to Administration Console, enter a valid user name and password in the Login window, and click **Login**.

General options

The console includes the following general options:

Act as
Grants user access to the system if the user is delegated as an administrator.

Logout
Exits the user from the console.

Change Password
Enables the user to change the current password.

Help
Displays the help information.

License
Displays information about Identity Governance and Intelligence licenses and upgrades.

Modules

The console includes a list of Identity Governance and Intelligence modules. Every module contains a set of common characteristics, which are outlined in Chapter 3, "Identity Governance and Intelligence modules," on page 55.

For more information about the different Administration Console modules, see the corresponding references.

Table 1. Administration Console modules

Image	Description
Chapter 21, "Introduction to Access Governance Core," on page 167	Chapter 25, "Introduction to Access Optimizer," on page 449

Table 1. Administration Console modules (continued)

Image	Description
Chapter 22, “Introduction to Access Risk Controls,” on page 333	SAP Chapter 26, “Introduction to Access Risk Controls for SAP,” on page 539
Chapter 23, “Introduction to Process Designer,” on page 367	Chapter 27, “Introduction to Report Designer,” on page 577
Chapter 24, “Introduction to Enterprise Connectors,” on page 413	Chapter 28, “Introduction to Task Planner,” on page 637
Chapter 18, “Target administration,” on page 143	

Realms

After you log in, select an operating realm. You do not need to log in again if you want to change realms.

Demo

A predefined realm with a large amount of coherent data that can be used for learning various about aspects of Identity Governance and Intelligence.

Sandbox

An empty realm with one basic data set that is used to start the operation.

Admin

The administration realm.

After you select a realm, click the module that you want. For every module, a specific tab opens by default.

Chapter 2. Data Model and Main Features: overview

All the features available in IBM® Security Identity Governance and Intelligence are based on different specialized integrated modules and on several architectural elements.

IBM Security Identity Governance and Intelligence uses these main architectural elements:

- A solid data model, for matching all the main characteristics of any organization.
- A flexible rules engine, for customizing the business policies for every organization.
- An integration interface, for integrating IBM Security Identity Governance and Intelligence platform with the pre-existing organization's architecture and the related repositories that contain users' information and authorizations.
- Several features of advanced customization for fitting the special needs of any organization.

You need a solid knowledge of these basic aspects before you start the administration activities of the platform:

- Core Data Model
- Extended Data Model
- Rules Engine
- Integration Interface
- Audit

IBM Security Identity Governance Core Data Model

AG Core provides a modeler capable of systematically outlining an organization's current situation as it relates to its different parts through a procedure that defines organizational and technical components.

This description of a realm is implemented by a database that literally photographs how the company is structured in terms of its

- Organization units
- Users
- Resources
- Applications
- Other elements of the IBM Security Identity Governance and Intelligence data model.

Based on this description, an authorization profile is built for each user within the organization. The authorization profile determines what a user can do within the realm and what resources are available.

An authorization profile intrinsically introduces rules about the visibility of objects that are described in the realm. Only those applications and resources that are outlined in the user's profile are made accessible to the user.

The main elements of the IBM Security Identity Governance and Intelligence data model are shown in the following Figure.

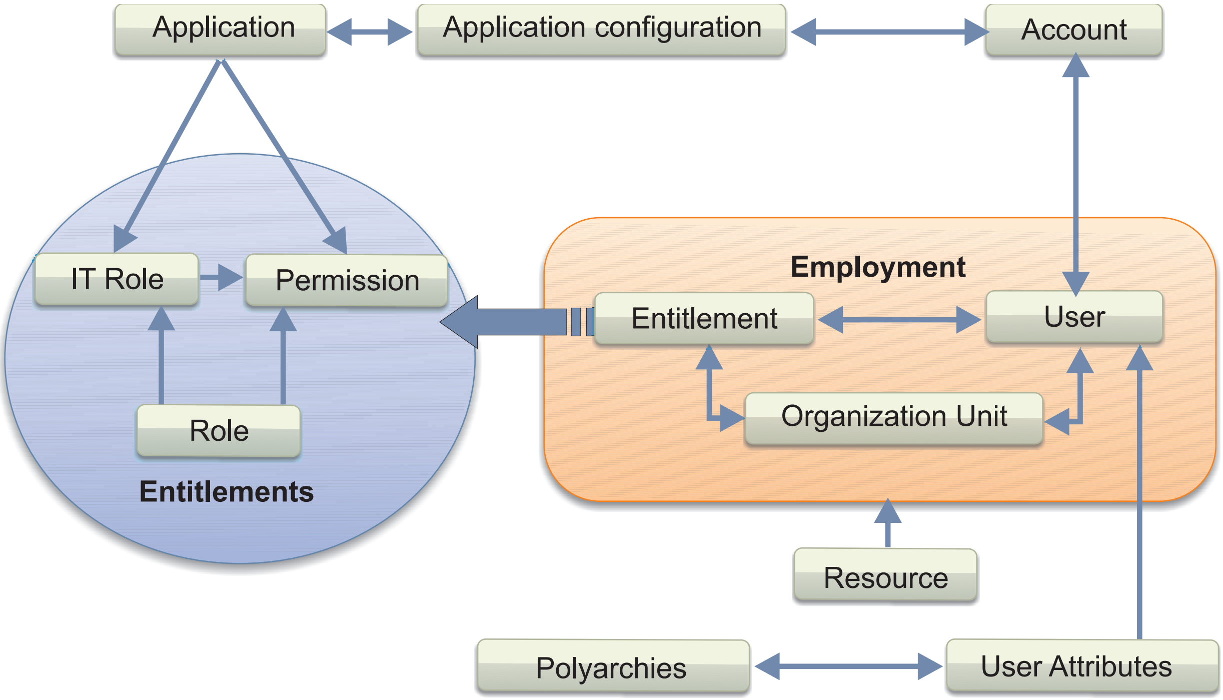


Figure 1. IBM Security Identity Governance and Intelligence data model

IBM Security Identity Governance and Intelligence data model has these main elements:

- Realm
- User
- "Organization unit" on page 8
- Entitlement
- Resource
- "Rights" on page 18
- "Applications" on page 21
- "Accounts" on page 23

Concept of realm

IBM Security Identity Governance and Intelligence Platform can manage multiple realms. It enables the modeling of multiple organizations to define the management of each of these organizations and keeps the contexts separate in relation to the different realms.

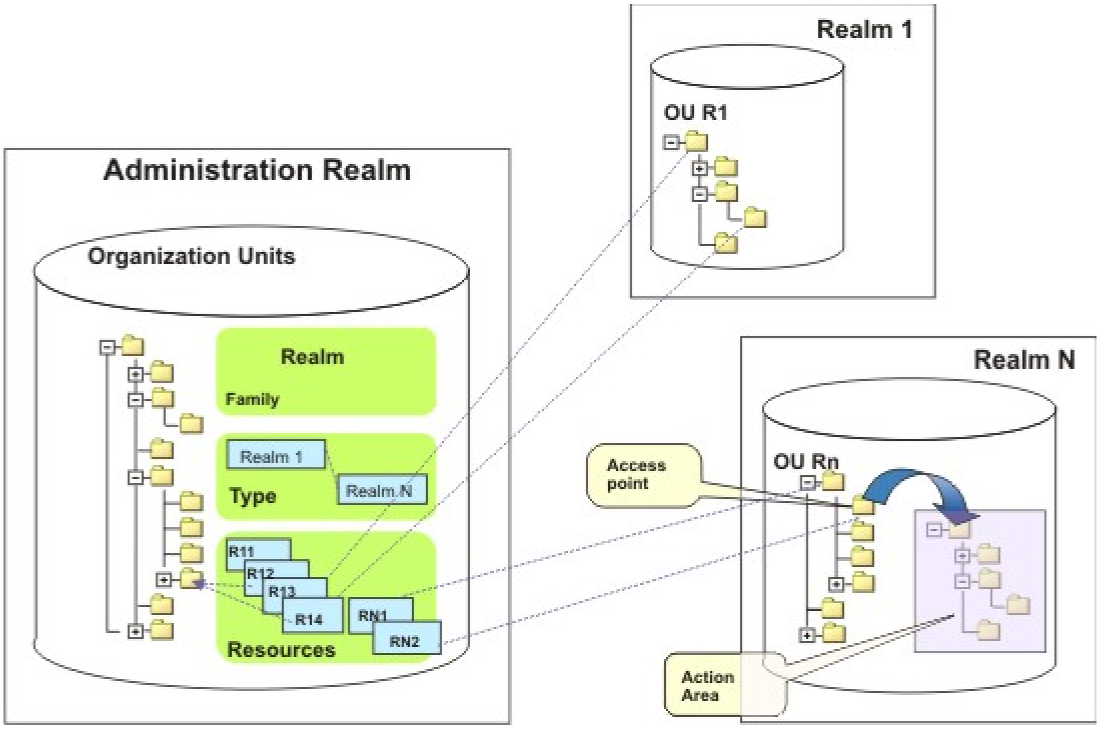


Figure 2. IBM Security Identity Governance and Intelligence realms

Each realm is separated from other realms. Data separation is assured and different set of policies can be applied for each realm. This feature can be useful for service providers, where each realm can contain a single customer.

IBM Security Identity Governance and Intelligence is provided with two standard realms:

Administration Realm
In this realm, IBM Security Identity Governance and Intelligence administrators, product administrators who can access product configuration and monitoring, are managed.

Production Realm
This default realm is not empty. It provides some basic configurations such as product rules, reports, and other basic settings.

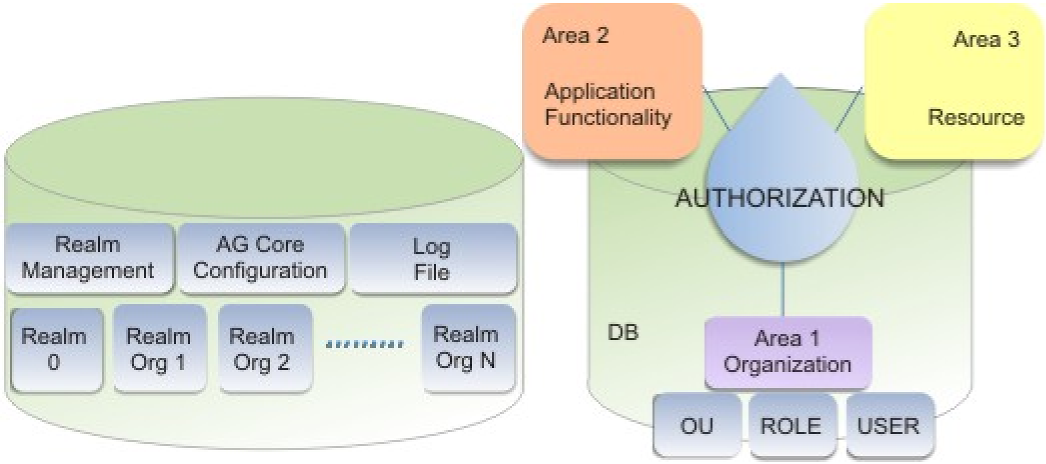


Figure 3. Logic architecture of the IBM Security Identity Governance and Intelligence Core DB

From a logical viewpoint, the IBM Security Identity Governance and Intelligence Core DB can be laid out in two main sections:

- The first section contains information for managing the realms and data for the AG Core configuration.
- The second section of the database contains as many copies as the number of realms or different organizations that are managed. Realm 0 is used to define administrators and authorizations that are related to them.

Organization unit

An organization unit is a basic element of an organization. An organization can be hierarchically structured in different ways according to different classifications.

For example, some organizations are organized by a geographical classification.

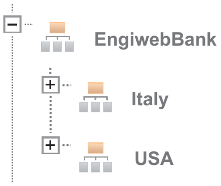


Figure 4. Geographical organization

Others must be organized through a hierarchy of functional units.

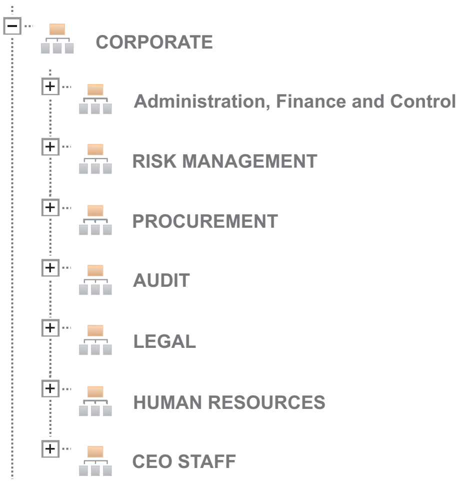


Figure 5. Hierarchical organization

Others might use a combination of both approaches.

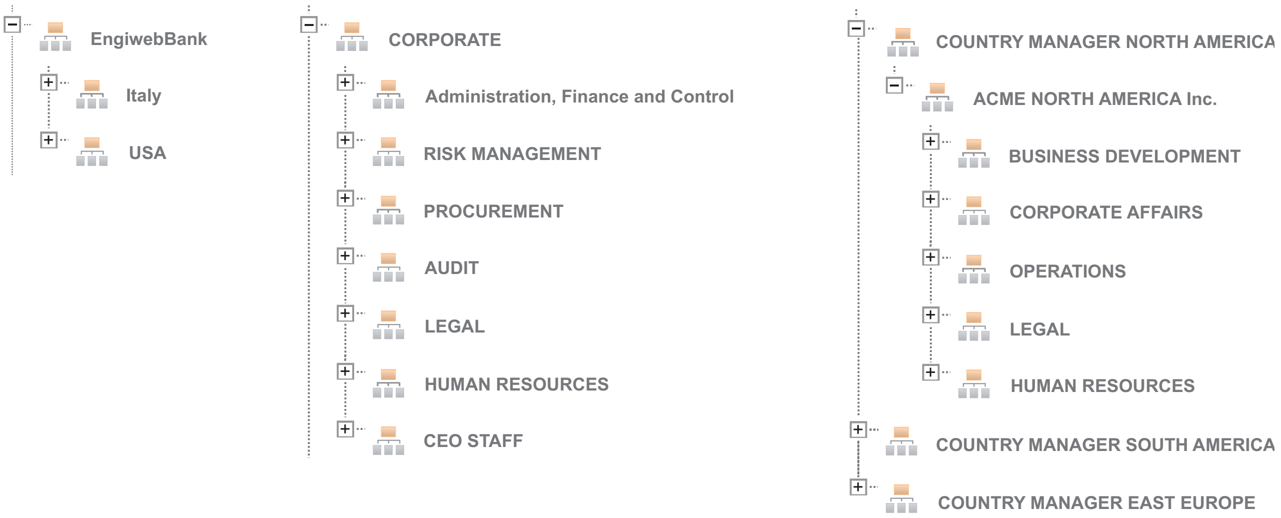


Figure 6. Mixed organization

Other possible classifications can be built as well.

In the IBM Security Identity Governance and Intelligence Core Model, every type of organization can be described as a hierarchy of organization units (OUs). Every OU in the hierarchy is displayed as an expandable directory tree if associated child elements exist with a free number of distinct levels in the hierarchy. A single OU is aggregated to a set of users and to a set of entitlements that can be assigned to every user.

Users, attributes, and polyarchies

In IBM Security Identity Governance and Intelligence, identities are called users.

A user represents a set of information that is connected to an individual or virtual identity (service users).

IBM Security Identity Governance and Intelligence supports the concept of primary and secondary users as well as user multiple entries (UME).

A UME can have more than one account on the same target system.

If users are separated for organizational reasons, IBM Security Identity Governance and Intelligence tightly connects the primary user with secondary users, UME, or both by automatically synchronizing any changes.

Different roles and permissions can be granted to primary and secondary users. IBM Security Identity Governance and Intelligence automatically incorporates authorizations for analysis (like SOD and risks).

In IBM Security Identity Governance and Intelligence a user:
- belongs to a specific group of a hierarchy
- is characterized by a set of permissions
- is aggregated to an account (at least one)
- can dispose of a set of resources
- is characterized by a set of user attributes.

User attributes can be expanded at any time.

Attributes and Polyarchies

In addition to the traditional representation of an organization as a hierarchy of Organization Units (OUs), other hierarchical views, commonly indicated as polyarchies, can be built based on user attributes.

A Polyarchy can be created at anytime by grouping users based on attribute values.

If the attribute contains hierarchy path, it is translated in a hierarchy notation; otherwise, the attribute is represented as a flat hierarchy.

For example, a multinational enterprise can build a polyarchy by using the attribute LOCALITY for grouping users based on their current workplace. You can then apply specific rules that are related to local regulatory laws, to certify a compliance criteria for any group of users.

Attribute-based Access Roles

Use the Access Governance Core module to build hierarchies based on different User attributes.

These attributes are made available through the Attribute Mapping of the USER_ERC table.

A user who belongs to a certain hierarchy can be linked to a specific Role related to that hierarchy.

For example, when you begin a complex project, you can set up a hierarchy of projects, structured in N sub-areas (Project 1, Project 2, ... Project N).

User Mark Brown, who belongs to an OU named Manager, holds all the roles needed for running managerial tasks in the Manager OU.

But Mark Brown is also the Project Manager of Project 3 in the Projects hierarchy. He is therefore assigned also all the necessary Access Attributes Roles (ABA Roles) for Project 3.

From this point of view, the traditional Role assignment policy, which is based mainly on OU hierarchy, is a specific instance of the ABA Roles approach.

Hierarchy of Entitlements

In the IBM Security Identity Governance and Intelligence data model, an entitlement identifies a structured set of permissions. These permissions are assigned to a generic user to access the resources of an organization.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:

Business Role (BRole) IT Role Permission

External Role

A business role (BRole) can be hierarchically formed by business roles, IT roles, external roles, and permissions. An IT role can be formed by IT roles and permissions. An external role can include other external roles and permissions.

The generic hierarchical structure of an entitlement is shown in the following figure.

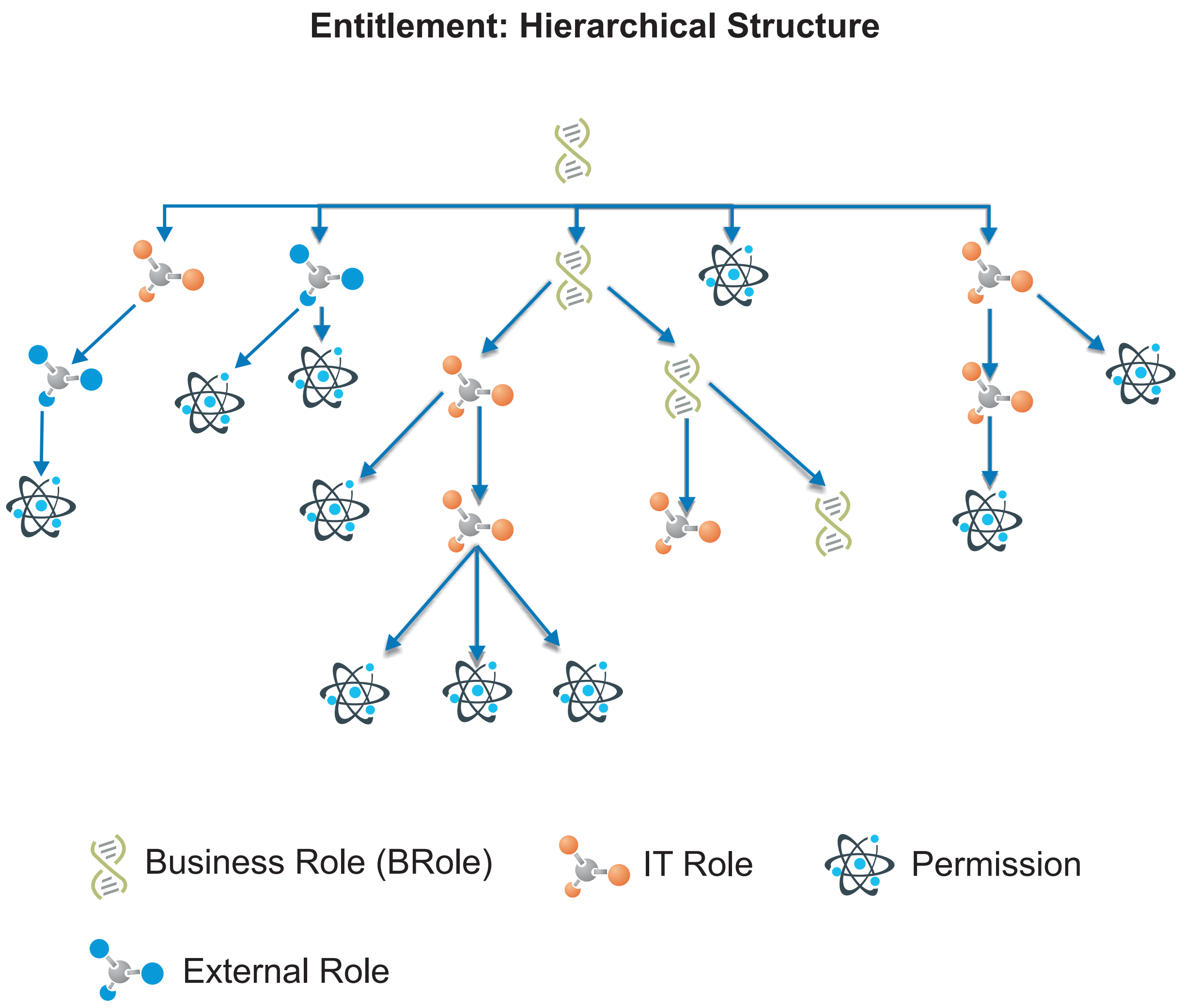


Figure 7. Structure of a generic entitlement

The IBM Security Identity Governance and Intelligence entitlements model does not limit the number of hierarchy levels.

Permissions can maps also user attributes (see Permissions based on user attributes).

In IBM Security Identity Governance and Intelligence, you can select *N* permissions that are filtered by an application in several sections. The IT Role object collects a set of permissions that are related to the same application.

You can have two types of scenarios.

- An entitlement that is assigned in a direct mode (direct assignment)
- An entitlement that is in a hierarchical structure (hierarchical assignment) is assigned in a hierarchical mode.

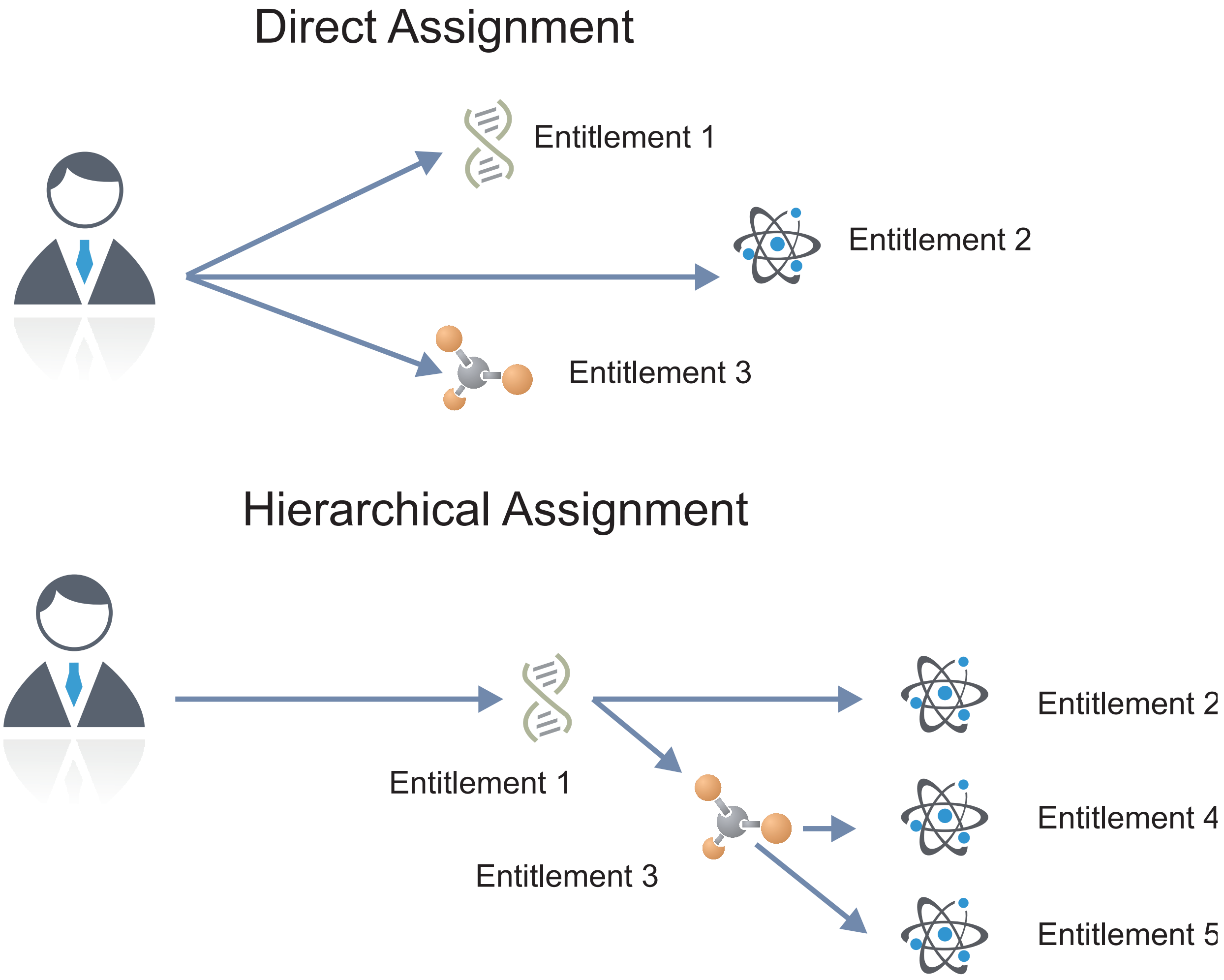


Figure 8. Direct and hierarchical assignment

If you assign the Entitlement 2 (Permission 2) to a user, you directly assign the Entitlement 2 only.

If you assign the Entitlement 1 (Business Role 1) to a user, you directly assign the Entitlement 1. Hierarchically, the user is assigned the Entitlements 2 - 5.

The permissions that are grouped in an external role are by definition that is handled by hierarchical assignment, since they cannot be granted individually.

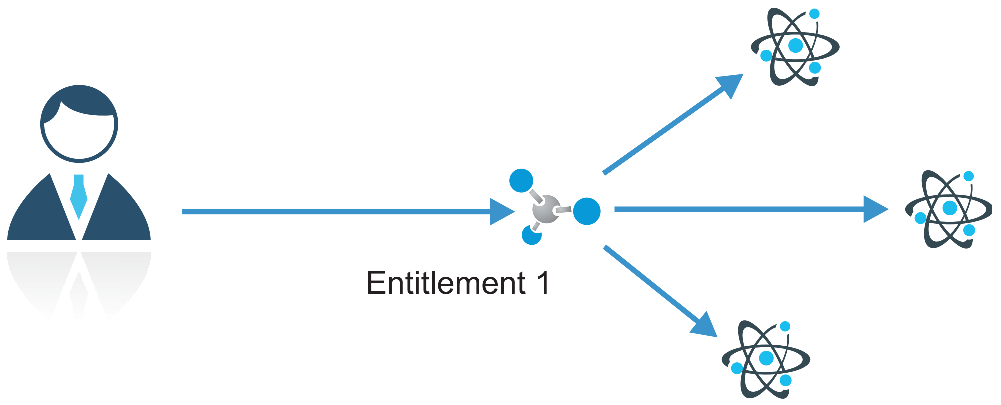


Figure 9. Hierarchical assignment for external roles

Before an entitlement is assigned, it must be published. An entitlement can be in the system, but is not available for assignment unless it is published.

Employment and resources

When an entitlement is assigned to a user that belongs to a specific OU, it also defines the user's employment. By extension, if a user is assigned two or more entitlements, two or more employments are defined for the user.

Resources are entities that are needed for a user to perform business activities. The resources are assigned to employment definitions.

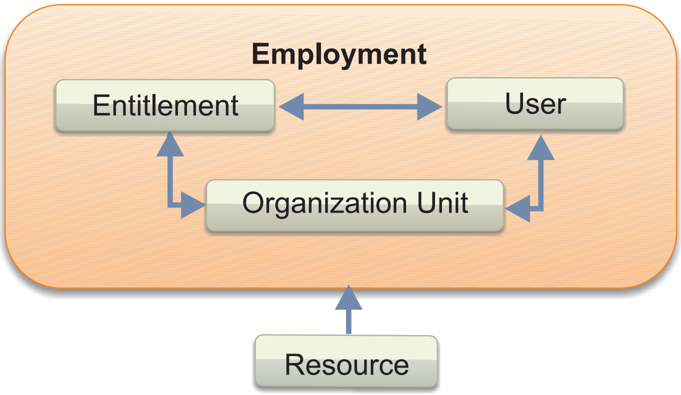


Figure 10. Employment and resources

Each employment can have any number or type of resources. The same resources can be assigned to different employments.

The use of resources considerably increases the flexibility and granularity for the definition of the IBM Security Identity Governance and Intelligence authorization profiles.

Aggregation user - entitlement can be considered as the "first-level" of authorization

Two different Users (U1, U2) who are assigned the same Business Role (BR1), possess the same first level of authorization.

Aggregation employment - resource can be considered as the "second-level" of authorization

Two different Users (U1, U2), are assigned the same business role (BR1) and belong to the same OU. They are characterized by the same employment, although their operations can be differentiated by their resource.

As an example, consider a banking scenario where two employees are in two different branches, one in Rome and the other in Milan.

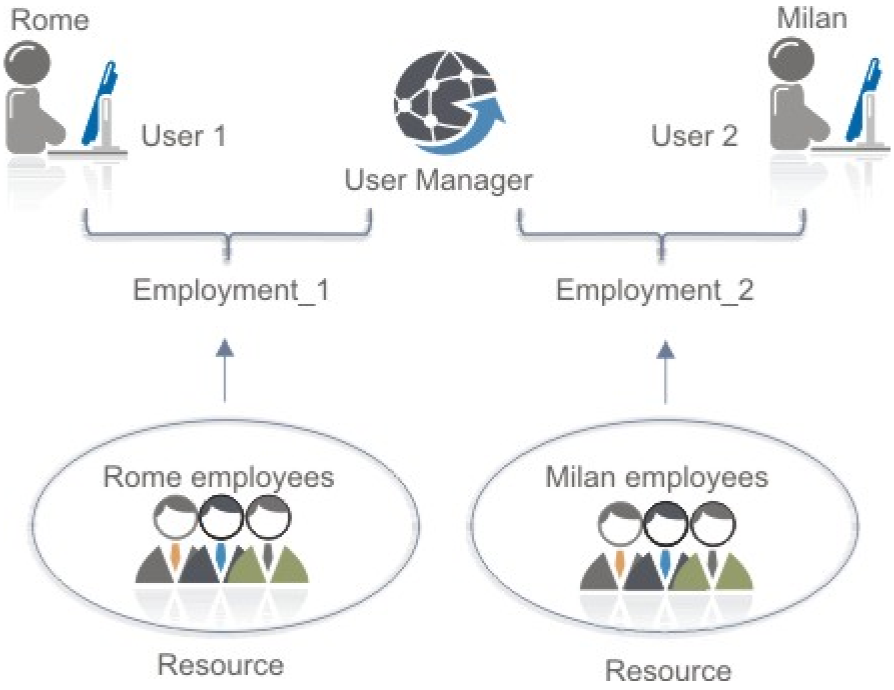


Figure 11. Second level of authorization

Holding the same role, they can access the same set of functions, but must obviously relate to the customers of their own respective branches. A customer resource that defines every customer through a current account number, differentiates the two users' operating environments, even if they hold the same role.

A resource can be connected to a user directly or by inheritance from the OU that it belongs to. Resources (objects in the RBAC model) are important for Authorization Server operations where unstructured data is the main part of the authorization process. Unstructured data can be network folders, files, or documents.

All the main entities of IBM Security Identity Governance and Intelligence model such as hierarchies, applications, roles, and risks are modeled as internal resources. They are used to restrict administrator access rights to a subset of administered entities. The intersection of different subsets of resources defines the scope.

Two IBM Security Identity Governance and Intelligence administrators with the same basic authorizations with different scopes have different operational impacts inside the organization. For example, two user managers or two security officers can have different sets of assigned resources.

Permissions based on user attributes

An attribute permission is a specific type of permission that is used for mapping a user attribute that is imported from a target system. For harmonizing this feature with the role-based access control standard of the Identity Governance and Intelligence data model, you can use permissions and rights.

Overview

A user attribute is mapped with an attribute permission.

If the user attribute is a Boolean data type:

- The attribute is mapped with the permission name, if the attribute value is *True*.
- The attribute is not mapped, if the attribute value is *False*.

If the user attribute is a string data type:

- The attribute name is mapped with the permission name.
- The attribute value is mapped with the value of a right that is associated to the permission (see Rights).

This mapping is fundamental for addressing some important features of Identity Governance and Intelligence, such as Segregation of Duties computing based on user attributes.

Attribute permissions icon

An attribute permission is represented by the ordinary icon used for any other permission.

Main properties and constraints

An attribute permission can host a right that is tagged as *required*, like a common permission (see Rights).

A required attribute permission maps a mandatory user attribute on the target system.

If the right is required, also the attribute permission must be considered required, and near the ordinary icon , the name of the permission is rendered in brown.

As with a common permission, the attribute permission can be associated to a user directly or indirectly (hierarchically), as shown in Hierarchy of Entitlements.

A required attribute permission builds a strong link with the user attributes on a target system. This link implies that there are some constraints and side effects that are related to operations of removing of attribute permissions.

Creating and deleting an attribute permission

An attribute permission can be created (registered) in the system or deleted like a common permission.

If you delete a required attribute permission that represents a mandatory user attribute, an event of deletion is automatically generated and sent to the target system.

If the user attribute is considered mandatory, thus *required*, on the target system, the deletion must be considered incongruous.

Adding and removing the association for user-attribute permission

An attribute permission can be associated (added) to a user like a common permission.

Several considerations must be carefully made when you plan to remove the association based on a required attribute permission.

A *required* attribute permission, which is directly associated to a user, cannot be removed (a message is displayed through the user interface).

The *required* property is linked to a mandatory user attribute on the target system.

However, in the Identity Governance and Intelligence data model, you can also associate a permission to a user in an indirect (hierarchical) way.

Commonly, you have users that are associated to a Business Role (or an IT Role) that can host a required attribute permission. In this case, it's always possible to remove the association between a user and Business Role (IT Role), but with side effects.

For example, you can remove the association *User - IT Role* for an IT Role with three permissions: P1, P2, and P3, where P3 is a required attribute permission. In this case, while the association with P1 and P2 is removed, P3 is associated directly to the user.

Specific actions when you remove the association for user-required attribute permission

If you remove the association of the user-required attribute permission through a Business Role (IT Role), a specific sequence of actions is performed by the system for every attribute permission that is involved:

1. The attribute permission is published (if not previously published).
2. The attribute permission is added, if not already present, to the organizational unit of the user, in visibility violation. If already present, the visibility violation attribute is absent.
3. Assign the attribute permission directly to the user.

Rights values are already set.

The user that is associated to the required attribute permission before the removal of the Business Role (IT Role), maintains it after the removal.

A *required* attribute permission, which is directly associated to a user, cannot be removed (a message is displayed through the user interface).

Related concepts:

Chapter 7, “Attribute-to-permission mapping service,” on page 69
Administrators can map account attributes from a target system to permissions in Identity Governance and Intelligence. Administrators can also map allowed values for attributes to rights values, so that you can set a business-friendly name for the rights value.

Related information:

“Attribute-to-Permission Mapping” on page 233
Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and Intelligence that is based on the attribute settings on the target systems.

“Insert Attribute-to-Permission Mapping Track” on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

“Application Access” on page 211
Documents how to manage application permissions.

Rights

Rights are extra attributes that are related to permissions.

A Right is defined by two qualifiers: **Key** and **Value**.

Key is an identifying name, while **Value** can be defined every time the right is defined.

Value can have a default value that can later be modified.

Rights can be either single-value or multi-value.

The following figure shows an example for a single-value right.

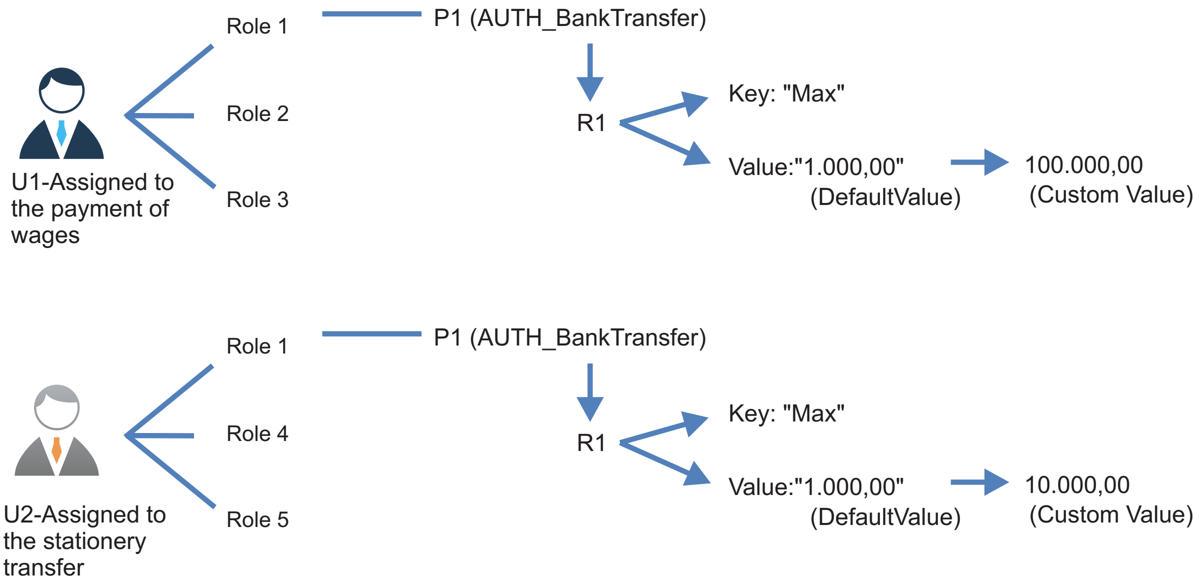


Figure 12. Single-value right

In this example, users U1 and U2 run different assignments. Both can make transactions (P1), as defined by the Role1 business role assigned to them.

Assigning a right, R1, to permission, P1, you can define the range of values available for transactions of each user.

Both U1 and U2 have the same default value of $1,000.00 as the lower boundary, but they have different upper boundaries.

U1 up to $100,000.00

U2 up to $10,000.00

The upper customized boundary value of R1 is defined when the permission is assigned to the user.

The following figure shows an example of a multi-value right.

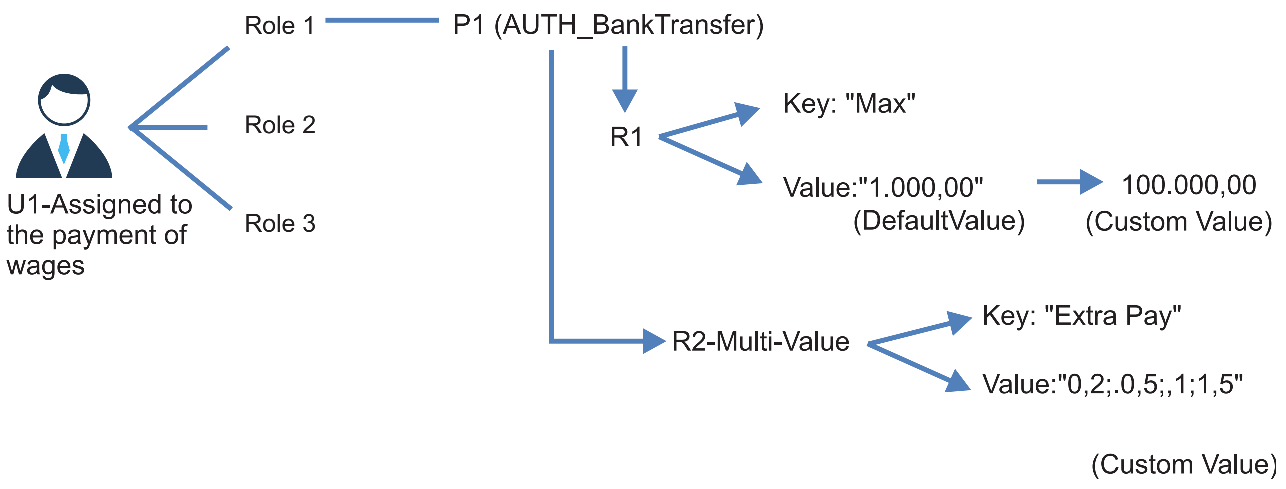


Figure 13. Multi-value right

User U1 is assigned to the payment of wages by rights R1 and R2. User U1 can modify the amount of wages for a worker according to a business policy named Extra Pay, the key of R2. The extra pay is a variable amount that is added according to the value of a multiplier, the R2 value. In the example, R2 has four possible values.

```
0,2 ; 0,5 ; 1 ; 1,5.
```

As the example shows, you can assign more than one single-value or multi-value right to the same permission.

You can choose from a predefined set of values by using **lookup**. These predefined values are assigned when a right is defined and added to a permission.

Lookup for a single-value right
You can choose only one value from the list of values.

Lookup for a multi-value right
You can choose one or more values from the list of values.

A right can be also **Required** or **Not Required**.

If the right is **Required**, at least one value have to be always set.

For more information about rights, see the following topics:

- Life-Cycle of a Right
- Rights and Resources

The lifecycle of a right

The lifecycle of a right is based on three steps:

1. Define a right and add it to a permission:
   a. Define a lookup table of values (optional): you can define multiple lookup tables, to represent different set of values. See **Access Governance Core** > **Configure** > **Rights Lookup**.
   b. Define a right joined to a permission (see **Access Governance Core** > **Manage** > **Application Access** > **Rights**.
2. Assign a right to a user.

3. After you assign a right to a user, the value of a right can be updated. See **Access Governance Core** > **Manage** > **Users** > **Rights**.

You can assign rights to a user in different modules of IBM Security Identity Governance and Intelligence:

Assignment	Modules
Assign a permission aggregated to a right.	Access Governance Core, Business Activity Mapping
Assign an entitlement that hosts a permission aggregated to a right.	Access Governance Core
Assign a one or more permissions to an activity.	Access Risk Controls
Assign a permission or entitlement through an authorization workflow.	Access Request
Assign a permission or entitlement through the rule engine.	Access Governance Core or any other business process triggered by a rule

Rights and resources

It is important to understand the difference between rights and resources.

- A resource determines a second level of authorization for a specific entitlement.
- A right determines the set of values for a generic transaction that is enabled by a permission.

Returning to the example shown for resources, consider a banking scenario where two employees are in two different branches, one in Rome and the other in Milan. They have the same role and they can access the same set of functions but have different customer resources that are specific to the branches.

Add a permission, **Check Validation**. It has a single-value right, **Amount**, in which the value joined to the key can vary. The bank can provide a policy that uses a specific procedure to validate any check that exceeds a specified value.

Two employees with the same role who work on different customer resources with a specific permission that enables them to validate checks. Use the right added to the permission to enable different validation policies.

Applications

In IBM Security Identity Governance and Intelligence, an application is a set of permissions that are related to a certain target. IBM Security Identity Governance and Intelligence visualizes and extends the concept of target as a "pure technical view" of an IT application and is only suitable for provisioning.

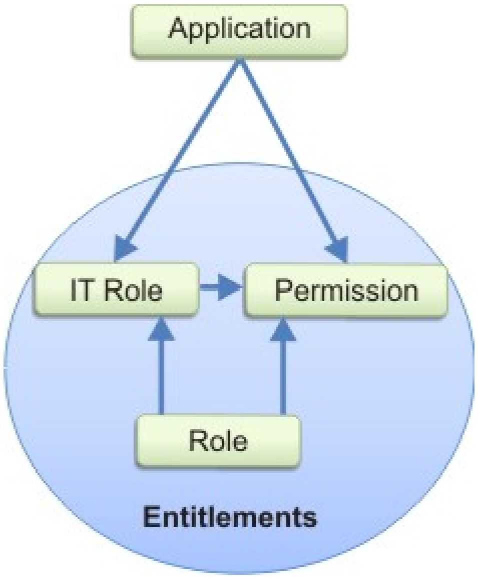


Figure 14. Application entitlements

Every target can host several applications. A target can be often used as an authentication or authorization server, for example Active Directory (AD), where different applications share different permissions with a single account.

Many applications that are connected to the same target can share account configuration policies and can be subject to several:

- Provisioning policies
- Logical configurations
- Risks

Applications, targets, and account policies, for example password policies or UID rules, are tied together. There can be one or more targets to an application, or one or more accounts to a target, or one or more accounts to an application. The IBM Security Identity Governance and Intelligence model manages the policies that are implied in these relations. For example, password synchronization between different targets that share an account policy.

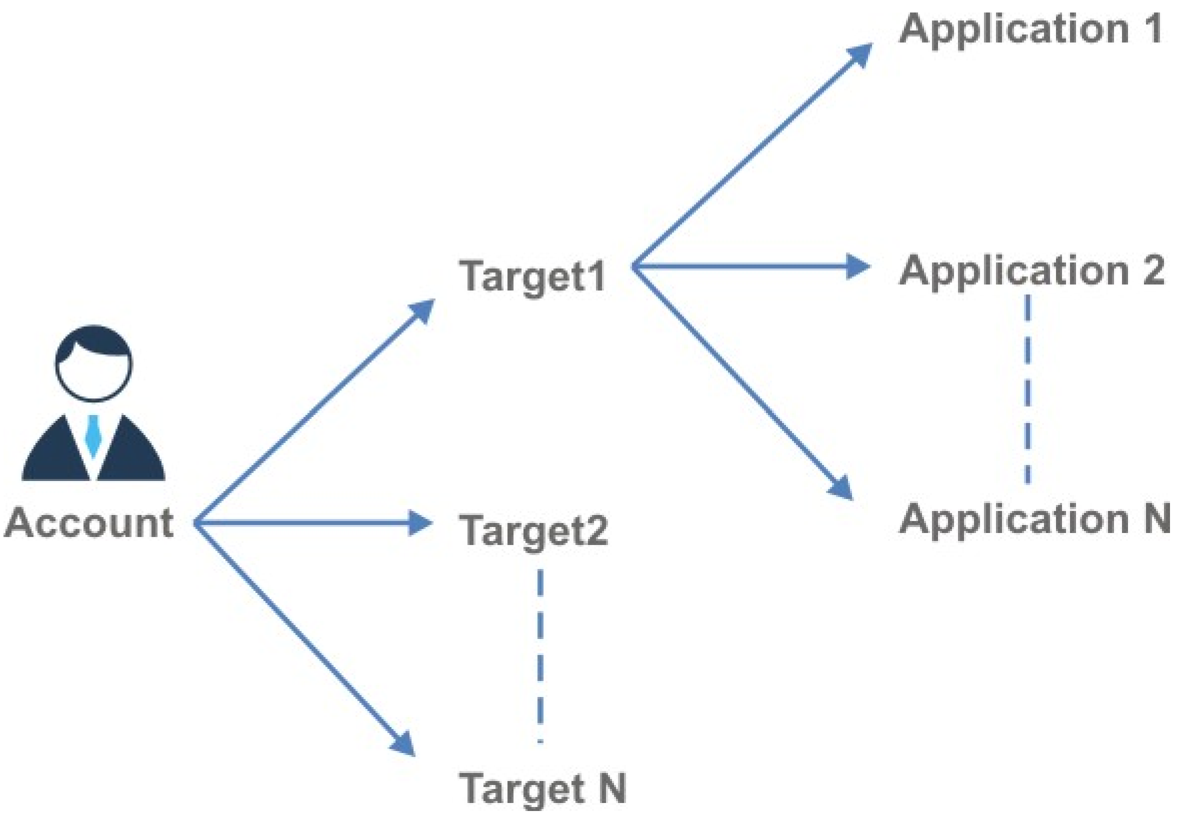


Figure 15. Accounts, targets, and applications

Applications can be either:

Custom

These applications use Java API or the web services of IBM Security Identity Governance and Intelligence platform, the IBM Security Identity Governance and Intelligence SDK, for authentication or authorization activities. For this type, the AG Core module operates as the authorization server.

External

These applications use external authorization systems that are connected to the AG Core module.

For example, Active Directory (AD) is an external authorization system or target system.

IBM Security Identity Governance and Intelligence can be also configured to send events, such as add or remove permissions, to targets or applications. These events are sent through the IBM Security Identity Governance and Intelligence Integration Interface and Enterprise Connectors module.

Accounts

In the IBM Security Identity Governance and Intelligence data model, a user can be added to a specific account.

An account is the IT representation of an identity, expressed through an account configuration, made-up by a set of user information such as UID, email, password, and status. An account configuration is used by an application that requires authentication of the user.

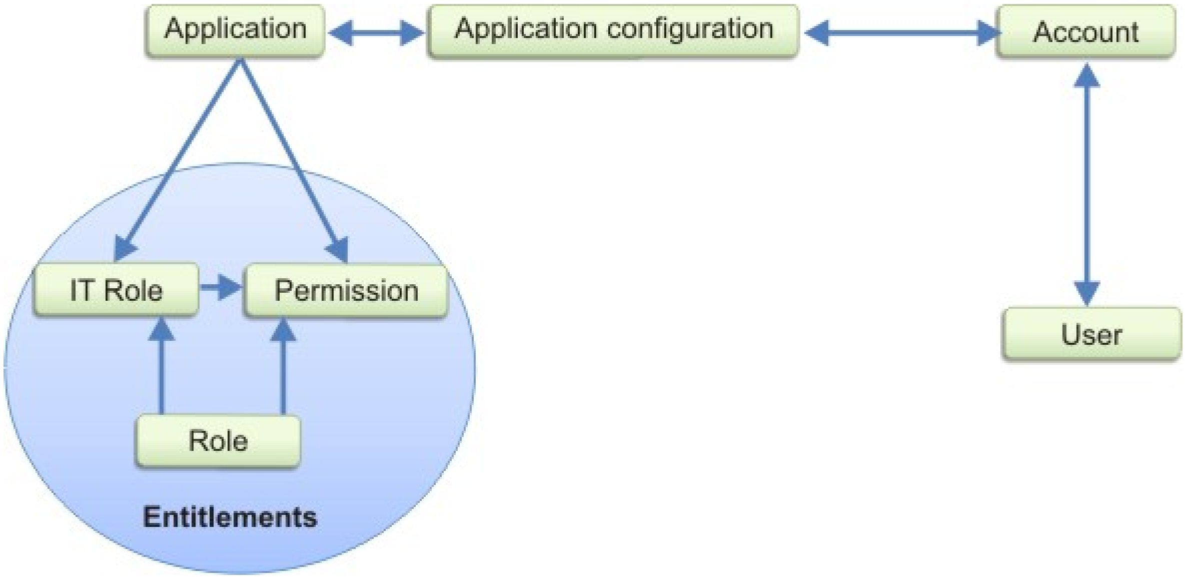


Figure 16. Application and account relationship

Several users can be associated with the same account configuration and use the same authentication rules for the same application.

Account configurations are used to define account properties; in particular, password settings.

In IBM Security Identity Governance and Intelligence, multiple accounts can be assigned to a single user. The user can manage different passwords and lock status for each application.

Every user that is registered in the IBM Security Identity Governance and Intelligence platform is automatically added to the IBM Security Identity Governance and Intelligence account configuration.

Note: In IBM Security Identity Governance and Intelligence, entitlements are tied to users rather than to accounts. A role is assigned to a user and cannot be assigned to an account because a role can contain permissions for different applications that are related to different accounts.

IBM Security Identity Governance and Intelligence extended data model

The IBM Security Identity Governance and Intelligence extended data model supports the risk definition and detection layer of IBM Security Identity Governance and Intelligence.

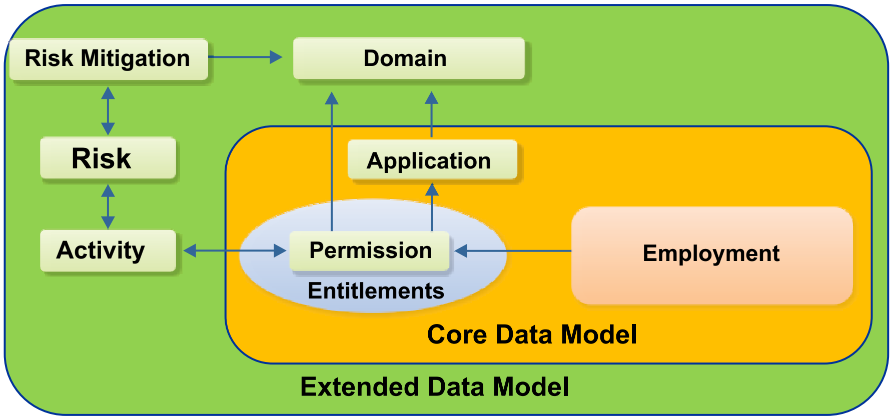


Figure 17. IBM Security Identity Governance and Intelligence extended data model

The Access Risk Controls (ARC) module manages this layer based on two relationships.

- The relation between the business activities model and the RBAC model.
- The relation between risks and business activities.

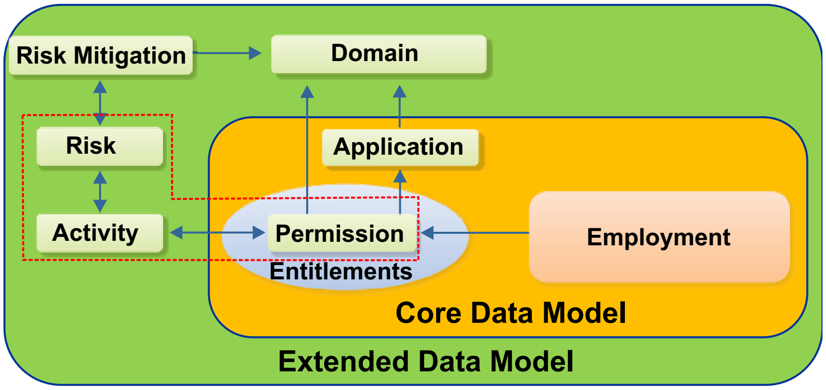


Figure 18. IBM Security Identity Governance and Intelligence extended data model - subsystem risk, activity, and permission

IBM Security Identity Governance and Intelligence extended data model has these main model elements:

- Business Activities Layer and RBAC Model
- Risk Definition and Detection
- Segregation of Duties
- Risk Mitigation
- Mitigation Actions
- Domains
- The Risk's Hierarchy

Business activities model and RBAC model

IBM Security Identity Governance and Intelligence integrates and correlates the business activities model of an organization and the RBAC model that IBM Security Identity Governance and Intelligence is based on.

Business activity is an innovative key concept for modeling a specific task or set of tasks by defining a specific part of a generic business process. A process can be structured as a set of activities.

An activity identifies an operation or a uniform set of operations that the user can perform.

A generic business process is structured through a set of activities. Each activity can be subdivided into subactivities. Multiple activities can be grouped to form a macro-activity. An activity hierarchy is defined and organized as a tree structure, an activity tree.

Each activity requires one or more entitlements. An entitlement is the permission that a user needs to perform the activity.

In the RBAC model, a role is a particular type of entitlement that can be assigned to a user. The role and can have multiple permissions that are arranged in a hierarchy.

By linking the business model to the RBAC model, each activity can be aggregated to the necessary entitlements or permissions.

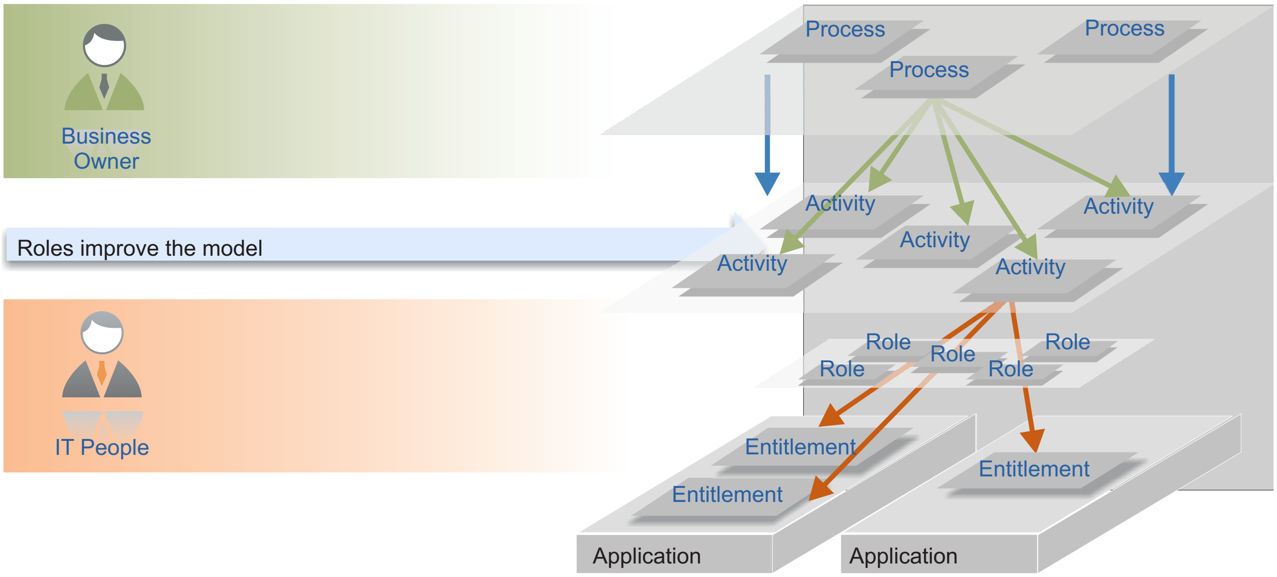


Figure 19. Business model linked to the RBAC model

Risk definition and detection in IBM Security Identity Governance and Intelligence

Risk is a wide range of possible critical situations that can be associated with a generic business activity.

In the IBM Security Identity Governance and Intelligence data model, a specific business activity can be associated with a risk.

This information is used to evaluate the "aggregated risk" of the set of activities that are assigned to a user.

Consider a financial management activity and an ICT technical activity. Typically, these types of activities require specialized and extensive knowledge.

Is it reasonable to entrust these activities to the same user?

From an organizational standpoint, depending on the user's prevalent competency, either financial or technical, there is a valid risk in assigning these two unrelated activities to a single user. An activity such as financial management can be considered sensitive even if it is not part of a set of activities. It makes sense to associate a risk evaluation to a single activity.

Generally, possible aggregations are of the following type:

- A risk to a single activity
- A risk to a single set of at-risk or conflicting activities
- Multiple risk to a single activity
- Multiple risk to a single set of at-risk or conflicting activities

According to this information, it is possible to evaluate the aggregated risk of the set of activities that are assigned to a user.

The ARC module extends features of the RBAC model by introducing the concept of at-risk activities and provides the tools necessary to link activities to entitlements or permissions.

The assessment of the risk level of activities can be translated into the risk level of entitlements or permissions that are assigned to users involved in those activities.

The following figure shows all the IBM Security Identity Governance and Intelligence extended data model elements that are involved in the risk definition and detection layer.

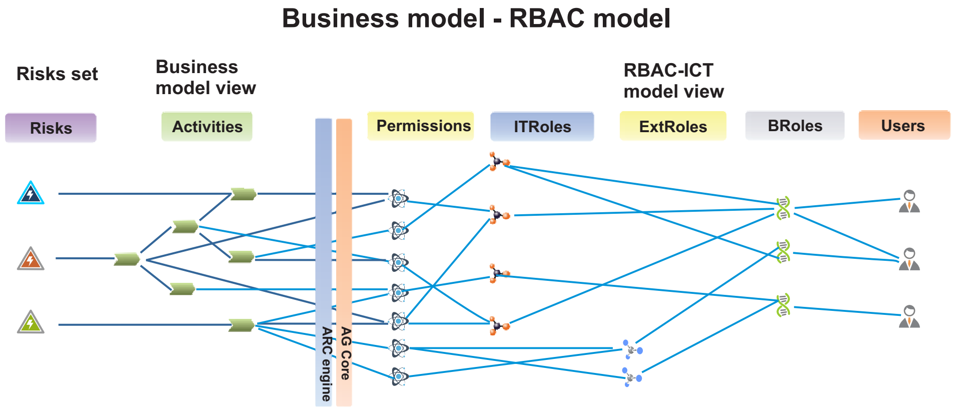


Figure 20. ARC engine and AG Core: Business Model - RBAC Model

The figure shows an example with few elements.

In a generic large organization, you might find:

- Permissions (>200,000)
- IT roles (>100,000)
- External roles (>15000)

- Business roles (>1000 and <5000)
- Business activities (<500).

In a large organization, the number of business activities is drastically lower than roles and permissions.

The advantage of defining risks as activity-driven is clear. By using the assessment of risk that is associated with activities, conflicts among permissions or entitlements can be traced. Conflicts among roles are easier to trace. They are less complex because the number of activities is lower than the number of permissions or BRoles.

Segregation of Duties (SoD): a specific type of Risk

It is important to prevent members of an organization from gaining operational privileges that might cause conflicts of interest that can be detrimental to the organization.

You must establish constraints when you assign entitlements to users.

Segregation of duty (SoD) mechanisms are designed to manage conflicting relationships between certain model entities. Entities that are characterized by reciprocal conflict, cannot be aggregated to the same user.

IBM Security Identity Governance and Intelligence data model identifies a SoD risk as a specific type of risk. Most of the existing models for SoD show that conflicts are defined based on permissions and roles.

Defining conflicting roles can lead to inconsistent results.

For example, an organization has three roles, R1, R2, and R3. Two of these roles, R1 and R2, are defined as conflicting.

If R2 and R3 are built with the same permissions, then both pairs (R1, R2) and (R1, R3) would give the user access to conflicting permissions. Basically R2 is equivalent to R3, even though, by definition, only the pair (R1, R2) can be considered as conflicting roles.

According to the RBAC model, roles are containers of groups of permissions; the user's actual operating capacity depends on the permissions that define the operational characteristics of a role.

In the previous example, one method is to redefine the conflicting permissions. The conflict between roles is caused by the conflicting permissions.

In large organizations, IT systems can register hundreds of thousands of permissions. Redefining permissions is impractical.

The ARC module offers a different approach that reduces the complexity of the problem. An SoD is defined by activities. An SoD risk arises when a specific set of activities is performed.

There is also the option of managing External SoD, based on risk information provided directly by an external system.

External SoD

In some situations, it is possible to read risk information raised on a given user from an external target system.

This action proceed through a **ReST** web service or a specific **Java class** that transforms the data from the target system in a consistent IGI format.

The risk detected, related to users registered into IGI database, is shown in the same way as the "internal SoD" information.

However, internal/external SoD are two options mutually exclusive and you can set it from **Access Governance Core** > **Settings** > **General** panel of **Access Governance Core** module.

When you use External SoD, some functions are not effective because External SoD is not associated with some elements of IGI data model.

Generally, any type of function that involves the management of risk mitigation is not relevant when External SoD is set.

The following functions might be available through the User Interface, but they do not provide relevant results when you set the External SoD:

- Associate mitigation to SoD Risks. See **Access Risk Controls** > **Manage** > **Mitigation Controls** > **Applicable Risks** > **Actions** > **Add** or any functions in **Access Risk Controls**.
- Configure a campaign of type **Risk Violation Mitigation**. See **Access Governance Core** > **Configure** > **Certification Campaigns** > **Actions** > **Add**.
- Run certification campaigns of type **Risk Violation Mitigation**. See **Access Certifier**.
- Run a specific subset of reports. See the official list of available reports.

Risk mitigation: classes of mitigation

You can reduce risks by preventing users from performing activities that conflict with each other.

Sometimes in a business situation, users must be able to work despite the presence of an SoD conflict or other types of risk.

For example, a user that is covering for another employee, who is on holiday, needs to gain access to a particular repository of the company. A risk violation review detects a conflict and denies the user access to the repository.

If the SoD requirements are strictly observed, the data in this repository is inaccessible, and the user cannot perform the functions of the absent employee. The company loses productivity and in some cases, more than an SoD violation can be generated.

You can use a mitigation control policy to resolve this situation.

Mitigation control is a policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

The user can access the restricted repository, if a mitigation control that provides a complete and in-depth trace of the user's activity on the repository, is activated.

This solution:

- Does not nullify the SoD or other type of risk constraints that arise from the conflict analysis.
- Enables the user to perform work activities.

Mitigation Control is not a workaround to evade the SoD or other types of risk requirements. Rather, it is an added control that enables the user to perform some needed tasks during a transitory but critical time period. You can aggregate a mitigation control to a user for an indefinite time period. A user can have *N* aggregated mitigation controls.

The same user can be involved in a set of risks or conflicting activities.

You can aggregate mitigation controls in a number of ways:

- A single mitigation control with a single set of risks or conflicting activities
- A single mitigation control with a subset of a set of risks or conflicting activities
- More than one mitigation control that is aggregated to a single set of risks or conflicting activities - over mitigation
- Sets of conflicting activities that are not aggregated to any mitigation control - under mitigation
- A mitigation control that is not aggregated to any activity.

It is common to have different sets of risk activities, where every set can be characterized by a specific risk. A user that is involved in a specific set of activities, is exposed to the related risks.

For every specific risk, several mitigation controls are available and every set of risk activities can be aggregated to more than one risk.

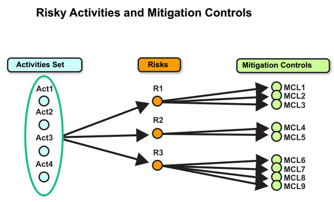


Figure 21. Risk activities and mitigation controls

The following figure displays a simple case, where every set of risk or conflicting activities is composed of two activities only.

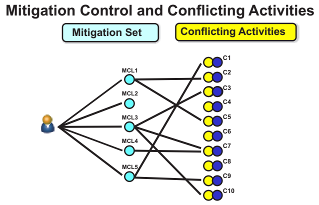


Figure 22. Mitigation model

MCL4 is aggregated to C7 only.

Mitigation control MCL1 is aggregated to C2 and C5; MCL3 to C3, C7, and C10; and MCL5 to C1 and C9.

C7 is aggregated to MCL3 and MCL4.

C4, C6, and C8 are not aggregated to any mitigation control.

The following references describe the four classes of mitigation:

- Under Mitigation
- Over Mitigation
- Under/Over Mitigation
- Complete Mitigation

Under mitigation

Under mitigation occurs if an MCL is not aggregated to the conflicting activities, as shown for C3 in the following figure:

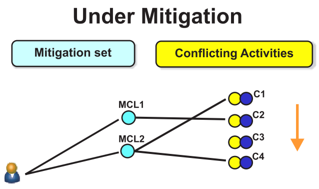


Figure 23. Under mitigation model

Over mitigation

Over mitigation occurs if the mitigation control MCL3 is aggregated to C5 only, as shown in the following figure:

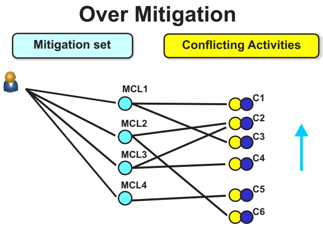


Figure 24. Over mitigation model

MCL2 and MCL3 are aggregated to the same pairs of risking/conflicting activities. So, in this case the aggregation arrow MCL3-C2 can be deleted.

Under-over mitigation

Under-over mitigation occurs if an MCL is not aggregated to some of the conflicting activities and one or more MCLs are aggregated to the same activities, as shown in the following figure:

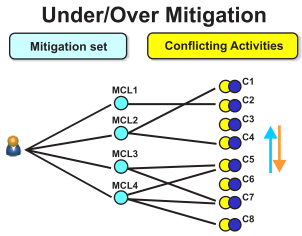


Figure 25. Under-over mitigation model

C3 and C6 do not have any MCL aggregated, while MCL3 and MCL4 are aggregated to the C5 and C7.

Complete mitigation

Complete mitigation occurs if every set of risk or conflicting activities is covered by at least one mitigation, as shown in the following figure:

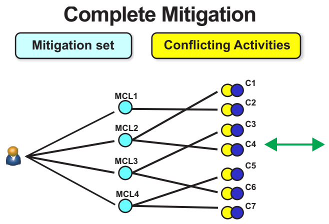


Figure 26. Complete mitigation model

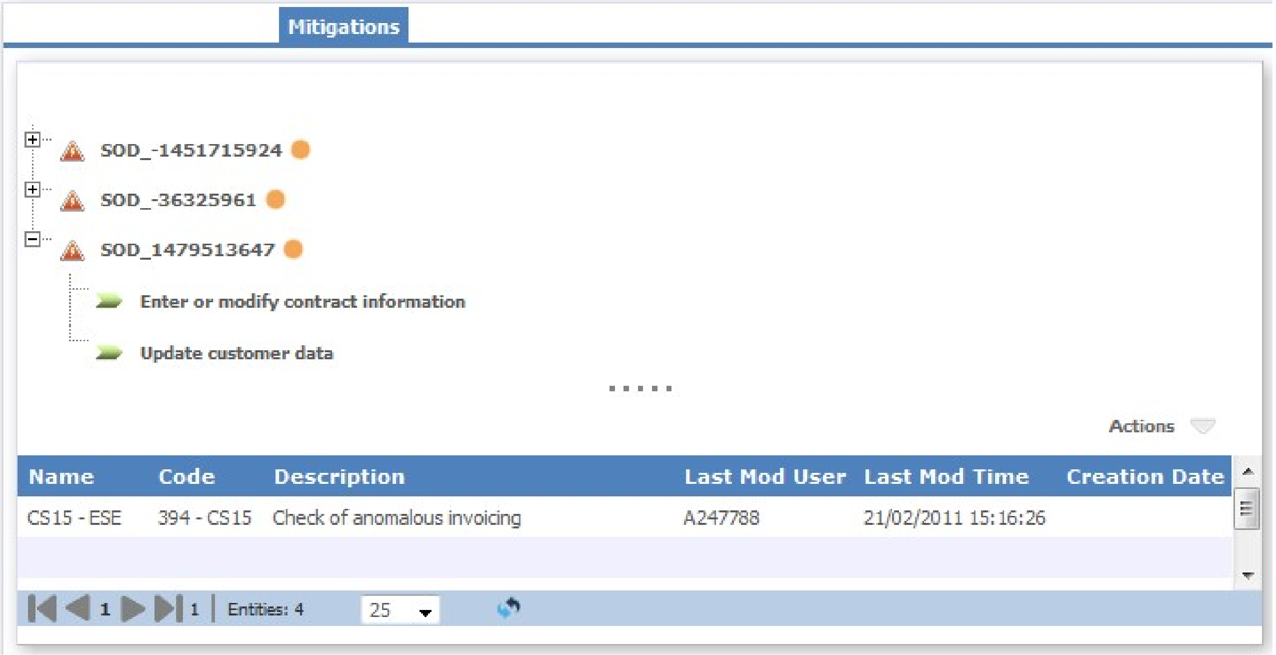
Mitigation actions

You can define mitigation actions to manage risks based on the needs of the user.

In IBM Security Identity Governance and Intelligence, it is possible to define mitigation actions according to the Risk management needs related to a user.

The first step is to deploy a mitigation and join it to a specific risk (see ARC module, **Manage** > **Mitigation Controls** > **Actions menu** > **Add**).

Through two modules of IBM Security Identity Governance and Intelligence, ARC and AGC, you can join a mitigation to a user by using the **Mitigations** tab that is shown in the following illustration:



SOD_-1451715924

SOD_-36325961

SOD_1479513647

- Enter or modify contract information
- Update customer data

Name	Code	Description	Last Mod User	Last Mod Time	Creation Date
CS15 - ESE	394 - CS15	Check of anomalous invoicing	A247788	21/02/2011 15:16:26	

Figure 27. Mitigation GUI

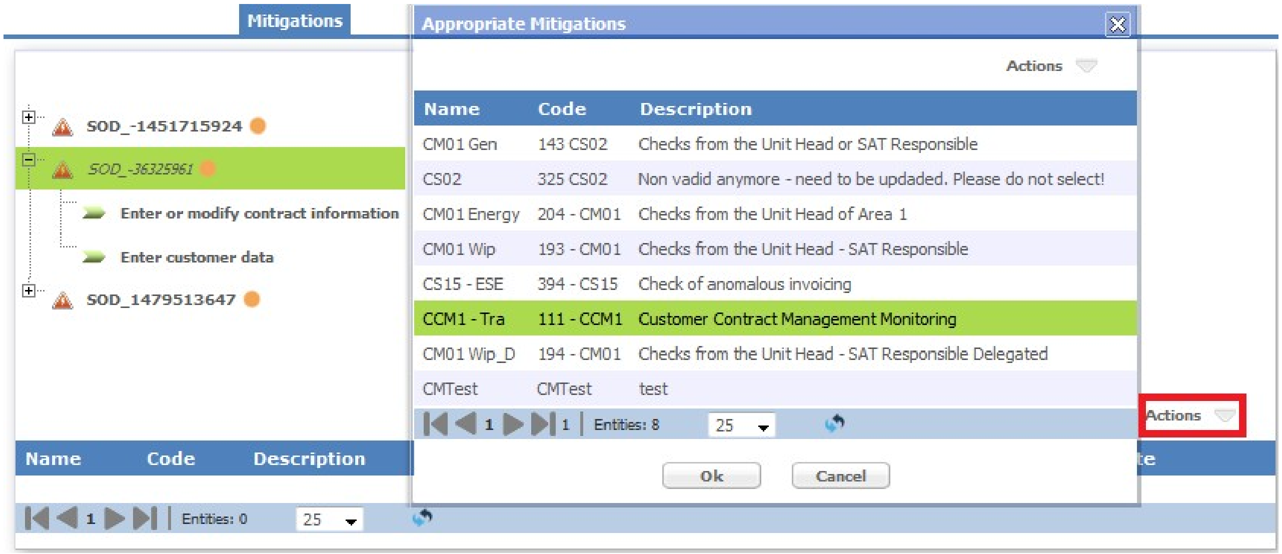
In the upper part of the GUI, the risk joined to a user is described.

In the lower part, mitigations that are already assigned to the user are listed.

In this example, the mitigation CS15 - ESE is already assigned to the user but it is not joined to any of the risks that are shown in the GUI. The user is in a situation that is known as over mitigation. To remove a useless action of mitigation is not mandatory, but can be considered as a best practice.

A generic risk is characterized by any set of risk activities. In this example, a risk is defined by only two activities.

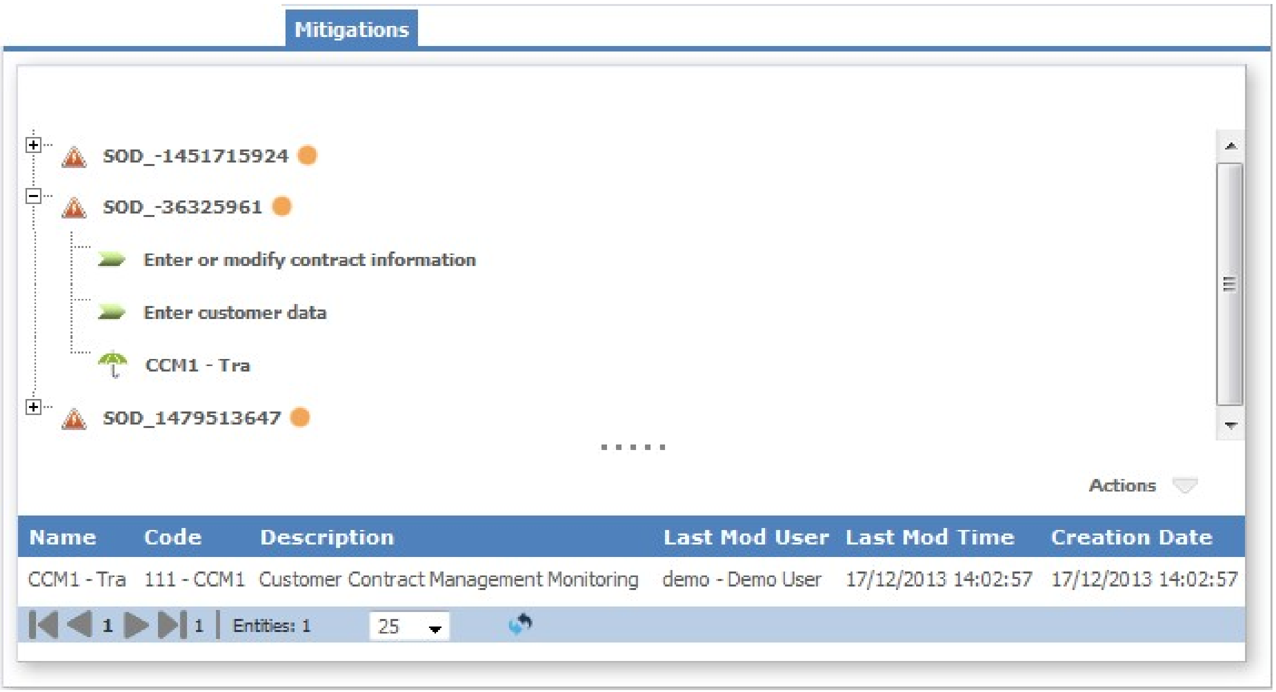
After the risk selection, from the **Actions** menu, you can add or remove a mitigation.



Name	Code	Description
CM01 Gen	143 CS02	Checks from the Unit Head or SAT Responsible
CS02	325 CS02	Non vadid anymore - need to be updaded. Please do not select!
CM01 Energy	204 - CM01	Checks from the Unit Head of Area 1
CM01 Wip	193 - CM01	Checks from the Unit Head - SAT Responsible
CS15 - ESE	394 - CS15	Check of anomalous invoicing
CCM1 - Tra	111 - CCM1	Customer Contract Management Monitoring
CM01 Wip_D	194 - CM01	Checks from the Unit Head - SAT Responsible Delegated
CMTest	CMTest	test

Figure 28. Mitigation GUI: add a mitigation to a selected risk

The mitigation that was added to mitigate the risk SOD_-36325961, is shown in the risk tree with a green umbrella icon



Name	Code	Description	Last Mod User	Last Mod Time	Creation Date
CCM1 - Tra	111 - CCM1	Customer Contract Management Monitoring	demo - Demo User	17/12/2013 14:02:57	17/12/2013 14:02:57

Figure 29. Mitigation GUI: added risk

Domains: conflicting and risk activities

A domain is a set of data that is subject to conflict analysis.

Domains are used to separate an enterprise into logically separate business areas.

It can coincide with the entire set of model data or with a single subset.

The data domain is used by the ARC module to implement a "correlation" between the activities a conflict analysis is required for.

Consider for example, the case of the two activities A1 and A2:

- A1: Payment of suppliers
- A2: Quality control of goods that are purchased by suppliers

To avoid a potential conflict of interest, these activities must not be completed by the same user.

Assume that activity A1 is performed by a user in relation to stationary goods in a certain OU within the company. The same user is authorized to complete activity A2 relating to raw materials used for the production processes of the OU. For example, PVC sheets that are used to produce molded plastic utensils.

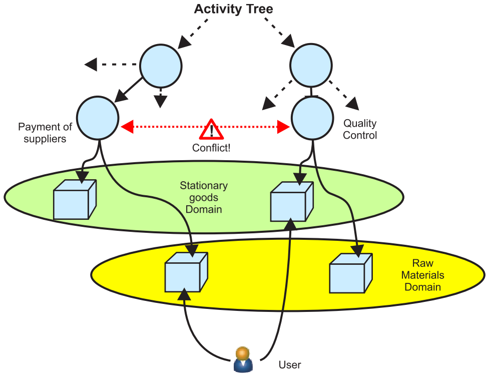


Figure 30. Data domains

The analysis of conflicts is performed where it is logical to perform it, where the two activities can occur on the same data domain.

You must contextualize the meaning of activities A1 and A2 by introducing two different domains, stationary goods and raw materials. Using two domains neutralizes the conflict between activities A1 and A2 for the user.

In the ARC model, a data domain is identified as a set of data on which various applications can operate. A domain can be identified by a set of applications. However, an application can be contained in various domains. Suppose that each application has only one corresponding permission. By using the ARC module, it is possible to aggregate applications with domains by using the link between applications and permissions. Permissions are in turn related to the domains.

The following figure shows a qualitative example of the description:

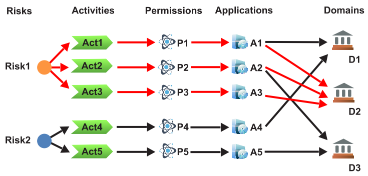


Figure 31. Activities, permissions, and domains

Assume that two risks exist: Risk1 and Risk2.

Risk1 arises if a generic user runs all of the three activities: Act 1, Act 2, and Act 3.

The same occurs for Risk 2 joined to activities: Act 4 and Act 5.

In this example, the five activities are linked to the five permissions P1, P2, P3, P4, and P5. These five permissions are linked 1:1 to five applications A1, A2, A3, A4, and A5.

The red arrows indicate that activities Act 1, Act 2, and Act 3 need permissions P1, P2, and P3 that link to application A1, A2, and A3. These three applications are hosted on Domain D2.

Risk1 falls into D2 and any user that performs Act1, Act2 and Act3 is considered as a risk user in that domain.

A user who performs activities Act 4 and Act 5 is not considered a risk user because those permissions and applications are linked to different domains D1 and D3. Risk 2 is neutralized.

How to read the tree of the risks of a user

The **Risk Info** graphical user interface (GUI) hosts an expandable tree structure.

At the root level, **Level 0**, you find one or more domains at the same level. 🏛

Expanding the **Domain** node, you can find one or more risks at **Level 1**.

Risks are divided into two categories:

- ⚠ **SOD risk**
- ⚠ **Generic risk**

Every risk is characterized by a specific risk level:

- 🔴 High
- 🟠 Medium
- 🔵 Low

For every risk at **Level 2**, you find at least one set of risky activities. ➤

For every activity at **Level 3**, all of the entitlements that are associated with that activity are listed.

For any generic couple, **Activity 1** - **Activity 2** for example, that consists of conflicting, or risky, activities, every **Activity 1** entitlement conflicts with every **Activity 2** entitlement.

A mitigating action, indicated by the presence of the following icon, is provided for a risky activity or for a couple of conflicting activities: ☂

One or more mitigations can be provided for each risk.

Introduction to Rules Engine

IBM Security Identity Governance and Intelligence platform implements a complete model of a generic organization, containing:

- All entities that are registered in the organization such as users, applications, and roles
- Links and relationships between these entities
- Policies and processes that the organization uses to manage these entities, such as automatic creation of a company email account for a new employee.

To cater to different organizations, the IBM Security Identity Governance and Intelligence platform needs to be structured in the following manner:

- With a robust data model, to manage common and standard authorization paradigms
- With a flexible engine to construct business policies that cover different situations in various organizations, ones that vary throughout the lifecycle of an organization.

For addressing the second point, IBM Security Identity Governance and Intelligence adopts a solution based on a rules engine.

Rules can be used in different situations and can be considered a layer of intelligence that enhances the expressive nature of the data model. The rules engine guarantees the flexibility and expressive strength that is required to model the customization of all company processes, especially those processes that are subject to frequent change.

In the current version, rules can be managed in these modules:

- The Access Governance Core module
- The Access Requests module (according to Process Designer configurations)
- The Enterprise Connectors module
- The Access Risk Controls for SAP module

To access the rules section in Access Governance Core, Process Designer, and Access Risk Controls for SAP, from the tabs bar select **Configure** > **Rules**.

To access the rules sections in the Enterprise Connectors, from the tabs bar select **Manage** > **Connectors** > **Channels**.

Drools rules engine

A rules engine (RE) is a module that automates the management of certain highly variable processes. The fundamental concept consists of separating the objects that are involved in processes from the logic that implements those processes.

The logic is defined by writing rules. For each process, the RE recognizes which rules to apply and on which objects to operate. If there is a variation in the logic, the rules can be changed without having to intervene in the system architecture. The IBM Security Identity Governance and Intelligence framework uses the open source Drools Rules Engine (www.jboss.org/drools), which enables the properties and advantages mentioned.

Introduction to Drools

You must understand the fundamental characteristics of Drools to understand the rest of the manual. Drools has its own syntax for writing rules in a declarative, concise, and unambiguous format. A rule has the following structure:

```
when
conditions
then
actions
```

The *conditions* are edited according to certain rules of Drools syntax. According to this syntax, setting up a condition means verifying a deed.

The context in which the rules are applied is characterized by a group of deeds. All these deeds, which describe the present situation in which the RE operates, are asserted in a working memory.

To understand whether to apply a rule, the RE verifies whether a deed was effectively asserted in the working memory. If it has, then the rule is applied.

The *actions* area is edited in normal Java code and contains the actions to perform if the conditions are verified. The rules that are to be applied are contained in a production memory. The RE compares the actions that are hypothesized in the rules in the Production Memory with those deeds that are asserted in the working memory. If there is a compatibility, the RE executes one or more rules.

Note: The *conditions* wording that is normally adopted in the Drools documentation can be misleading.

This area is only declared when the rule is applied. The rule is applied only if the presupposed actions are effectively asserted in the working memory.

Conditions that determine the context-based effect of rules are normally set up in the *actions* area. These conditions can hypothesize on deeds present in the working memory.

The deeds asserted in the working memory represent the situation under examination. Architecturally, a deed can be the presence of an event, a user or both, in the working memory.

Elements of Drools syntax

You must understand the essential syntax notions. Setting up a condition according to Drools is equivalent to presupposing a deed. A deed is represented as an object in the working memory. If the object is found, the deed is asserted, and an action can be performed.

To presuppose the presence of an object, you must state it in the *conditions* area of the rule. If a user wants to verify the presence of a `UserBean`:

```
UserBean()
```

A variable that supports the potential object that is found can be declared as follows:

```
user : UserBean()
```

Thus, if a user bean is found, it is supported by the user variable. The variables that are declared as such, are local, that is, they have limited visibility to the Rule. Object searches can be filtered according to their attributes.

To verify the UserBean Name=James, write:

```
UserBean ( name == James )
```

This syntax is admitted only if a method exists to read the attribute **`getName()`**.

Starting from the attribute name, Drools can go back to the corresponding method and use it to extract the value of the object that is found. If the extracted value coincides with the presupposed value, Drools proceeds with the action. Attributes of the object that is found can be supported in local variables, which are stated in brackets:

```
UserBean ( username : name )
```

The name of the user that is found is supported in the local variable *username*. Lastly, the Drools function **`eval`**, which considers a Boolean expression that is written in Java language, is often used:

```
user : UserBean()
eval ( user.getName() == James )
```

Conditions can be written by using normal Java, if necessary.

Note: In the *conditions* area of the standard rules that is provided by the AG Core, only a group of beans are declared without using conditions on the bean attributes or the **`eval`** function.

All other types of conditions are set in the *actions* area with a normal `Java IF` construct. Each loaded rule, in the presence of the requested bean, is always applied. Programmers, however, are free to use their preferred strategy to set the conditions of the written rules.

The *actions* area is written in Java code. Programming in Java requires knowledge of all the classes necessary for implementing the actions.

In particular, the following two types of classes are used to write rules for IBM Security Identity Governance and Intelligence.

Beans Beans represent the objects that are managed by the AG Core.

Actions
Actions represent the actions that can be executed on these objects through the AG Core administration module.

For example, an instance of the `UserBean` class can represent a user.

This instance has attributes that contain data of the user that it represents. The possible actions on the users are represented in the methods of the `UserAction` class.

If a corresponding action class is not defined for an object, no actions are expected on that object. The `get` and `set` method types are responsible for reading and modifying attributes of the corresponding bean.

Each rule has objects that are available in the working memory only. The Action methods can be applied on these objects only.

IBM Security Identity Governance and Intelligence integration interface

As a centralized RBAC repository for IBM Security Identity Governance and Intelligence platform authorizations, the AG Core must be integrated with an organization's previous architecture. Typically, in such pre-existing architectures, the available repositories that contain users' personal information and authorizations are not well-formed RBAC repositories.

The AG Core thus interacts with the surrounding environment in various ways:

AG Core Administration Module
Through the administration module, all main aspects of an organization can be described and translated to the IBM Security Identity Governance and Intelligence data model.

Provisioning
The AG Core can interface with a provisioning module that integrates a component for authorization workflow management.

Batch A batch is group of procedures for bulk data loading and realignment.

External Repository
An external repository is a generic repository for data that must be kept aligned with data in the AG Core. By maintaining data alignment, the AG Core can propagate authorizations to other systems.

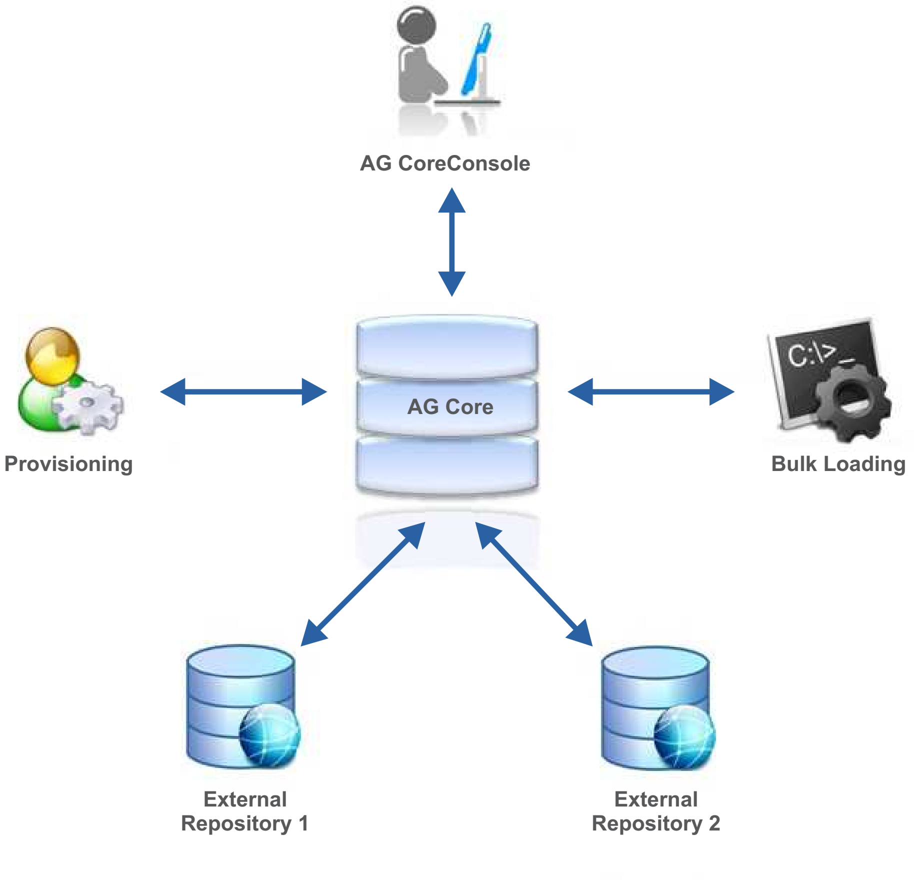


Figure 32. AG Core integration

The external repositories connect to the AG Core through a dedicated integration interface (II). Any number of external repositories can connect through this interface.

A flexible interface synchronizes and aligns the AG Core with the external repositories.

AG Core interacts with two types of repositories:

- Personal data repository
- Authorization repository

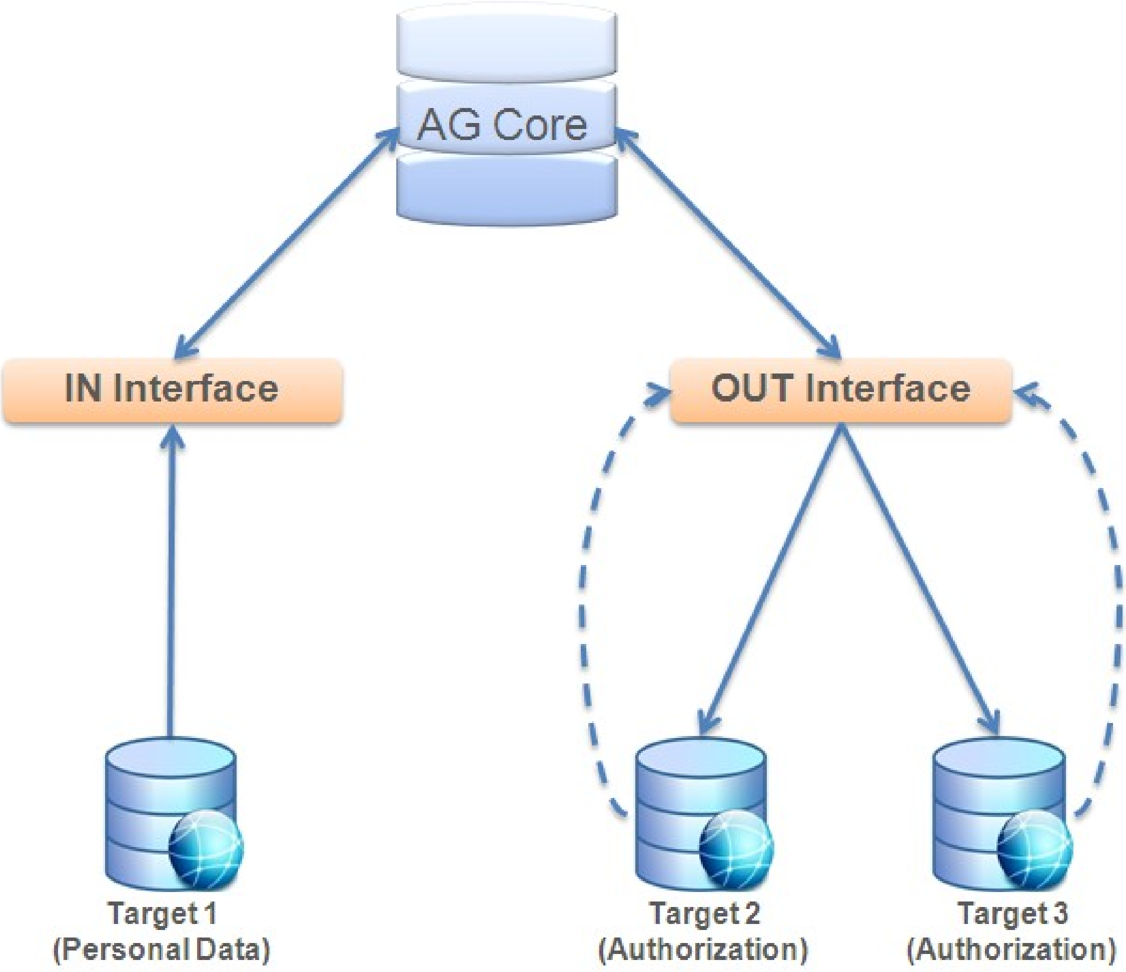


Figure 33. Types of external repositories

The basic framework has an input interface that passes information from personal data systems to the AG Core. Through the output interface, the AG Core transmits authorization information to the target systems. Any number of target systems can be connected to both the input and the output. The interface distinctly manages communication with each of them.

Brief introduction to events

The integration interface (II) syncohonizes and aligns the data in the AG Core database with the data in the target systems.

Events play a key role in synchronization management. An event is a brief yet complete description of interaction between any of the architecture's parts and any one of its elements.

Usually, the AG Core itself or the target systems generate events. Each time a system acts on the data, the executed changes are copied into appropriate packages, events, which are then sent to inform the other “listening” systems about the action.

Events are contained in appropriate event tables that are integral parts of the interface that is used to communicate with the target systems. The AG Core always communicates with the interface through events.

The target system that is connected through the input interface communicates each change that is made to its data. The interface then works to create an event with the required alignment information and transmits it to the AG Core.

The AG Core itself changes the data, creates the corresponding events, and transmits them to the output interface that is connected to the respective target systems.

For each event, a state attribute is always set and indicates the event's state within the connection flow.

An event can have one of the following states:

Unprocessed
The event is generated but data alignment is not yet executed.

Success
The data alignment was successful. An event in this state can automatically be eliminated or kept as a reminder of the modification.

Error The event was generated correctly but a data alignment error was detected.

Basic Structure of the Interface

The following topic provides more information about the structure of the IBM Security Identity Governance and Intelligence integration interface (II).

The following figure provides a more detailed illustration of the basic structure of the IBM Security Identity Governance II.

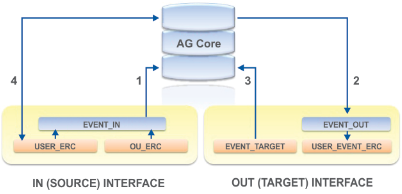


Figure 34. Layered structure of the integration interface

The II communicates with external systems through the USER_ERC and USER_EVENT_ERC tables.

The USER_ERC table contains a copy of user data from the external system.

The IBM Security Identity Governance enterprise connector module (ECONN)is the principle way of loading data into the USER_ERC table.

The USER_EVENT_ERC table contains information that is related to authorization changes registered in the AG Core, in the form of events. This table contains events that are ready for transmission to the target systems.

EVENT_IN and EVENT_OUT are event tables that are required for communication between the interface and the AG Core.

OU_ERC contains information that is related to OU changes.

AG Core and USER_ERC are involved in both directions for the following reasons:

- The AG Core calculates some attributes are writes them back to the table, making them available for targets;
- Some attributes are linked with the AG Core database PERSON table and are automatically synchronized in both directions. See flow 4.

The structure of the USER_ERC table can be highly customized to fit the needs of each client. Different targets use different fields, which are then carried back to the USER_ERC table.

It is fundamental to establish which attributes in the USER_ERC table are mapped to the AG Core table/attributes. See the following diagram.

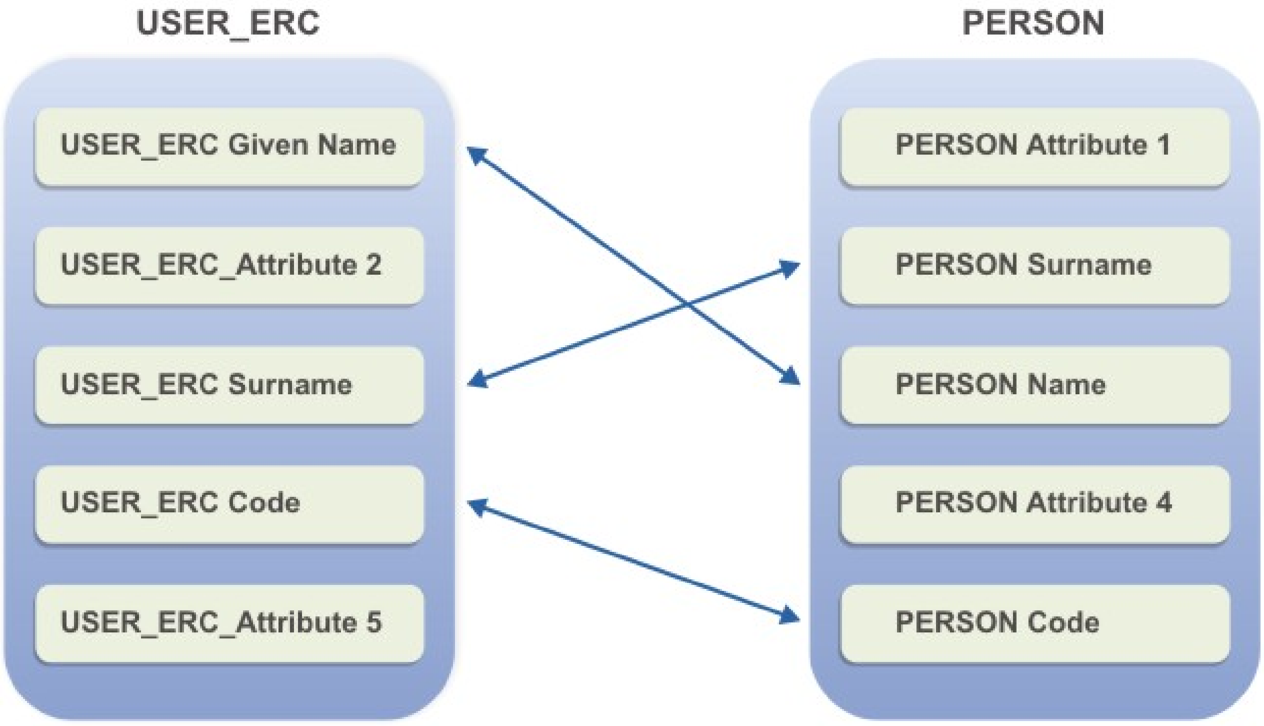


Figure 35. Virtualization of attributes in the PERSON table

In the diagram, attribute 1 **USER_ERC Given Name** of the USER_ERC is mapped to attribute 3 **PERSON Name** of the PERSON table that contains the user's personal data in the AG Core module.

When USER_ERC is modified by the external personal data system, the data that is contained in attribute 1 of USER_ERC is copied in attribute 3 of PERSON. The contrary is also true: changing **PERSON Name** automatically changes **USER_ERC Given Name** . See bidirectional flow 4.

However, it is possible to map other attributes of USER_ERC, outside of PERSON table, and visualize them as external data in the Data frame of the User Management GUI of AG Core.

For example, you can consider the **USER_ERC** table as repository involved into the virtual mapping.

Each attribute can be set in two different modes:

Mode 1

The **USER_ERC** attribute (listed under the column **Name**), is mapped with an attribute of **PERSON**. Changing the value of an attribute in one table causes the same change in the other table. To customize an attribute with Mode 1, insert the name of the **PERSON** attribute to be associated, preceded by an underscore ("_"), into the **Label** column.

Mode 2

The attribute in **USER_ERC** is only displayed among the users' external data, on the User Management page of the AG Core Console. To customize an attribute by using Mode 2, insert the attribute and assign it a name in the **Label** text-box. In this case, the change in **USER_ERC** is also reflected in the external table.

Examples of Rules

In the IBM Security Identity Governance and Intelligence platform, the rules engine provides the flexibility and expressive strength that is required to model the customization of company processes.

Rules can be used in different situations, which in IBM Security Identity Governance and Intelligence, represents a layer of intelligence that enhances the expressive nature of the data model. Rules are used to implement specific and dynamic behaviors.

The following example situations demonstrate how the AG Core is linked to the external repository by integrating specific rules with simple USER_ERC attribute mapping.

Example 1

In an external system that contains personal data, the **User Type** attribute is set for each user. It is defined by a grouping of codes that have a specific meaning in the system, for example `46=External Consultant`. Assume that there is one attribute with the same meaning, but that the types have different names, `External Consultant=Consultant`.

In this case, the simple mapping that is described in the previous paragraph does not work.

The problem can be resolved with a rule that implements the following simple logic:

```
if type=46 AG Type=Consultant
```

This rule must be applied automatically each time a mapping is executed.

Example 2

Assume that based on the value of each USER_ERC attribute, the value of the PERSON attribute can be calculated from either of the following methods:

NAME and SURNAME â **MAIL**=<*NAME*>.<*SURNAME*>@<*companyname*>.com

ID NUMBER â **USERID**=<*constant*><*ID NUMBER*>

Again, a rule can automatically implement the same logic. The use of a rule is not limited to mappings between USER_ERC and PERSON. It can also be applied in many general cases of communication between the AG Core and an external repository. See the following examples.

Example 3

A rule can be used to automatically create an account on the target system when a new user is inserted.

Example 4

Certain codes in the external system can indicate whether a user is on sick-leave, on holiday, or temporarily transferred. Based on these codes, a rule can be used to temporarily disable the user's account.

Example 5

As a function of **User Type**, **OU Type**, or **Reason for Transfer**, a rule can regulate which roles the user maintains when the user is transferred from one OU to another.

Example 6

By using a rule, you can ensure that a user has an account on the target system before you assign an entitlement to that user. If the user has no account, one can be created.

The rules engine (RE) in AG Core Architecture: read-from and write-to branches

Each time there is a new event to manage, the RE is activated and applies rules based on the type of event.

For more information about events, see “Brief introduction to events” on page 42.

The RE directly interfaces with the event tables. It periodically polls them and applies rules when it finds new events.

The RE filters event propagation and takes responsibility for any newly generated event. It analyzes the event changes and applies the appropriate rules according to company policies.

The following diagram illustrates the flow structure that enables communication between the target system that contains personal data and the AG Core:

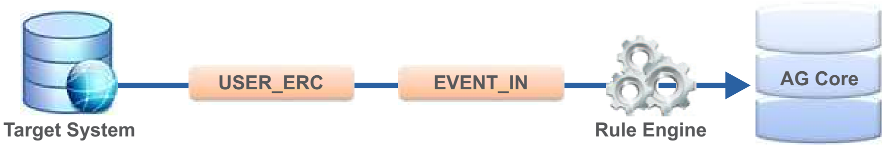


Figure 36. Read-from communication: flow 1

Each time the target system changes the **USER_ERC** table, an event that describes what occurred is automatically generated in the **EVENT_IN** table. The rules engine notices the presence of a new event in the **EVENT_IN** table and applies the rules necessary for proper AG Core data alignment.

The following diagram illustrates the flow structure that enables communication between the AG Core and the generic target system:

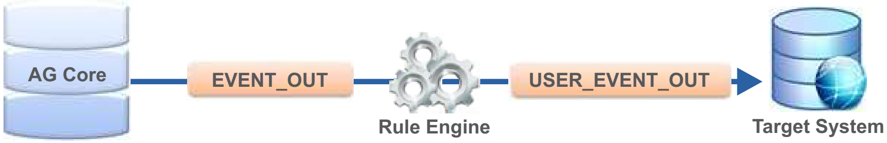


Figure 37. Write-to communication: flow 2

The AG Core changes the data and generates the necessary events to describe the change. The RE takes charge of the events and processes them. After the RE successfully processes the events, it passes them to the output interface, which then communicates the updates to the appropriate target systems.

Only correctly processed events are propagated to the output interface. If any errors are detected during event processing, propagation is blocked until the operator takes further action.

When an error is detected, an operator intervenes to remove the cause of the error and restarts event processing by using functions that are provided by the AG Core module.

Synchronization branch

The usual approach with target systems is to establish a master-subordinate mechanism between the target systems and the AG Core. The user authorizations are not set by single target system consoles. The AG Core communicates the user authorizations to the target system consoles.

When you migrate to an RBAC system managed by IBM Security Identity Governance and Intelligence, a transitional period in which operators continue to directly set and use the target systems is important.

However, synchronizing changes that are executed directly on the target systems is complicated because authorizations are managed through roles that use the RBAC standard.

In non-RBAC-based target systems, entitlements are directly assigned to users and are not mediated by RBAC standards.

The IBM Security Identity Governance and Intelligence framework contains a synchronization branch with an interface. The interface informs the AG Core about what occurred in the target systems, which avoids misalignment or inconsistencies.

Because of the rules that are implemented for this branch, the RE can automatically repair an error condition or send the event, which provokes an inconsistency.

After an error occurs, the administrator runs an analysis from a dedicated section of the AG Core module. In this case, from the AG Core, rules can be used to set a resolution strategy that assigns the functions to the users.

The following diagram illustrates the structure of the synchronization branch:

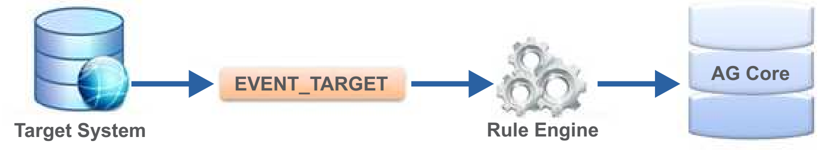


Figure 38. Synchronization branch

Complete Architecture of the IBM Security Identity Governance Integration Interface

The IBM Security Identity Governance and Intelligence architecture includes all branches that allow the AG Core module to interface with all types of external systems.

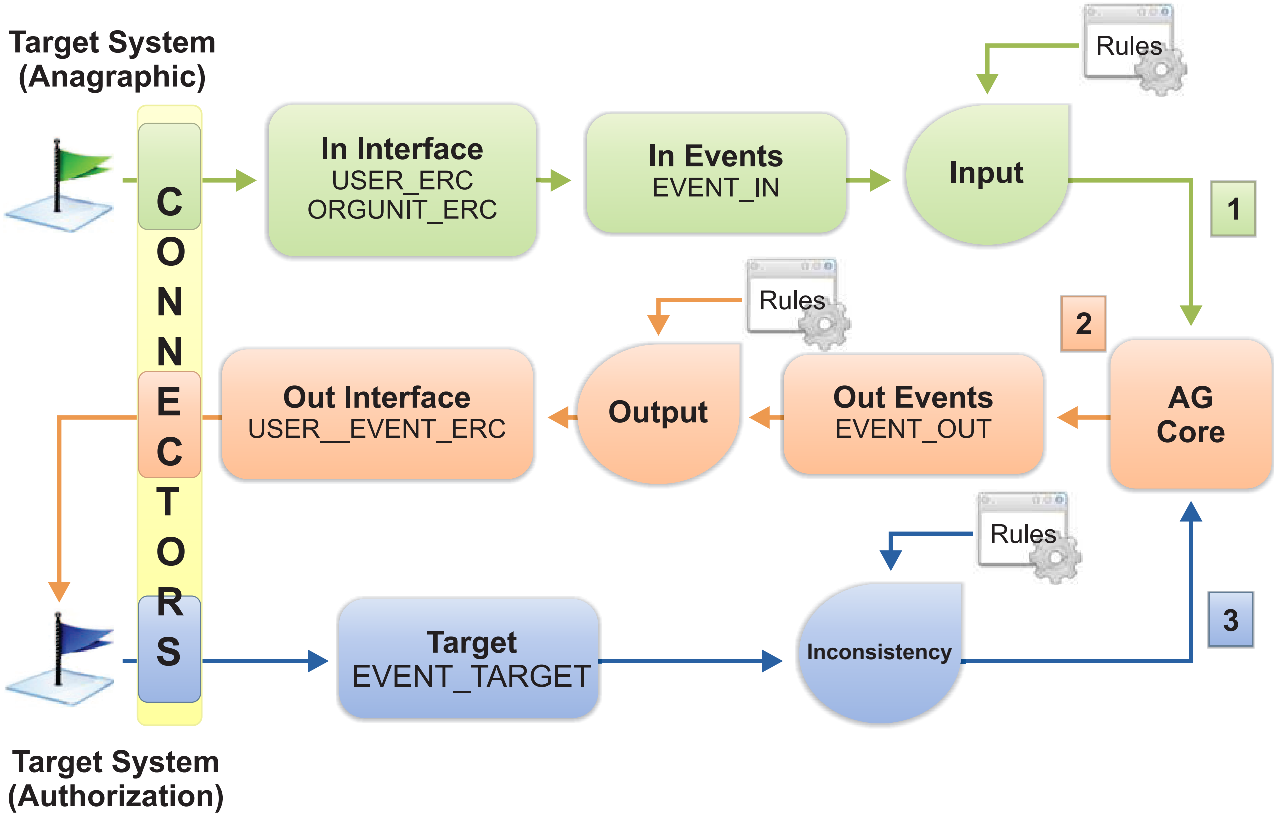


Figure 39. IBM Security Identity Governance and Intelligence II overview

The diagram displays the interface tables and three distinct flows:

- Read-from (flow 1)
- Write-to (flow 2)
- Synchronization (flow 3)

Events that are generated during propagation of information to the three branches are classified in the input events (EVENT_IN), output events (EVENT_OUT), and synchronization events (EVENT_TARGET). The table ORGUNIT_ERC contains a copy of the organization unit data that is registered in the personal data system. The function of this table is identical to that of USER_ERC.

Another important element that is shown in the figure is the ECONN module layer. Through all the previously outlined branches, this module is involved in communications and alignment between the AG Core centralized DB and the peripheral target systems.

However, the logical behavior of the II is not dependent on the presence of an ECONN layer.

The following list is a brief summary of the three branches:

Read-from
Each change that is made to data in the personal data target systems is copied to the `USER_ERC` for a user or `ORGUNIT_ERC` for an OU in the input interface. This action generates a new event in the input events table. The event contains the minimum information that is required to reconstruct what was modified. The input RE takes responsibility for the event. It applies the input rules and, if no processing problems occur, communicates the information to the AG Core, which can then be aligned.

Write-to
Each change that is made to data in the AG Core generates a new event in the output events table. The event contains the minimum information that is required to reconstruct what was modified. The output RE takes responsibility of the event. It applies the output rules. It communicates the information to the output interface if no processing problems occur. The output interface propagates the information to the target system, which can then be aligned.

Synchronization
Each change to the data in any of the authoritative target systems generates a new event in the `EVENT_TARGET` table. The event contains the minimum information that is required to reconstruct what was modified. The inconsistency RE takes responsibility for the event. It applies the inconsistency rules. If no processing problems occurs, it aligns the AG Core.

SAP GRC integration scheme

Identity Governance and Intelligence can interface a SAP GRC system, with a particular focus on External SoD features. The interaction can be managed through a ReST or a Java interface.

The basic common scheme of integration is shown below:

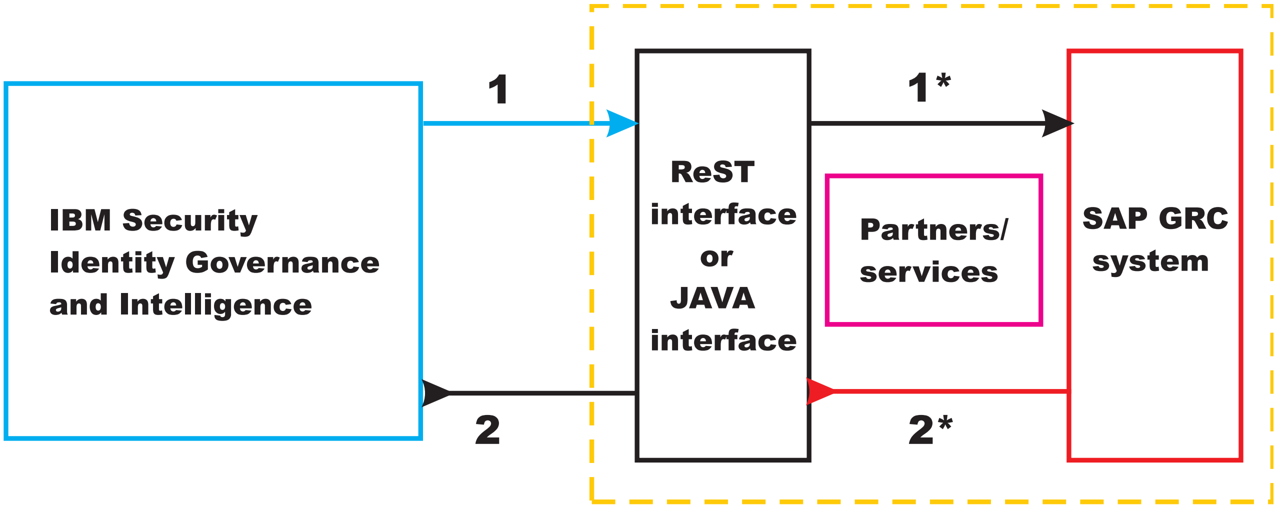


Figure 40. SAP GRC integration

- 1 - Start a request to the ReST/Java interface.
- 1* - The ReST/Java interface transforms the request in a consistent SAP GRC format.
- 2* - The SAP GRC system returns the requested data.
- 2 - The ReST/Java interface converts the data provided in step 2* to a consistent Identity Governance and Intelligence format.

ReST integration scheme

Identity Governance and Intelligence includes a ReST (Representational State Transfer) web service layer that can use HTTP to exchange data with an external target system.

The basic common scheme of integration is shown below:

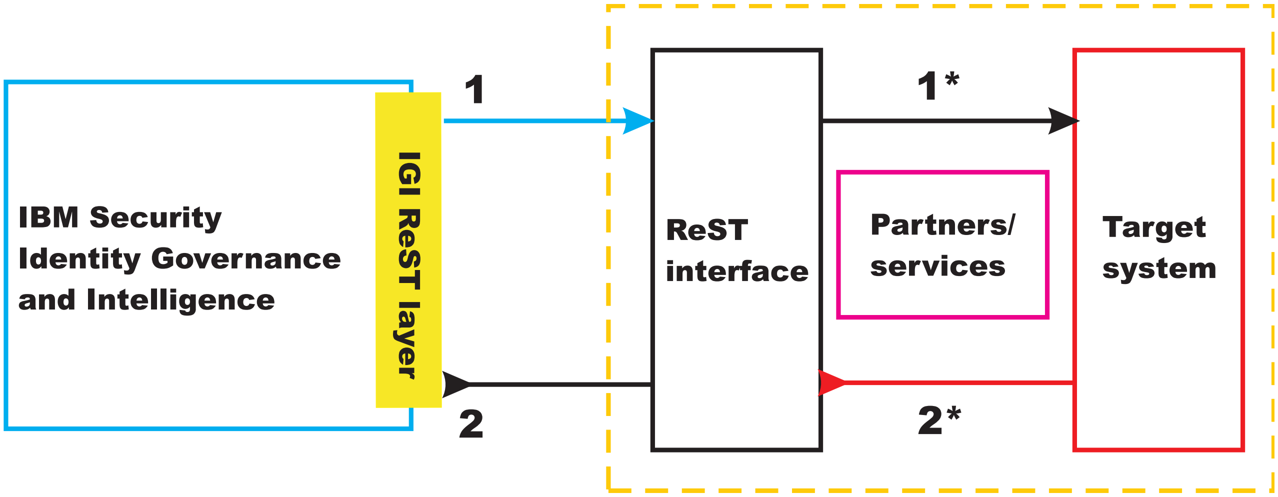


Figure 41. ReST integration

- 1 - A request is sent from the ReST layer of Identity Governance and Intelligence to the ReST interface of the target system.

- 1* - The ReST interface of the target system converts the request to a consistent target system format.
- 2* - The target system returns the requested data to the ReST interface.
- 2 - The ReST interface converts the data provided in step 2* to a consistent Identity Governance and Intelligence format.

Introduction to audit

IBM Security Identity Governance and Intelligence Audit is a centralized module. By default, it is always active.

All the IBM Security Identity Governance and Intelligence modules are required to send notifications to the Audit module for large sets of operations.

The following table shows a sample of an audit events table.

Table 2. Audit events table

Event ID	Description	Module
1	`LOGIN`	AG Core
2	`LOGIN WARNING`	AG Core
3	`LOGIN ERROR`	AG Core
4	`Sub module access`	AG Core
5	`Password change`	AG Core
6	`Delegation start`	AG Core
7	`Delegation end`	AG Core
8	`Disabled`	AG Core
11	`Resource to user added`	AG Core
12	`Resource to user removed`	AG Core
13	`Org unit to user - internal resource added`	AG Core
14	`Org unit to user - internal resource removed`	AG Core
15	`Application to user - internal resource added`	AG Core
16	`Application to user - internal resource added`	AG Core
17	Entitlement to user - internal resources added	AG Core
18	Entitlement to user - internal resources removed	AG Core
19	Activity to user - internal resources added	AG Core
20	Assigned role to user	AG Core
21	Removed role from User	AG Core
23	`User assigned to OU`	AG Core
23	`Move user to OU`	AG Core
24	`Profile assigned to role`	AG Core
26	`Role assigned to OU-single`	AG Core

Table 2. Audit events table (continued)

Event ID	Description	Module
27	Role removed from OU-single	AG Core
28	Role assigned to OU-hierarchy	AG Core
29	Role removed from OU-hierarchy	AG Core
30	IT role assigned to role	AG Core
31	IT role removed from role	AG Core
32	Profile assigned to role	AG Core
33	Removed profile from role	AG Core
40	New role	AG Core
41	Role removed	AG Core
42	Add user	AG Core
43	User removed	AG Core
44	User modified	AG Core
45	Add Org.Unit	AG Core
46	Org.Unit removed	AG Core
47	Add delegation to user	AG Core
48	Delegation removed	AG Core
49	Add account	AG Core
50	Account removed	AG Core
60	Add remediation to user	AG Core
61	Remove Remediation from user	AG Core
62	Risk added to user	AG Core
63	Risk removed from user	AG Core
64	Add remediation state to user	AG Core
65	Remove remediation status from user	AG Core
71	Core engine error	AG Core
72	Core engine alert	AG Core
80	Organization unit entitlement attestation approved	AG Core
81	Organization unit entitlement attestation revoked	AG Core
82	Organization unit entitlement attestation required	AG Core
85	User entitlement attestation approved	AG Core

Table 2. Audit events table (continued)

Event ID	Description	Module
86	User entitlement attestation revoked	AG Core
87	User entitlement attestation required	AG Core
90	User remediation attestation approved	AG Core
91	User remediation attestation revoked	AG Core
92	User remediation attestation required	AG Core
40000	Release to AGC	Access Optimizer (AO)
40001	Risk Based Campaign	Access Optimizer (AO)
50000	Insert activity	Process designer (PD)
50001	Update activity	Process designer (PD)
50002	Delete activity	Process designer (PD)
50003	Insert workflow	Process designer (PD)
50004	Update workflow	Process designer (PD)
50005	Delete workflow	Process designer (PD)
60000	Download report	Report designer (RD)
60001	Insert query	Report designer (RD)
60002	Update query	Report designer (RD)
60003	Delete query	Report designer (RD)
60004	Insert report	Report designer (RD)
60005	Update report	Report designer (RD)
60006	Delete report	Report designer (RD)
60007	Submit report	Report designer (RD)
70000	Adding permission to user	Enterprise connectors (ERC)
70001	Removing permission from user	Enterprise connectors (ERC)
70002	Suspending user	Enterprise connectors (ERC)
70003	Activating user	Enterprise connectors (ERC)
70004	Creating user account	Enterprise connectors (ERC)
70005	Deleting user account	Enterprise connectors (ERC)
70006	Renaming user	Enterprise connectors (ERC)
70007	Modifying user account	Enterprise connectors (ERC)
70008	Start reconciliation	Enterprise connectors (ERC)
70009	End reconciliation	Enterprise connectors (ERC)
80000	Start task	Task planner (TSKP)
80001	Stop task	Task planner (TSKP)
80002	Synchronize	Task planner (TSKP)
90000	Generate request	Access requests (AR)
90001	Authorize request	Access requests (AR)

Table 2. Audit events table (continued)

Event ID	Description	Module
90002	`Execute request`	Access requests (AR)
90003	`Execute request by rule`	Access requests (AR)
100000	`Save configurations`	Email service
100001	`Insert template`	Email service
100002	`Update template`	Email service
100003	`Delete template`	Email service
100004	`Submit email`	Email service

Chapter 3. Identity Governance and Intelligence modules

Every Identity Governance and Intelligence module has a set of common features.

General features

- For every module, a specific tab opens by default.
- There are **Help** and **Logout** options in the module frame.
- There is an IBM logo that you can mouse over to activate the Icons bar where you can directly access the other modules.

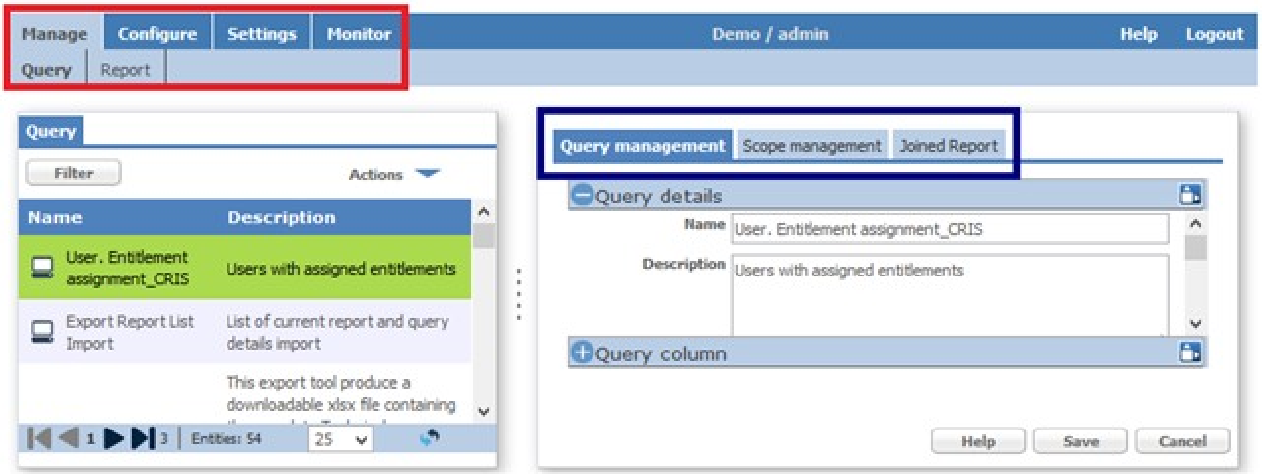
Tabs

In every module, you can always find two levels of tabs that are indicated in the red rectangle.

The action area tabs are in the first level of tabs. They indicate general actions you can perform on entities in the second level of tabs. The second level displays a set of specific working areas.

There might be a third level tab, which is known in a blue rectangle. It has one or more specific operations that belong to one of the second level tabs.

The following figure shows an example of the 3-levels tabs module:



Name	Description
User. Entitlement assignment_CRIS	Users with assigned entitlements
Export Report List Import	List of current report and query details import
	This export tool produce a downloadable xlsx file containing

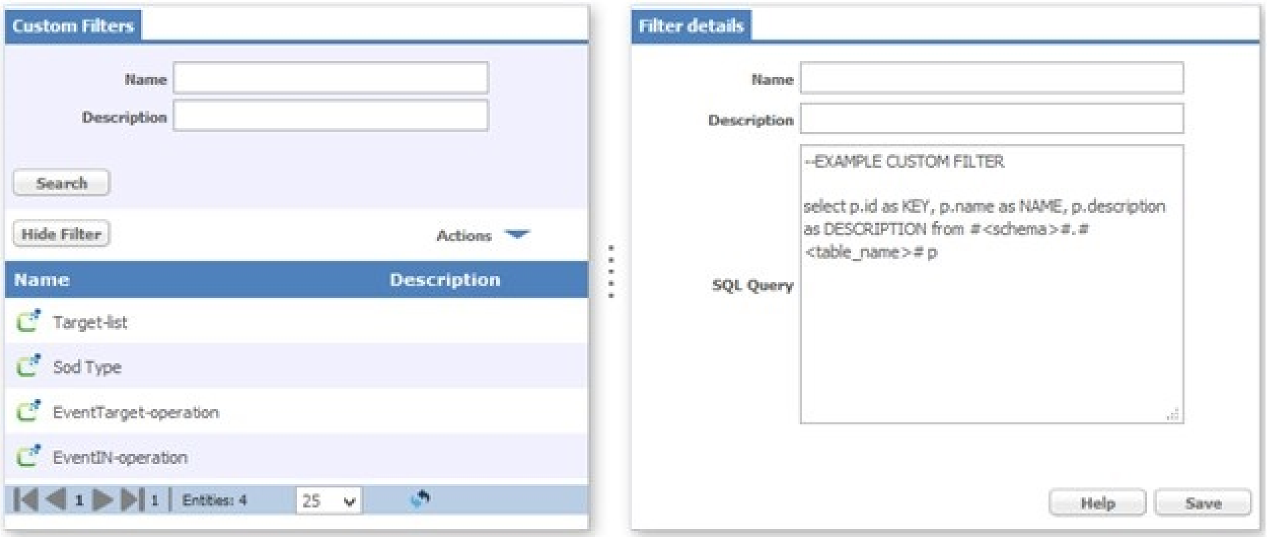
Name: User. Entitlement assignment_CRIS

Description: Users with assigned entitlements

Figure 42. Example of a generic Identity Governance and Intelligence module GUI with three levels of tabs

Frames

The standard GUI is organized in two frames.



Name	Description
Target-list	
Sod Type	
EventTarget-operation	
EventIN-operation	

1 1 Entities: 4 25

```
--EXAMPLE CUSTOM FILTER

select p.id as KEY, p.name as NAME, p.description
as DESCRIPTION from #<schema>#.#
<table_name># p
```

Figure 43. Example of a typical section of a generic Identity Governance and Intelligence module

On the left frame, you can find the following common elements.

Filter/Hide Filter
Show or hides the filters option.

In most cases, search filters correspond to a subset of the attributes of an item. The following wildcard characters modify the search criteria:

% Searches for any sequence of characters.

_ (underscore)
Indicates a single character.

Search
Gets results according to the filters setting.

Go to ⏮ ◀ ▶ ⏭
Navigates through the pages.

Pagination
Selects the number of items that are paged after the search operation, such as 10, 25, 50, 100, or 200.

Refresh ⟳
Refreshes the contents.

Actions
Contains functional buttons that perform operations such as **Add**, **Remove**, **Import**, **Export**, **Build**.

Note: Every Identity Governance and Intelligence module can have a different set of functional buttons in the actions menu.

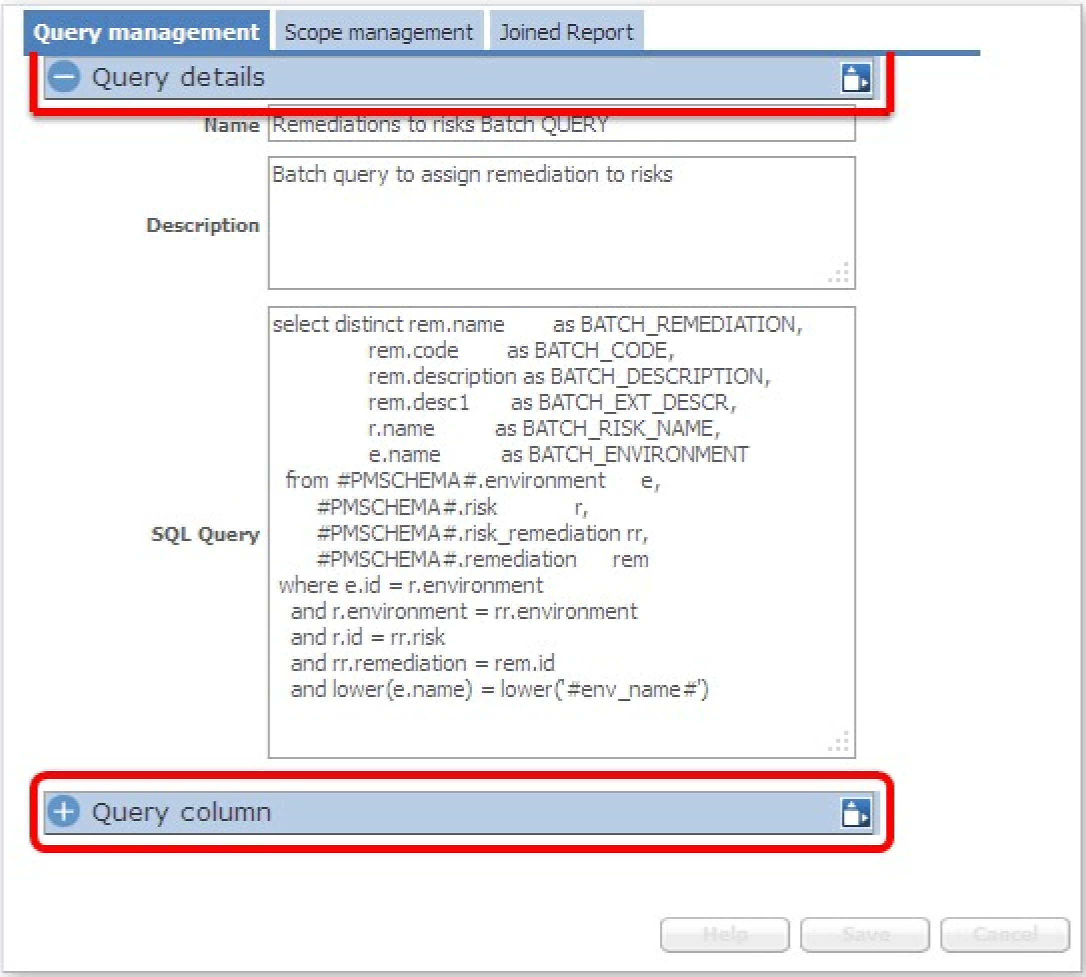
In the lists of items that are subdivided into one or more information columns, you can click any column heading to reorder the list items for that specific column. In these frames, you can also find one or more buttons to perform specific operations.

The right frame consists of dedicated sections to perform different kinds of operations. In these frames, it is common to find command buttons and accordion panes. Typical command buttons are of the following type:

Save Saves the performed operations.

Cancel
Deletes all the data that is entered in the different fields.

Different operative sections can be hosted into accordion panes. In the following example, you see the **Query management** section of the **Report Designer** module with two accordion panes.



Name: Remediations to risks Batch QUERY

Description: Batch query to assign remediation to risks

SQL Query:

```
select distinct rem.name        as BATCH_REMEDIATION,
                rem.code        as BATCH_CODE,
                rem.description as BATCH_DESCRIPTION,
                rem.desc1       as BATCH_EXT_DESCR,
                r.name          as BATCH_RISK_NAME,
                e.name          as BATCH_ENVIRONMENT
 from #PMSCHEMA#.environment     e,
      #PMSCHEMA#.risk            r,
      #PMSCHEMA#.risk_remediation rr,
      #PMSCHEMA#.remediation     rem
where e.id = r.environment
  and r.environment = rr.environment
  and r.id = rr.risk
  and rr.remediation = rem.id
  and lower(e.name) = lower('#env_name#')
```

Figure 44. Example of accordion panes

To open or close the panes, click anywhere on the pane bar title. Click the **Maximize** /**Minimize** buttons to maximize or minimize the pane.

Buttons & Icons

The following table lists the most common icons and buttons in Identity Governance and Intelligence modules.

Table 3. Common buttons and icons

Button / Icon	Description
❏	Represents a product type of item in the Report Designer module.
🖥	Represents a custom type of item in the Report Designer module.
⊗	Clears the contents that are inserted in a text box.
⋯	Searches for specific entity or item.
⇧ / ⇩	Moves an item up or down.
🔄	Refreshes the page.
⊕ / ⊖	Opens or closes accordion panes.
ⓘ	Displays the details of an item.
📂	Indicates an item in a hierarchy.
📂	Indicates the error status of an item.
📂	Indicates the completed status of an item.
✓ / ✗ / !	Represents the status of a request • Complete • Error • Warning
⤢ / ⤡	Maximizes or minimizes the frame.
⚛	Represents the Permission type of entitlement.
⊶	Represents the IT Role type of entitlement.
🧬	Represents the Business Role type of entitlement.
🖧	Represents the organization unit.
👤	Represents the UME entity.
👤	Represents the user entity.
⚠	Represents a generic risk.
⚠	Represents a Segregation of Duties risk
🔴 / 🔵 / 🟠	Represents the Segregation of Duties level. • High • Low • Medium

Any Identity Governance and Intelligence module can be customized to use a subset of specific icons.

Chapter 4. Account administration

Identity Governance and Intelligence administrators use the Administration Console to do account administration tasks, such as adding accounts.

Related concepts:

Chapter 7, "Attribute-to-permission mapping service," on page 69
Administrators can map account attributes from a target system to permissions in Identity Governance and Intelligence. Administrators can also map allowed values for attributes to rights values, so that you can set a business-friendly name for the rights value.

Related information:

"Accounts" on page 225
Describes how to customize an account configuration for an application.

Adding an account

Complete this task to register a new account into the Identity Governance and Intelligence data model.

About this task

An account in the Identity Governance and Intelligence data model is a grouping of applications. All policies that are associated with the account are applied to the related applications.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select **Actions** > **Add**.
5. In the **Details** tab, define a basic Account profile. See the related help topic for the options and their descriptions.

   Name Specify a name for the Account.

   Fulfillment
   Set the value to **Automatic**.
6. Click **Save**. The new account is automatically listed and selected in the **Account Configuration** pane.
7. Access the **Password Creation** tab and select the **Enable Password Construction** check box.
8. Click **Save**.
9. In the Information window, click **Ok**.

Related information:

"Accounts" on page 225
Describes how to customize an account configuration for an application.

Discovering attributes from an imported account

Complete this task to discover attributes incoming from an account that is imported through Target Administration Console and associate these attributes to all the users associated to the account in the Access Governance Core module.

About this task

You can select a subset of attributes that are related to an account.

This task provides steps for discovering the attributes of an account, select the right subset of attributes and associate it to all users that are associated to the account.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select an account.
5. In the **Account Attributes** pane, select **Action** > **Discover from target**. The Discover Attributes from Target page is displayed.
6. Select the attributes that you want to import from an account, and then click **Import**. The attributes are added to the list shown in **Account Attributes** pane.
7. If you want to show the attribute in all context where it can be shown, select the check-box `Visible`.
8. Click ... `Attribute Localization`, for opening the Attribute Localization window, where you can localize the attribute in nine languages.
9. Select the right option from the combo-box `UI Rendering`, for setting the right type of data associated to the selected attribute.
10. Click **Action** > **Save**. The settings that are made in previous steps are confirmed.

What to do next

The set of attributes can be updated in any time. If you want to remove an attribute, select it, thus select **Account Attributes** > **Action** > **Remove**.

"Account attributes" on page 234
Access Governance Core supports different policies for managing the account attributes. You can choose a free subset of attributes of a specific account. This subset is associated to users information for all users that are linked to the account.

"Discovering attributes from a target system" on page 75
Complete this task to discover attributes from a target system, import the attribute names, and map them to permissions in the Access Governance Core module.

Managing attributes related to a standard account

Complete this task to manage attributes that are related to standard account (not imported through Target Administration Console) and associate these attributes to all the users associated to the account in the Access Governance Core module.

About this task

You can select a subset of attributes that are related to a standard account set through the **Account Configuration** > **Action** > **Add** operation.

This task provides steps for managing the attributes of an account, select the right subset of attributes and associate it to all users that are associated to the account.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select an account.
5. In the **Account Attributes** pane, select **Action** > **Add**. The Add a new custom attribute key pane is displayed.
6. Set the `Name` of the new attribute.
7. If you want to show the attribute in all context where it can be shown, select the check-box `Visible`.
8. Select the right option from the combo-box `UI Rendering`, for setting the right type of data associated to the selected attribute.
9. Click **Ok**. The settings that are made in previous steps are confirmed.
10. In the **Account Attributes** pane, click ⋯ `Attribute Localization`, for opening the Attribute Localization window, where you can localize the attribute in nine languages.
11. Click **Action** > **Save**. The settings that are made in previous steps are confirmed.

What to do next

The set of attributes can be updated in any time. If you want to remove an attribute, select it, thus select **Account Attributes** > **Action** > **Remove**.

Related information:

"Account attributes" on page 234
Access Governance Core supports different policies for managing the account attributes. You can choose a free subset of attributes of a specific account. This subset is associated to users information for all users that are linked to the account.

Importing account attributes

Along with the manual procedure for defining the attributes of an account, you can use other methods to import and modify them in bulk.

Identity Governance and Intelligence provides two standard ways to import attributes for accounts.

- Bulk load procedures that are available in **Access Governance Core** > **Tools** > **Bulk Data Load**

  Insert Account Attributes

  Inserts and updates attribute keys of given account configurations. Run this procedure to add or modify attributes to any account configuration other than the Ideas account.

Insert User Account Attributes

Inserts and updates details and attribute values of user accounts. Run this procedure to add or modify the access details of users to account configurations, including account attribute values. This procedure does not apply to the Ideas account and to accounts that are imported with the Target Administration module.

Bulk load procedures are also available for removing account attributes and user account attributes.

- A custom rule that must be written with the objective of retrieving account attributes from external targets to add them into Identity Governance and Intelligence. The rule must be added in the ACCOUNT_CREATE and ACCOUNT_MODIFY rule flows.

Important: Accounts that are on external targets, which are accessed with the Target Administration module, are excluded from this option, since they are imported by the Identity Brokerage Adapters.

To accomplish the task of importing the account attributes, the rule must satisfy the following conditions:

1. The rule must include in the `when` section a variable whose value is the `AccountAttrValueList` bean, as the following example shows:

```
when
        event:EventTargetBean()
        account:AccountBean()
        attributes:AccountAttrValueList()
then
```

   where the variable is optionally named `attributes`.
2. `AccountAttrValueList` must contain the keys or names and the values of the account attributes that you want to import.

The rest of the rule structure is optional and is determined by your requirements.

Chapter 5. Activities and processes

Identity Governance and Intelligence administrators use Process Designer in the Administration Console to define and manage activities and processes. The processes generate requests and activities in the Service Center.

Use the Administration Console to do these tasks:

Table 4. Designing activities and processes

Task	Refer to
Enabling authorization requests to be redirected to other approvers	"Enabling authorization requests to be redirected to other approvers"

Enabling authorization requests to be redirected to other approvers

At times, the user with the role that is assigned to authorize a request might not be in the condition of handling the request. Reasons might include time constraints or other factors that preclude the capability of accepting or rejecting the request.

About this task

In such cases, the assignee can redirect the authorization step to other users who are appointed with the Redirection Approver role. These users are also specified in the authorization activity that underlies that type of authorization requests.

To provide your managers with the capability of redirecting an authorization request to another empowered person, use the Administration Console to do these tasks:

- Assign the Redirection Approver administrative role to selected users in Access Governance Core.
- Select classes of users in the **Redirect Scope** tab in the Activity pane of the authoritative step of a WorkFlow process in Process Designer.

Procedure

1. Assign the Redirection Approver administrative role to selected users.
   a. In Access Governance Core, select **Configure** > **Admin Roles**.
   b. Scroll the list of administrative roles, or use **Filter**, to find and select **Redirection Approver**.
   c. With **Redirection Approver** selected, click **Users** on top of the right pane. If users are already empowered to this role, they are listed in this pane.
   d. Select **Actions** > **Add** to assign the role to an extra user. The Add Users window displays the list of users that are defined in the organization.
   e. Scroll the list, or use **Filter**, to find and select the user. Click **Ok**. The Date Selection window is displayed.
   f. Click the calendar icons to select a time period for the validity of the assignment of the role to this user. Click **Ok** to confirm. The user is added to the list of assignees of this role.
   g. Repeat the steps for as many users as you need.

2. Select classes of users in the **Redirect Scope** tab of an authorization activity of a WorkFlow process in Process Designer. You encounter the **Redirect Scope** tab in one of the following situations.
   - When you define a WorkFlow activity in Authorization mode, starting from **Manage** > **Activity** > **Actions** > **Add**.
   - When you create or update a WorkFlow process, starting from **Manage** > **Process**. As you configure the Authorization step of the process, you either create or update the settings of the corresponding activity with the **Create** or **Details** option. See Defining and configuring a process for details on configuring a process.

     Alternatively, you can click the block of the Authorization step of a configured WorkFlow process to view the activity details.

   a. Select the **Redirect Scope** tab in the activity details pane. The **User Set** section of this tab shows the following classes of users to whom the authorization requests that are based on the process can be redirected:

Table 5. Classes of users to whom the authorization can be redirected by the user with the assigned role

Users for redirection	Description
All Users	All the users in the organization
Actor	Only the user with the assigned role - the logged in user. This selection is the default. It is equivalent to excluding the option to redirect the request, since the user who is assigned with the task redirects it to itself.
All Users belonging to an OU	All the users who are associated with a selected OU
All Users belonging to an OU (including hierarchy)	All the users of a selected OU and the entire subtree. Thus, all the users associated with the hierarchy.
All Users belonging to logged OU	All the users of all the OUs that are visible to the user with the assigned role
All Users belonging to logged OU (including hierarchy)	All the users of all the OUs that are visible to the user with the assigned role. Thus, all the users associated with the hierarchy.
All Users belonging to logged Hierarchy	The users of all the groups of a specific hierarchy that are visible to the user with the assigned role

   b. Select a class of users. Within the class of users that you select, the users to whom the requests can be redirected are the ones who are also assigned with the Redirection Approver role.

Results

The user in Service Center who is in charge of accepting or rejecting the request can also choose to redirect it to another authorized user. It can select **Redirect** at the bottom of the subrequest pane to display a window, where it can pick from a list of candidate users. The user to whom the request is transferred, can in turn accept, reject, or return the request without acting on it.

Chapter 6. Application administration

Identity Governance and Intelligence administrators use the Administration Console to do application administration tasks, such as adding applications.

Application administration tasks

Use the Administration Console to do these tasks:

Table 6. Application administration tasks

Task	Refer to
Add an application to the system	"Adding an application"

Related information:

"Accounts" on page 225
Describes how to customize an account configuration for an application.

Adding an application

Complete this task to register a new application. By default, a new application is joined to the default *System Account IDEAS* and the related *Events Marker IDEAS*.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Applications**.
4. In the **Applications** tab, click **Actions** > **Add**.
5. In the **Details** tab, define a basic Application profile. See the related help topic for the options and their descriptions.
6. Optional: If you want to create a new event marker with the same name of the application, select **<NEW>** from the **Events Marker** combination box. Otherwise, select the event marker that you want to use.
7. Click **Save**.

Related information:

"Applications" on page 209
Documents the functions required for the management of Applications.

Chapter 7. Attribute-to-permission mapping service

Administrators can map account attributes from a target system to permissions in Identity Governance and Intelligence. Administrators can also map allowed values for attributes to rights values, so that you can set a business-friendly name for the rights value.

An attribute-based permission is a specific type of permission that is used for mapping a user attribute that comes from a target system. For details, see "Permissions based on user attributes" on page 16.

Mapping method	When to use	For more information
Import attributes with the bulk load tool	A bulk load operation is useful when you need to import large amounts of data to import into Identity Governance and Intelligence. You can use a bulk load operation when you have several targets of the same type and want to map the same attributes on each target. A bulk load can load attributes and all the other settings from a target. You can also use a bulk load operation when you need to map attributes of a target that is not integrated with Identity Governance and Intelligence.	"Importing an attribute-to-permission mapping with a bulk load operation" on page 70
Discover attributes from a target system	This option is useful when you are using a target that is integrated with Identity Governance and Intelligence through Identity Brokerage or IBM Security Identity Manager. The process of discovering attributes from a target imports the attributes from the target, but it does not import other settings like a bulk load operation does.	"Discovering attributes from a target system" on page 75
Add attributes individually	This option is useful when you are configuring applications through the user interface for a small number if attributes. It is also useful when you are adding new attributes to an established application configuration.	"Adding an attribute-to-permission mapping manually" on page 72

Prerequisites for importing attributes and mapping them to permissions

Table 7. Prerequisites for importing attributes and mapping them to permissions

Prerequisite procedure	For more information
For HR feed profiles, configure the rule for the unique user ID	"Configuring the rule for the unique user ID" on page 133
Import a target type (adapter profile)	Chapter 17, "Target type administration," on page 131
Create a target instance	Chapter 18, "Target administration," on page 143
Reconcile the data	Chapter 14, "Reconciliation management," on page 117

Attribute names must be unique. When the attributes are imported into Identity Governance and Intelligence, the names are normalized. Therefore, attribute names are not case sensitive.

Editing, enabling, and removing the mapping

When you add an attribute mapping, you can edit it until the time that you enable it. If you want to update the permission name after you enable a mapping, you must remove it and then create it again. Because removing the attribute mapping also removes the permission, ensure that no users have entitlements before you remove the permission. There's not a way to find which users have the entitlements. You can view the list of users for that permission. Remove all the users from that permission, and then you can delete the permission.

Related concepts:

"Permissions based on user attributes" on page 16
An attribute permission is a specific type of permission that is used for mapping a user attribute that is imported from a target system. For harmonizing this feature with the role-based access control standard of the Identity Governance and Intelligence data model, you can use permissions and rights.

Related information:

"Attribute-to-Permission Mapping" on page 233
Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and Intelligence that is based on the attribute settings on the target systems.

"Insert Attribute-to-Permission Mapping Track" on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

"Application Access" on page 211
Documents how to manage application permissions.

Importing an attribute-to-permission mapping with a bulk load operation

Complete this task to import an attribute-to-permission mapping by using a bulk load operation.

Before you begin

A target profile must be imported, and a target instance must be defined. For more information, see the following topics:

- Chapter 17, “Target type administration,” on page 131
- Chapter 18, “Target administration,” on page 143

About this task

A bulk load operation is useful when you need to import large amounts of data to import into Identity Governance and Intelligence. You can use a bulk load operation when you have several targets of the same type and want to map the same attributes on each target. A bulk load can load not only attributes, but it can load all the other settings from the target.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Tools** > **Bulk Data Load**.
4. In the **Action** tab, select **Insert Attribute-to-Permission Mapping**.
5. In the **File Batch** tab, click the **Download** icon to download a template in the form of an Excel XLS spreadsheet file.
6. Open the spreadsheet template into your spreadsheet application, such as Excel.
7. In the spreadsheet template, complete the columns and rows according to your data specifications, and then save your spreadsheet. For a description of how to complete the columns, see “Insert Attribute-to-Permission Mapping Track” on page 288.
8. In the **File Batch** tab, click **Browse** to locate and upload your Excel XLS file that contains the attribute-to-permission mapping definitions.

   Note: The status of the operation, *Pending* to *Completed* is displayed at the bottom of the tab.
9. In the Information window, click **Ok**.

What to do next

After the mappings are successfully imported, you can modify the mappings, if necessary. Then, you must enable the mappings before they can be used in Identity Governance and Intelligence. For more information, see the following topics:

- “Editing an attribute-to-permission mapping” on page 78
- “Enabling an attribute-to-permission mapping” on page 81
- “Attribute-to-Permission Mapping” on page 233

Related tasks:

“Adding an attribute-to-permission mapping manually” on page 72
Complete this task to individually map attributes from a target system to permissions in the Access Governance Core module.

Related information:

“Insert Attribute-to-Permission Mapping Track” on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Bulk Data Load in the Access Governance Core module
You can load bulk data in the AG Core database.

Adding an attribute-to-permission mapping manually

Complete this task to individually map attributes from a target system to permissions in the Access Governance Core module.

Before you begin

A target profile must be imported, and a target instance must be defined. For more information, see the following topics:

- Chapter 17, “Target type administration,” on page 131
- Chapter 18, “Target administration,” on page 143

About this task

You can map attributes to permissions either manually or by discovering the attributes from the target system. This task provides steps for mapping the attributes from a target system to the permissions in the Identity Governance and Intelligence data model.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select an account.
5. Optional: In the **Attribute-to-Permission Mapping** tab, click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.
6. In the **Attribute-to-Permission Mapping** tab, select **Action** > **Add**. The Add Attribute Mapping page is displayed.
7. On the Add Attribute Mapping page, complete these fields:

   Attribute name
   Type the attribute name from the target system.

   Permission name
   Type the permission name from Identity Governance and Intelligence.

   Type Select either `boolean` or `string`. Depending on which type that you select, you need to complete different fields.

Option	Description
For `boolean` attribute types, complete these additional fields	**Required** This field is always selected for boolean attribute types. **Multi-value** This field is never selected for boolean attribute types. **Value if user has this permission** Provide a value for when the user has this permission. For example, `yes`. **Value if user does not have this permission** Provide a value for when the user has this permission. For example, `no`.

Option	Description
For `string` attribute types, complete these additional fields to map attribute values to rights values	**Required** Select this field to specify that the attribute is required. If an attribute is required on the target system, it must also be required in Identity Governance and Intelligence. **Multi-value** Select this field to specify that the attribute has multiple values. Deselect this field to specify that the attribute has a single value. If this attribute is not multi-value on the target system, then it cannot be multi-value in Identity Governance and Intelligence. **Attribute Value** Provide the name of the attribute value from the target system. **Rights Value** Provide the name of the rights value from the Identity Governance and Intelligence data model. **Active** Select this check box if the value is active. More than one value can be active. **Default** Select this option to specify the default value. Only one value can be the default. If this attribute is required, a default value must be selected. Inactive values cannot be specified as the default. To remove a value from this attribute, click the trash icon that is next to the value. Removing a value might cause errors if any users have a permission with this value. To add more values to this attribute, click **Add Value**.

8. Click **Save**. The mapping for the attribute and permission is updated in the table on the Attribute-to-Permission Mapping tab.

Related information:

"Attribute-to-Permission Mapping" on page 233
Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and Intelligence that is based on the attribute settings on the target systems.

"Insert Attribute-to-Permission Mapping Track" on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Discovering attributes from a target system

Complete this task to discover attributes from a target system, import the attribute names, and map them to permissions in the Access Governance Core module.

Before you begin

This task applies to any schema that is integrated with Identity Governance and Intelligence. The schema is registered when the target is created, whether the target is external or whether it is created by importing a profile with the Target Administration Console.

For more information, see the following topics:
- Chapter 17, “Target type administration,” on page 131
- Chapter 18, “Target administration,” on page 143
- Chapter 19, “Target management using Enterprise Connectors,” on page 157
- Integration with IBM Security Identity Manager

About this task

You can map attributes to permissions either individually or by importing the attributes from the target system. This task provides steps for discovering the attributes from a target system, importing them, and then mapping them to the permissions in the Identity Governance and Intelligence data model.

Note: Attribute values are not discovered and imported from the target. You must manually map each attribute value to a corresponding rights value.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select an account.
5. Optional: In the **Attribute-to-Permission Mapping** tab, click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.
6. In the **Attribute-to-Permission Mapping** tab, select **Actions** > **Discover account attributes from target**. The Discover Attributes from Target page is displayed.
7. On the Discover Attributes from Target page, select the attributes that you want to import from the target system, and then click **Import**. The attributes are added to the table on the Attribute-to-Permission Mapping tab. Initially, the permission name and the attribute name are the same for each imported attribute.
8. To configure the mapping for each attribute, select the attribute and then select **Actions** > **Edit**. The Edit Attribute Mapping page is displayed.
9. On the Edit Attribute Mapping page, complete these fields:

   Attribute name
   This field is read-only. It shows the attribute name from the target system.

Permission name

Type the permission name that you want for Identity Governance and Intelligence.

Depending on the type of attribute, whether `boolean` or `string`, you need to complete different fields.

Option	Description
For `boolean` attribute types, complete these additional fields	**Required** This field is always selected for boolean attribute types. **Multi-value** This field is never selected for boolean attribute types. **Value if user has this permission** Provide a value for when the user has this permission. For example, `yes`. **Value if user does not have this permission** Provide a value for when the user has this permission. For example, `no`.

Option	Description
For `string` attribute types, complete these additional fields to map attribute values to rights values	**Required** Select this field to specify that the attribute is required. If an attribute is required on the target system, it must also be required in Identity Governance and Intelligence. **Multi-value** Select this field to specify that the attribute has multiple values. Clear this field to specify that the attribute has a single value. If this attribute is not multi-value on the target system, then it cannot be multi-value in Identity Governance and Intelligence. **Attribute Value** Provide the name of the attribute value from the target system. **Rights Value** Provide the name of the rights value from the Identity Governance and Intelligence data model. **Active** If the value is active, select this check box. More than one value can be active. **Default** Select this option to specify the default attribute value. Only one value can be the default. If this attribute is required, a default value must be selected. Inactive values cannot be specified as the default. To remove a value from this attribute, click the trash icon that is next to the value. If any users have a permission with this value, removing a value might cause errors. To add more values to this attribute, click **Add Value**.

10. Click **Save**. The mapping for the attribute and permission is added to the table on the Attribute-to-Permission Mapping tab.

What to do next

On subsequent discoveries from the same target system, the attributes that are already mapped are displayed in read-only mode on the Discover Attributes from Target page. If you want to remove mappings, go to the Attribute-to-Permission Mapping tab and select **Actions** > **Remove**.

Related tasks:

"Discovering attributes from an imported account" on page 62
Complete this task to discover attributes incoming from an account that is imported through Target Administration Console and associate these attributes to

all the users associated to the account in the Access Governance Core module.

Related information:

"Attribute-to-Permission Mapping" on page 233
Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and Intelligence that is based on the attribute settings on the target systems.

"Insert Attribute-to-Permission Mapping Track" on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Editing an attribute-to-permission mapping

Complete this task to individually edit the attribute-to-permission mapping in the Access Governance Core module.

Before you begin

A target profile must be imported, and a target instance must be defined. For more information, see the following topics:

- Chapter 17, "Target type administration," on page 131
- Chapter 18, "Target administration," on page 143

Attribute-to-permission mappings must already be created, either by importing the mappings by using a bulk load operation, discovering attributes from a target system, or adding attributes manually. For more information, see the following topics:

- "Importing an attribute-to-permission mapping with a bulk load operation" on page 70
- "Discovering attributes from a target system" on page 75
- "Adding an attribute-to-permission mapping manually" on page 72

About this task

You can edit the attribute-to-permission mapping that you added manually or that you imported from the target system, either by discovery or by a bulk load operation.

If a mapping is	You can edit these fields	You cannot edit these fields
Boolean but *not enabled*	• **Permission name** • **Required** • **Multi-value** • **Value if user has this permission** • **Value if user does not have this permission**	• **Attribute name** • **Type**

If a mapping is	You can edit these fields	You cannot edit these fields
String but *not enabled*	- **Permission name** - **Required** - **Multi-value** - **Attribute value** - **Rights value** - **Active** - **Default**	- **Attribute name** - **Type**
Boolean and enabled	None	All
String and enabled	- **Active**: Indicates whether the value is active - **Default**: Indicates whether the value is the default You can add and remove values, but you cannot modify the existing values.	- **Attribute name** - **Permission name** - **Type** - **Required** - **Multi-value** - **Attribute value** - **Rights value**

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select an account.
5. Optional: In the **Attribute-to-Permission Mapping** tab, click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.
6. In the **Attribute-to-Permission Mapping** tab, select an attribute mapping, and then select **Action** > **Edit**. The Edit Attribute Mapping page is displayed.

   Note: After a boolean mapping is enabled, you cannot edit any fields or values. After a string attribute is enabled, you can add or remove values, and you can modify only the **Active** and **Default** fields.
7. On the Edit Attribute Mapping page, you can modify these fields if the mapping is *not enabled*:

   Permission name
   Type the permission name from Identity Governance and Intelligence.

   Required
   Select this option to indicate that the attribute is required. When an attribute is required, a default must be specified. When an attribute is not required, a default can be specified or not.

   Multi-value
   Select this option to indicate that the attribute is multi-value.

Option	Description
For boolean attribute types, complete these additional fields	**Value if user has this permission** Provide a value for when the user has this permission. For example, yes. **Value if user does not have this permission** Provide a value for when the user does not have this permission. For example, no.
For string attribute types, complete these additional fields to map attribute values to rights values	**Attribute Value** Provide the name of the attribute value from the target system. **Rights Value** Provide the name of the rights value from the Identity Governance and Intelligence data model. **Active** Select this check box if the value is active. More than one value can be active. **Default** Select this option to specify the default value. Only one value can be the default. If this attribute is required, a default value must be selected. Inactive values cannot be specified as the default. To remove a value from this attribute, click the trash icon that is next to the value. Removing a value might cause errors if any users have a permission with this value. To add more values to this attribute, click **Add Value**.

8. Click **Save**. The mapping for the attribute and permission is updated in the table on the Attribute-to-Permission Mapping tab.

What to do next

Whenever you edit a mapping, you must enable it, even if it was already enabled. For more information, see "Enabling an attribute-to-permission mapping" on page 81.

Related tasks:

"Enabling an attribute-to-permission mapping" on page 81
Complete this task to enable an attribute-to-permission mapping in the Access Governance Core module.

Related information:

"Attribute-to-Permission Mapping" on page 233
Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and

Intelligence that is based on the attribute settings on the target systems.

"Insert Attribute-to-Permission Mapping Track" on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Enabling an attribute-to-permission mapping

Complete this task to enable an attribute-to-permission mapping in the Access Governance Core module.

Before you begin

A target profile must be imported, and a target instance must be defined. For more information, see the following topics:

- Chapter 17, "Target type administration," on page 131
- Chapter 18, "Target administration," on page 143

Attribute-to-permission mappings must already be created, either by importing the mappings using a bulk load operation, discovering attributes from a target system, or adding attributes manually. For more information, see the following topics:

- "Importing an attribute-to-permission mapping with a bulk load operation" on page 70
- "Discovering attributes from a target system" on page 75
- "Adding an attribute-to-permission mapping manually" on page 72

Ensure that the mappings are exactly how you want them before you enable them. Perhaps have another person review the mappings to ensure that they are correct for your data set.

About this task

You can enable an attribute-to-permission mapping that you added individually or that you imported from the target system.

Enabling the mapping makes the information available in Identity Governance and Intelligence and propagates the definition so that it is ready for use. Enabling the attribute mapping creates a permission in the **Application Access** page of the Access Governance Core module.

When mappings are enabled, validation is performed on each attribute. For example, the following validations are performed during the enablement process:

- If a value is required for a string attribute, a default value must be specified.
- If values are specified for a string attribute, a default value must be specified.
- If an attribute is boolean, values must be defined.
- If values are specified, at least one active value must be specified.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select an account.

5. Optional: In the **Attribute-to-Permission Mapping** tab, click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.
6. In the **Attribute-to-Permission Mapping** tab, select an attribute mapping, and then select **Actions** > **Enable**. The Validation page is displayed. It lists all items that must be corrected in the mapping before it can be enabled for use in Identity Governance and Intelligence.

Results

When the mapping is enabled, a green check mark is displayed next to the permission name in the Attribute-to-Permission Mapping tab.

If a mapping is	You can edit these fields	You cannot edit these fields
Boolean but *not enabled*	• **Permission name** • **Required** • **Multi-value** • **Value if user has this permission** • **Value if user does not have this permission**	• **Attribute name** • **Type**
String but *not enabled*	• **Permission name** • **Required** • **Multi-value** • **Attribute value** • **Rights value** • **Active** • **Default**	• **Attribute name** • **Type**
Boolean and enabled	None	All
String and enabled	• **Active**: Indicate whether the value is active • **Default**: Indicate whether the value is the default You can add and remove values, but you cannot modify the existing values.	• **Attribute name** • **Permission name** • **Type** • **Required** • **Multi-value** • **Attribute value** • **Rights value**

What to do next

Verify that the mapping is displayed in the application. For more information, see "Verifying that an attribute-to-permission mapping is enabled" on page 83.

Related tasks:

"Editing an attribute-to-permission mapping" on page 78
Complete this task to individually edit the attribute-to-permission mapping in the Access Governance Core module.

Related information:

"Attribute-to-Permission Mapping" on page 233
Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and Intelligence that is based on the attribute settings on the target systems.

"Insert Attribute-to-Permission Mapping Track" on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Verifying that an attribute-to-permission mapping is enabled

Complete this task to verify that an attribute-to-permission mapping is enabled in the Access Governance Core module.

Before you begin

Enable the attribute-to-permission mapping. For more information, see "Enabling an attribute-to-permission mapping" on page 81.

About this task

You can verify that an attribute-to-permission mapping that you added individually or that you imported from the target system is enabled and ready for use in Identity Governance and Intelligence.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Applications**.
4. In the **Applications** pane, select an application.
5. In the **Application Access** tab, check the list of permissions to see whether your newly added permission is included in the list. Published permissions are shown in bold italics text. For example, ***Basic_Credentials***.

What to do next

You can check the details for each permission by selecting the permission in the **Application Access** and then selecting one of these tabs in the right pane:

- Details
- Properties
- Parent Hierarchy
- Rights
- History

If your permission does not display in the list, be sure that you enabled it. For information about enabling the permission, see "Enabling an attribute-to-permission mapping" on page 81.

Add the new permission (entitlement) to a user. For more information, see "Assigning an entitlement to a user" on page 101.

Related concepts:

"Permissions based on user attributes" on page 16
An attribute permission is a specific type of permission that is used for mapping a user attribute that is imported from a target system. For harmonizing this feature with the role-based access control standard of the Identity Governance and Intelligence data model, you can use permissions and rights.

Related information:

"Application Access" on page 211
Documents how to manage application permissions.

Removing an attribute-to-permission mapping

Complete this task to remove an attribute-to-permission mapping in the Access Governance Core module.

About this task

You can remove an attribute-to-permission mapping that you added individually or that you imported from the target system.

Because deleting the attribute mapping will also delete the permission, ensure that no users have entitlements before you delete the permission. There's not a way to find which users have the entitlements. You can view the list of users for that permission. Remove all the users from that permission, and then you can delete the permission.

Note: Removing an attribute permission mapping might cause errors if any users have this permission.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select an account.
5. Optional: In the **Attribute-to-Permission Mapping** tab, click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.
6. In the **Attribute-to-Permission Mapping** tab, select an attribute mapping, and then select **Action** > **Remove**. A message is displayed, which indicates that removing an attribute permission might cause errors when any users have this permission.
7. On the Remove Attribute message window, click **Ok**. The mapping for the attribute and permission is removed from the table on the Attribute-to-Permission Mapping tab.

Related concepts:

"Permissions based on user attributes" on page 16
An attribute permission is a specific type of permission that is used for mapping a user attribute that is imported from a target system. For harmonizing this feature with the role-based access control standard of the Identity Governance and Intelligence data model, you can use permissions and rights.

Related information:

"Attribute-to-Permission Mapping" on page 233
Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and Intelligence that is based on the attribute settings on the target systems.

"Insert Attribute-to-Permission Mapping Track" on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Chapter 8. Certification datasets

A campaign of certification is based on a dataset, which is built with elements that are analyzed during the campaign.

The following base entity sets can be used to define a dataset.

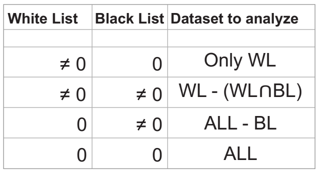
- **Groups**
- **Users**
- **Applications**
- **Entitlements**
- **Risks**
- **Account**
- **Advanced Settings**

For every entity set with exception of **Advanced Settings**, you can set a **White List** and a **Black List** of elements.

White List
Consists of elements to be analyzed.

Black List
Consists of elements that are excluded from analysis.

If an element in the white list is also put in the black list, it is not used for the analysis. The final entity set is determined according to the following table.



White List	Black List	Dataset to analyze
≠ 0	0	Only WL
≠ 0	≠ 0	WL - (WL∩BL)
0	≠ 0	ALL - BL
0	0	ALL

Only for the **Users** entity set, is possible to define a rule for loading a set of users into the **White List**.

Deploying a new dataset

About this task

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Click **Configure** > **Certification Datasets**.
4. In the left frame **Datasets**, click **Actions** > **Add**.
5. In the **Details** tab, set the identification attributes of the dataset. In the right frame, click the wanted entity tab:
   - **Group**
   - **Users**
   - **Applications**

- **Entitlements**
- **Risks**
- **Account**

6. For the selected entity tab, click **White List** or **Black List**.
   a. From the right pane, select the items that you want to add to the list.
   b. From the **Actions** menu, click **Add**.

   To remove an item from the list, select the item in the List pane and click **Remove** from the **Actions** menu
7. Select the **Advanced Settings** tab for choosing some advanced filters and click **Save**. The settings that are displayed depend on the type of selection you made in step 5.

Table 8. Advanced Settings

Setting	Description	Type of dataset
Visibility Violation	Includes assignments in Visibility Violations	Organization Unit Assignments - User Assignment
Disabled	Includes disabled users assignment or disabled OU assignments	Organization Unit Assignments - User Assignment
With Risk Violations	Includes accounts or users with violations.	Account - User Assignment
Delegated Roles	Includes assignment that is related to delegated roles	User Assignment
Account Disabled	Includes the disabled accounts	Account
Account not accessed since xxx Days	Includes account not accessed form *xxx* days.	Account
Assignments	Includes the assignments that are related to a Group or to User. It's possible to choose between Default Roles or not.	Organization Unit Assignments - User Assignment

Note: The advanced settings work in logic *and* with other tabs for defining a dataset. For example, if you have a user in the **White List** and select **Disabled**, the dataset is populated only by disabled roles that are related to the specified user.

For removing a dataset, select it in the left frame **Datasets**, then use **Actions** > **Remove**.

Related information:

"Certification data sets" on page 246
A campaign of certification is based on a data set, which is built with elements that are analyzed during the campaign.

Chapter 9. Data import with Bulk Data Load

Identity Governance and Intelligence administrators use the Administration Console to do data import tasks, such as importing users and entitlements into your security model.

Data import tasks

Use the Administration Console to do these tasks:

Table 9. Data import tasks

Task	Refer to
Populate the data model	“Creating a bulk load operation”
Import an attribute-to-permission mapping	“Importing an attribute-to-permission mapping with a bulk load operation” on page 70

Bulk Data Load in the Access Governance Core module
You can load bulk data in the AG Core database.

Bulk Data Load in the Access Risk Controls module
You can load large amounts of data.

Bulk Data Load in the Access Risk Controls for SAP module

Creating a bulk load operation

Complete this task to populate the data model.

Procedure

1. Log in to the Administration Console.
2. Select any of these modules:
   - **Access Governance Core**
   - **Access Risk Controls**
   - **Access Risk Controls for SAP**
3. Select **Tools** > **Bulk Data Load**.
4. In the **Action** tab, select one of the supported operations.
5. In the **File Batch** tab, click the **Download** icon to download a template that corresponds to the type of batch. This template is in the form of an Excel XLS spreadsheet file.
6. Open the spreadsheet template into your spreadsheet application, such as Excel.
7. In the spreadsheet template, complete the columns and rows according to your data specifications, and then save your spreadsheet. See the related help topic for the options and their descriptions.
8. In the **File Batch** tab, click **Browse** to locate and upload the Excel XLS file that corresponds to the selected operation.

   Note: The status of the operation, *Pending* to *Completed* is displayed at the bottom of the tab.
9. In the Information window, click **Ok**.

Bulk Data Load in the Access Governance Core module
You can load bulk data in the AG Core database.

Bulk Data Load in the Access Risk Controls module
You can load large amounts of data.

Bulk Data Load in the Access Risk Controls for SAP module

“Importing an attribute-to-permission mapping with a bulk load operation” on page 70
Complete this task to import an attribute-to-permission mapping by using a bulk load operation.

Chapter 10. Email and SMS notification administration

The Notification services enable administrators to associate emails and SMS messages to process steps. Thus, people in the organization are automatically notified upon the occurrence of an event that concerns them.

Administrators can set up notification templates and standardize them with the use of placeholders. The placeholders are replaced with values that are extracted from the process to which the notification - and its template - refers. Placeholders are available for notifications that refer to authorization requests, reports, certifications, and reminders.

In the processes that administrators configure for access requests in Process Designer, they can assign priorities to request steps and schedule periodic reminders before the requests expire. Administrators can also configure actions - accept, reject, escalate, do nothing - for authorization requests that expire and send notifications to the people concerned.

In Process Designer, administrators can configure in the activity extension of a process step the details of an email or SMS message that is sent when the activity completes.

Email administration tasks

Identity Governance and Intelligence administrators can set up and manage email notification templates and services in Access Governance Core.

Run these tasks in Access Governance Core and in Task Planner:

Table 10. Notification administration tasks

Task	Refer to
Setting up the notification service, creating templates, and tracking notifications	Configuring and managing notifications by email or SMS
Activating the email and SMS notification service	"Activating the EmailService task in Task Planner" on page 92
Attaching a notification after the completion of the steps of a process	"Configuring a notification extension in a process" on page 93

Priority and Reminder setup

In Process Designer, administrators can do these tasks:

- Associate a notification to the completion of an activity
- Configure Priority settings and expiration times for authorization requests
- Associate reminders to process steps

Table 11. Notification, Priority, and Reminder setup tasks in Process Designer

Task	Refer to
Defining notifications as activity configuration extensions	Activity extensions that you can define

Table 11. Notification, Priority, and Reminder setup tasks in Process Designer (continued)

Task	Refer to
Configuring priorities and expiration reminders	Configuring the priority and the expiration reminder for WorkFlow processes
Assigning expiration reminder policies to WorkFlow processes	Assigning an expiration reminder policy to a WorkFlow process
Assigning expiration reminder policies to Escalation processes	Assigning an expiration reminder policy to an Escalation process
Defining Redirect for Expiration escalation processes	Defining a Redirect for Expiration escalation process

Activating the EmailService task in Task Planner

The `EmailService` task runs the jobs that send email and SMS notifications as defined within work flows. This task must be active if you want all notifications to be sent automatically by Identity Governance and Intelligence.

About this task

This task must be active also if you want to test your templates in **Access Governance Core** > **Configure** > **Notifications** > **Notification Settings**.

The following procedure shows where to go to verify that the task is active and how to activate it if it is not.

Procedure

1. Select **Task Planner** in the Administration Console.
2. Select **Manage** > **Tasks**.
3. Scroll the list of tasks until you find `EmailService`. If the task is active, ✓, no further steps are necessary and you can exit Task Planner. If the task is not active, ✗, you must take these steps to activate it.
   a. Select **Settings** > **Scheduler** in Task Planner.
   b. Select `Singleton` from the list of schedulers and click **Actions** > **Synchronize**.
   c. Return to **Manage** > **Tasks** and check that `EmailService` is active. If the task still shows not active, select it and click **Actions** > **Start**.

Results

The `EmailService` task is active and the jobs that send emails and SMS messages from Identity Governance and Intelligence are ready to run.

The jobs of the EmailService task

The EmailService task includes jobs that handle the notification services of Identity Governance and Intelligence.

The task includes three jobs.

SystemEmailService
Forwards all email and SMS message notifications from Identity Governance and Intelligence.

AccessRequestNotification

Assembles the data that is entered in the authorization request by a user - template, placeholders, and recipients - in the notification and feeds it to SystemEmailService for delivery.

AccessRequestReminder

Manages reminder notifications that are sent before or after the expiration of an authorization request. Assembles the data that is entered in the Reminder pane for a Workflow and feeds it to SystemEmailService for delivery.

To view the setup of these jobs, follow these steps:

1. In Task Planner, select **Manage** > **Task** and select the EmailService task.

   The information for EmailService is displayed on the right.
2. Select **Jobs**.

   The jobs that are included in the task are displayed in a tree view.
3. Select any of the jobs to display their settings.

To change job settings, you must first stop the task. Then, you can take one of the following actions:

- Select **Actions** to add, remove, or move a job up or down the tree structure of EmailService.
- Select either job and click **Edit** at the lower right to change some of its settings.
  - For job SystemEmailService, you can change the EMAIL_ITERATIONS integer. This parameter is the maximum number of iterations that are used to search for a notification. You can change this number to lower or higher values.
  - For jobs AccessRequestNotification and AccessRequestReminder, you can change the NOTIFICATION_PAGING integer. This parameter is the maximum number of notification requests that the job can accept at a time. You can change this number to lower or higher values.

Configuring a notification extension in a process

You can add a notification extension to the activities of a process flow so that emails and SMS messages are sent after the activities complete.

About this task

You can add a notification to every activity of the process or to selected ones, since, you add the notifications to the individual activity blocks.

The notification can be by email, SMS, or both. Before you set up the notification in the Notification window, the following items must be defined in Access Governance Core:

- The notification template.
- The email address and the mobile phone number of each recipient. These data must be present in the **Email** and **Phone Number** fields of the user's definition in **Access Governance Core** > **Configure** > **Users** > **Details**.

Procedure

1. Right-click the arrow➔, that you find on the upper right of the activity block. A box menu is displayed.

2. Select **Add**.
3. Select **Notification**. The Notification window is displayed.
4. Click the downward arrow in **Type** and select a template type. The **Template** field lists only the templates of this type that are defined in Access Governance Core.
5. Click the downward arrow in **Template** and select a template. Select **Validate** to validate the placeholders that are included in the template. The placeholders are validated against the **Context** and **Functionality** of the activity for which the notification is sent. Click here to find which placeholders fit a specific context and functionality.
6. Select the recipients of the notification. Depending on your notification settings, on the definition of the template that you specified, and on your needs, specify the recipients of the email, the SMS, or both.
   a. If the notification includes an email, select the recipients in the **Email** section. Select at least one of the listed recipients.

      Requested For
      Send the email to the beneficiary of the request.

      Requested By
      Send the email to the generator of the request.

      Approvers
      Send the email to the approvers involved into the process.

      Fixed Addresses
      Send the email to other users. Specify the email addresses, separating them with semicolons, in the related field.

      Select carbon copy and blind carbon copy recipients. Note that for every type of recipient the **To**, **CC**, and **Bcc** selections are mutually exclusive.

      Select **Preview** to display a preview of the template. This option is not available if the template is not for emails.
   b. If the notification includes an SMS message, select the recipients in the **SMS** section. Select at least one of the listed recipients.

      Requested For
      Send the SMS message to the beneficiary of the request.

      Requested By
      Send the SMS message to the generator of the request.

      Approvers
      Send the SMS message to the approvers involved into the process.

      Fixed Phone Numbers
      Send the SMS message to other users. Specify the mobile telephone numbers, separating them with semicolons, in the related field.

      Select **Preview** to display a preview of the template. This option is not available if the template is not for SMS messages.
7. Select **Ok** to save your settings. This action validates the placeholders of the template. If the placeholders are out of context, an error message is displayed and the Notification window does not close.

Results

The **Notification** icon, ✉, is appended at the right of the activity block. You can at anytime select this icon to change the settings.

To remove the notification extension, right-click the arrow ➔ at the upper right of the activity block, and select **Remove** > **Notification**.

Matching placeholder keys to the context and functionality of an activity

When you specify the template for the notification extension of an activity, the placeholders that it might contain are validated against the **Context** and the **Functionality** that were specified for the activity.

A placeholder must be pertinent to the context and functionality of the activity. When the activity becomes part of the authorization request in Access Requests, the placeholder is resolved with the corresponding value that is entered in the request.

See the next table to be sure that the placeholders of the template that you specified are right for the context and the functionality of the concerned activity.

Remember: The true syntax of a placeholder in a template is `${`*`placeholder`*`}`.

Table 12. Placeholders by activity **Context** *and* **Functionality**

Context	Functionality	Placeholder
Account Change	Detailed Request, Request Authorization, and Request Execution	*account.name*
		account.password
		applicant.name
		applicant.surname
		applicant.userid
		beneficiary.name
		beneficiary.surname
		beneficiary.userid
		request.id
		request.status
		request.type
		subrequest.id

Table 12. Placeholders by activity **Context** *and* **Functionality** *(continued)*

Context	Functionality	Placeholder
Admin Access Change	Formal Request, Request Authorization, and Request Execution	*applicant.name*
		applicant.surname
		applicant.userid
		beneficiary.name
		beneficiary.surname
		beneficiary.userid
		request.id
		request.status
		request.type
		roles.name
		subrequest.id
Admin Delegation Change	Formal Request, Request Authorization, and Request Execution	*applicant.name*
		applicant.surname
		applicant.userid
		beneficiary.name
		beneficiary.surname
		beneficiary.userid
		delegator.name
		delegator.surname
		delegator.userid
		request.id
		request.status
		request.type
		roles.name
		subrequest.id
Delegation Change	Application Filtered Request, Request Authorization, and Request Execution	*applicant.name*
		applicant.surname
		applicant.userid
		beneficiary.name
		beneficiary.surname
		beneficiary.userid
		delegator.name
		delegator.surname
		delegator.userid
		request.id
		request.status
		request.type
		roles.name
		subrequest.id

Table 12. Placeholders by activity **Context** *and* **Functionality** *(continued)*

Context	Functionality	Placeholder
Entitlement Management	Authorize Insert Entitlement, Authorize Entitlement Update, Execute Entitlement Update, Execute Insert Entitlement, Insert Entitlement, and Update Entitlement	*applicant.name*
		applicant.surname
		applicant.userid
		main.role.name
		request.id
		request.status
		request.type
		role.fields
		roles.name
		subrequest.id
Incompatibility Management	Authorize Incompatibility in Delegation	*applicant.name*
		applicant.surname
		applicant.userid
		beneficiary.name
		beneficiary.surname
		beneficiary.userid
		request.id
		request.status
		request.type
		roles.name
		subrequest.id
Request Report	Request Report and Daily Work	*account.name*
		account.password
		applicant.name
		applicant.surname
		applicant.userid
		beneficiary.name
		beneficiary.surname
		beneficiary.userid
		delegator.name
		delegator.surname
		delegator.userid
		main.role.name
		request.id
		request.status
		request.type
		role.fields
		roles.name
		subrequest.id
		user.fields

Table 12. Placeholders by activity **Context** *and* **Functionality** *(continued)*

Context	Functionality	Placeholder
User Access Change	Formal Request, External Request Authorization, Request Authorization, and Request Execution	*applicant.name*
		applicant.surname
		applicant.userid
		beneficiary.name
		beneficiary.surname
		beneficiary.userid
		request.id
		request.status
		request.type
		roles.name
		subrequest.id
User Management	Authorize Insert User, Authorize Update User, Execute Insert User, Execute Update User, Insert User, Update User	*applicant.name*
		applicant.surname
		applicant.userid
		request.id
		request.status
		request.type
		subrequest.id
		user.fields

Chapter 11. Entitlement administration

Identity Governance and Intelligence administrators use the Administration Console to do entitlement administration tasks, such as adding roles and adding entitlements to organizational units.

“Roles” on page 201
A role identifies the set of permissions that are assigned to a user. Use this set of panels to define and manage roles in your organization.

“Entitlements” on page 196
You can view all the entitlements that are already associated to a group of a selected hierarchy.

Adding an entitlement

Complete this task to register a new entitlement into the Identity Governance and Intelligence data model.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Roles**.
4. Select the **FlatView** tab and click **Actions** > **Add**.
5. In the **Details** tab, define a basic entitlement profile. Specify information in the following fields and in the other fields, if applicable. See the related help topic for the options and their descriptions.
   - Name
   - Code
   - Type
   - Application
6. Click **Save**.
7. In the Information window, click **Ok**.

Related information:

“Roles” on page 201
A role identifies the set of permissions that are assigned to a user. Use this set of panels to define and manage roles in your organization.

Adding an entitlement to an organizational unit

You must assign the entitlement to the organizational unit before you can assign the entitlement to a user that belongs to the same hierarchy of the organizational unit.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Groups**.
4. In the **Hierarchy** field, select **ORGANIZATIONAL_UNIT**.

5. In the **View** tab, select the organizational unit from which to add the entitlement.
6. Access the **Entitlements** tab and click **Actions** > **Add**.
7. In the Add window, select the entitlement and click **OK**.
8. In the Insert Group Entitlements window, select the values for the following options. See the related help topic for the options and their descriptions.

   Default

   Select any of these options:
   - **No** for a basic configuration.
   - **Yes** to automatically assign this entitlement to all users that are added to the group.
   - **Yes, and align users** to automatically assign this entitlement to all users of the group. In this case, the administrator must assign the appropriate set of resources to each user.

   Visibility Violation

   Select **No** for a basic configuration.

   Enabled

   Select **Yes** for a basic configuration.

   Hierarchy

   Select the check box to assign the organizational unit to the hierarchy.
9. Click **OK**.

Related information:

"Entitlements" on page 196
You can view all the entitlements that are already associated to a group of a selected hierarchy.

Adding entitlements to an attribute group

Complete this task to join a set of entitlements to a group of an attribute hierarchy. For example, you can assign the entitlements to the users of the organizational unit.

About this task

The following procedure is an example way of completing this task. To create a different behavior, you can select other configuration settings based on your requirements or preferences.

Procedure

1. Complete "Creating an attribute hierarchy" on page 106.
2. Select **Manage** > **Groups**.
3. In the **Hierarchy** field, select the hierarchy.
4. In the **View** tab, select the group to which the entitlement is to be added.
5. Access the **Entitlements** tab.
6. Click **Actions** > **Add**.
7. In the Add window, select the entitlement to be added and click **OK**.
8. In the Insert Group Entitlements window, select the values for the following options. See the related help topic for the options and their descriptions.

Default

Select any of these options:

- **No** for a basic configuration.
- **Yes** to automatically assign this entitlement to all users that are added to the group.
- **Yes, and align users** to automatically assign this entitlement to all users of the group. In this case, the administrator must assign the appropriate set of resources to each user.

Visibility Violation

Select **No** for a basic configuration.

Enabled

Select **Yes** for a basic configuration.

Hierarchy

Select the check box to assign the Entitlement to the hierarchy.

9. Click **OK**.

Related information:

"Entitlements" on page 196
You can view all the entitlements that are already associated to a group of a selected hierarchy.

Publishing an entitlement

You must publish the entitlement before you can assign it to a user.

About this task

A published entitlement is displayed in ***italic bold*** in the **FlatView** list.

Procedure

1. Log in to the Administration Console.
2. Complete "Adding an entitlement" on page 99.
3. In the Administration Console, click **Access Governance Core**.
4. Select **Manage** > **Roles**.
5. In the **FlatView** tab, select the entitlement (role) to publish.

   Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.
6. Click **Actions** > **Publish**.
7. In the Information window, click **Ok**.

Related information:

"Roles" on page 201
A role identifies the set of permissions that are assigned to a user. Use this set of panels to define and manage roles in your organization.

Assigning an entitlement to a user

Complete this task to associate a new entitlement to a user.

Procedure

1. Log in to the Administration Console.
2. Optional: Complete "Adding a user" on page 163.

3. Optional: Complete “Publishing an entitlement” on page 101.
4. Optional: Complete “Adding an entitlement to an organizational unit” on page 99.
5. In the Administration Console, click **Access Governance Core**.
6. Select **Manage** > **Accounts**.
7. Select **Manage** > **Users**.
8. In the **Users** tab, select the user.
9. Select the **Entitlements** tab to view the list of entitlements that are already assigned to the user.

   Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.
10. In the **Entitlements** tab, click **Actions** > **Add** to add an entitlement to the user.
11. In the Add Entitlement window, select the new entitlement and click **OK**. You can check for conflicts by selecting **Actions** > **Conflicts**. The Associated Rights window is displayed if the right is a string type. If the new entitlement has a conflict, manage it in the Conflicting Entitlements window and click **OK**.
12. In the Associated Rights window, which is displayed only for rights that are string type, add or remove the wanted rights values and click **OK**. The Date Selection window is displayed.
13. In the Date Selection window, set the validity period of the assignment or leave it empty for an indefinite period and click **OK**. The entitlement is added to the user.

Related information:

“Users” on page 175
You can define and manage users and items that are associated to them, such as entitlements, resources, accounts, rights, mitigations, events, and activities.

“Entitlements” on page 179
Use the **Entitlements** tab to assign or delegate entitlements.

Adding a property content

This task can be run for adding properties to a role or to an application access.

About this task

This task can be run from two different panes like

- **Manage** > **Roles** > **Entitlement Properties**
- **Manage** > **Applications** > **Application Access** > **Properties**

Procedure

1. Click **Actions** > **Add**, for getting an empty line.
2. Click ⋯ **Add Key**, for setting a new key in Key Properties pop-up window.
3. If you need to add a property key, click **Actions** > **Add**.
4. Choose a key in Key Properties, selecting the related leftmost check-box.
5. If you need, select also the check-boxes **Searchable** and **Mutiple Value**.
6. Click **Ok**.
7. For the property just added, click ⋯ **Add Value**, for setting a new value in Value Properties pop-up window.
8. If the property is multi-value, click **Actions** > **Add** to add multiple values.

9. Click **Ok**.

Related information:

"Application Access" on page 211
Documents how to manage application permissions.

"Rights Lookup" on page 270
You can define the lookup tables sets for managing rights with lookup.

Adding *Right Lookup* content

Complete this task if a *Right Lookup* set of values is required.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Configure** > **Rights Lookup**.
4. Click **Actions** > **Add**.
5. In the Add window, set the name of the *Right Lookup* content and click **OK**.
6. Select the *Right Lookup* table that you just created.
7. In the right panel, click **Actions** > **Add**.
8. Add the values and click **OK**.

Related information:

"Rights Lookup" on page 270
You can define the lookup tables sets for managing rights with lookup.

Chapter 12. Group administration

Identity Governance and Intelligence administrators use the Administration Console to do group administration tasks, such as adding organizational units.

Group administration tasks

Use the Administration Console to do these tasks:

Table 13. Group administration tasks

Task	Refer to
Add an organizational unit to the system	"Adding an organizational unit"
Create an attribute hierarchy	"Creating an attribute hierarchy" on page 106
Configure a hierarchy to structure the organizational unit	"Configuring the attribute hierarchy" on page 106

"Groups" on page 193
You can use functions to manage a hierarchy. The main hierarchy is the ORGANIZATIONAL_UNITS hierarchy.

"Hierarchy (Polyarchies)" on page 267
In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.

Adding an organizational unit

Complete this task to register a new organizational unit.

About this task

The hierarchies of an organizational unit are a specific case of "Configuring the attribute hierarchy" on page 106.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Groups**.
4. In the **Hierarchy** field, select **ORGANIZATIONAL_UNIT**.
5. In the **View** tab, select which organization unit to add the new one and click **Actions** > **Add**.
6. In the **Details** tab, define a basic Organization Unit profile. See the related help topic for the options and their descriptions.
7. Click **Save**.
8. In the Inheritance window, specify whether to inherit the Entitlements and Resources that are deployed in the parent Organization Unit by selecting the corresponding check box.
9. Click **OK**.
10. In the Information window, click **Ok**.

Related information:

"Groups" on page 193
You can use functions to manage a hierarchy. The main hierarchy is the ORGANIZATIONAL_UNITS hierarchy.

Creating an attribute hierarchy

Complete this task every time you need to a build a hierarchy.

Procedure

1. Complete "Configuring the attribute hierarchy."
2. Select **Configure** > **Hierarchy**.
3. In the **Hierarchy** tab, click **Actions** > **Build**.
4. Select **Monitor** > **Scheduled Task** to check the build status. If the status is `Completed`, the build completed successfully.
5. To check the result, select **Configure** > **Attribute Groups** and select the attribute hierarchy that just built.

Related information:

"Hierarchy (Polyarchies)" on page 267
In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.

Configuring the attribute hierarchy

Complete this task to create a hierarchy to structure the organizational unit.

About this task

Identity Governance and Intelligence provides a mechanism to build an infinite number of hierarchies. The most common and traditional is the hierarchy of the organizational unit.

You can build a hierarchy based on:

User attributes
Every administrator can map their own and specific user attributes.

Rules Administrator can have an unlimited number of rules. Every rule can be configured with a different behavior.

The **Field** list contains the attributes of the **User Data** list. It refers to the **UserErc** table. To view these attributes, follow these steps:

1. From the Access Governance Core, select **Settings** > **Core Configurations** > **User Virtual Attributes**.
2. In the **Repository** tab, select the **UserErc** table.
3. Access the **Attribute Mapping** tab.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Configure** > **Hierarchy**.
4. In the **Hierarchy** tab, click **Actions** > **Add**.
5. In the **Details** tab, define a basic hierarchy profile. See the related help topic for the options and their descriptions.

Name Specify the hierarchy name.

Configuration Type
Select the configuration type.

Manual
Only the hierarchy is created. You must add the groups and users manually.

Simple

The group is created by using the value selected from **Field**list.

Advanced

The group is created by using an existing rule. You can opt to build the hierarchy automatically through a scheduled job or once.

Value Select from the following values.

Single Value

A node is added for each value of the attribute. Each user with that attribute is added in that node.

Multi Value

A node is added for each value of the attribute. If the attribute has multiple values, each value must be separated by a separator char. Specify the character in the **Separator Char** field. A user is added in each node with the specified value.

Hierarchy

The path that is specified in the selected **Field** of each user is used to create the hierarchical tree structure. Each user is added in the last node specified in the selected **Field**.

UserID Attribute (Automatic Scope Assignment)
Select this check box to assign the administrator role and its relative scope to the hierarchy.

UserID Assigned Role
If you selected **UserID Attribute (Automatic Scope Assignment)**, select an administrative role.

Note: The selected role must have the **Attribute Hierarchy** already selected from **Access Governance Core** > **Configure** > **Admin Roles** > **Scope**.

User ID Hierarchy
If you selected **Single Value**, select this check box to get a hierarchical tree structure, in which each node is set as a child of a node that has the same name as one of the users in that group.

6. Click **Save**.

Related information:

"Hierarchy (Polyarchies)" on page 267
In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.

Chapter 13. Password administration

Identity Governance and Intelligence administrators use the Administration Console to do password administration tasks, such as configuring the password service and changing account passwords for users.

Password administration tasks

Account passwords are used to access the accounts that a user is entitled to use. Accounts correspond to applications.

Service Center passwords are used to log in to the Service Center.

Use the Administration Console to do these tasks:

Table 14. Password administration tasks

Task	Refer to
Change a user's password for one or more accounts.	"Changing account passwords for users"
Force a password change for a Service Center user.	"Forcing a password change" on page 110
Configure the password service to enable password changes from the Service Center.	"Configuring password services" on page 110

For information about password-related tasks that managers and help desk personnel can do in the Service Center, see Chapter 33, "Password management," on page 673.

Related information:

"Accounts" on page 182
You can create and manage user accounts and set user passwords.

Changing account passwords for users

You can change the password for one or more accounts of a specific user.

Before you begin

The Identity Governance and Intelligence administrator, also known as the *Super Admin*, or other administrators must complete this task to change the password of a user.

About this task

Account passwords are used to access the accounts that a user is entitled to use. Accounts correspond to applications. For example, the Service Center application is associated with an account named `Ideas`. If you change the password of a Service Center user, you select `Ideas` from the list of accounts.

Procedure

1. Log in to the Administration Console.
2. Select **Access Governance Core**.
3. Select **Manage** > **Users**.
4. Select the user that you want to change the password for.
5. In the **Accounts** tab, select the account for that user.
6. Select **Actions** > **Change Pwd**.
7. In the **Change Password** window, specify the new password in the **Password** and **Confirm Password** fields, and click **OK**.

Results

The user password is changed. Click **OK** when you see the message that indicates a successful operation.

Related information:

"Accounts" on page 182
You can create and manage user accounts and set user passwords.

Forcing a password change

You can force users to change their password the next time that they log in to the Service Center.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. Log in to the **Administration Console**.
2. From the Administration Console, select **Access Governance Core**.
3. Select a user, and then select the **Accounts** tab for that user.
4. Select the account that you want to force the password change for, and then click **Actions** > **Force Pwd**.

Results

A green check mark is displayed in the **Force Change Pwd** column. The user is prompted to change the password during the next login to the Service Center.

Related information:

"Accounts" on page 182
You can create and manage user accounts and set user passwords.

Configuring password services

You must configure the password service in Access Governance Core to enable the features that are related to password management for Service Center users.

About this task

You must configure the password service to enable the following features:

Forgot password

Enables users to reset their Service Center password if they forget it. Users are first authenticated with their predefined security questions. Then, they can enter a new password or receive a system-generated password at their registered email address. Depending on the configuration setup, users might have the option to edit their email address.

Self Care

An application in the Service Center where users can change their own passwords.

Password reset

An account change process of the Access Requests application where a manager or entitled person can reset the password of a requesting user. This requires further configuration in the Process Designer. Two predefined workflows, one for the user manager and one for the application manager administrative roles, are provided ready-for-use.

To learn how to configure the password service in the Access Governance Core, see "Configuring the password service in Access Governance Core."

To learn how to configure the account change process for changing passwords in the Process Designer, see "Configuring the password service in Process Designer" on page 113.

Related information:

"Accounts" on page 182
You can create and manage user accounts and set user passwords.

Configuring the password service in Access Governance Core

Configure the password service in the Access Governance Core to enable the `Forget password`, `Self Care`, and `Password reset` features and to set up and manage the security questions.

About this task

This task is a required action to set up the user authentication process that is based on security questions. The authentication process verifies the identity of users who must use the `Forgot your password` feature or ask their manager or other entitled person, such as a help desk operator, to reset their Service Center password.

Procedure

1. Log in to the Administration Console.
2. Select **Access Governance Core**.
3. Select **Settings** > **Configure Password Service** > **Configure Forgotten Password Service**.
4. Complete the items described in the following table:

Table 15. Configuration items for Configure Forgotten Password Service

Section	Configuration options and descriptions
Admin configuration	**Enable password service**: Flag this check box to enable the following services: **Forgot password** Enables users to reset their password to enter the Service Center if they forget it. Users are first authenticated with security questions. Then, they can enter a new password or receive a system-generated password at their registered email address. Depending on the configuration setup, users might have the option to change their email address. **Self Care** Enables users to change their passwords in the Service Center. **Password reset** An account change process of the Access Requests application where a manager or entitled person can reset the password of a user.
Security questions configuration	**Number of security questions asked at first login** The number of security questions to ask a new user. The answers that are provided at this time are saved and used as benchmarks for verification when the user forgets the login password. **Number of security questions asked for reset** The number of security questions to ask a user who has forgotten a password. This number must be smaller or equal to the number of questions asked at first login. **Number of failed attempts allowed** The number of attempts that a user can try to correctly answer all the security questions. If the security questions are not answered correctly, the password is not provided, and the user must follow a different process to ask for help. For example, the user might contact the help desk, an administrator, or a manager. **Note:** This option applies to the `Forgot password` and `Self Care` features. It does not affect the `Password reset` feature. **Minimum length of the answer** The minimum number of characters required for every security answer.

Table 15. Configuration items for Configure Forgotten Password Service (continued)

Section	Configuration options and descriptions
Mode configuration	**Allow user to change password immediately** After a user successfully answers the security questions, the user is prompted to enter a new password and can login immediately. **Send one-time password to known user address** After a user successfully answers the security questions, a new password is emailed to the user. The password is valid for only one login, and the user is prompted to enter a new password. **Allow user to edit email address** Select this check box to let the user edit the address where the password is sent.

5. Select the **Security Questions** tab.
6. Select **Actions** > **Add** and add security questions. Add new questions in English before you add them in other languages. By default, new questions are saved with the **Active for user** check box not selected. This means that the questions are not visible to users. To make a question available for use, select the check box. Clear the check box before you edit a question or add a locale. This is not necessary when you remove a question. When a question is removed or modified, users who have that question in their `Forgot password` list are prompted to answer a new question at their next login.

Results

The password service is configured. To configure the **Password reset** service for the Access Requests application, see "Configuring the password service in Process Designer."

Related information:

"Accounts" on page 182
You can create and manage user accounts and set user passwords.

Configuring the password service in Process Designer

You must configure an account change workflow in the Process Designer to create a workflow for password reset requests in the Access Requests application of the Service Center.

Before you begin

Yo must also configure the password service in the Access Governance Core to enable the password reset workflows.

About this task

A password reset workflow is the process that a manager or entitled user runs through to reset the Service Center password of another user. The workflow runs in the Access Requests application.

Two preconfigured workflows of this kind are provided:

ManagerPasswordReset
This workflow is configured for a user that is entitled with the User

Manager administrative role. It empowers the User Manager (the applicant) to enter a new password for a user who belongs to the same organization unit (the beneficiary). The applicant does not use security questions to verify the identity of the beneficiary, types a new password for the beneficiary, and edits the email address of the beneficiary, if necessary. As the applicant submits the request, an email with the new password is forwarded to the beneficiary.

HelpDeskPasswordReset
This workflow is configured for a user that is entitled with the Application Manager administrative role. It empowers the Application Manager (the applicant) to enter a new password for any user, regardless of which organization unit the user belongs to (the beneficiary). The applicant uses security questions to verify the identity of the beneficiary, has the system generate a password, but cannot edit the email address of the beneficiary. As the applicant submits the request, an email with the new password is sent to the beneficiary.

Both workflows include a request generation and a request execution activity. From a practical point of view, the password is created and emailed to the beneficiary after the applicant clicks **Submit** at the end of the request generation flow.

You can use these workflows as they are, modify them, or configure new workflows starting from an Account Change process. As an example, the following procedure shows how to view or modify the details of the `ManagerPasswordReset` workflow.

Procedure

1. Log in to the Administration Console.
2. Select **Process Designer**.
3. Select **Manage** > **Process**.
4. Select `ManagerPasswordReset` in the list of processes. The right part of the window displays the workflow details. If you plan to modify the details, set the **Status** to `Off line`. A workflow in off line or in maintenance status is not available to users in the Access Requests application.
5. Click **Next** to proceed to the Configuration window where you can view the two activities that make up this workflow. The activities are:

   ManagerPasswordResetGEN
   Is the part of the flow where:

   - The user (beneficiary) whose password must be reset and the accounts for which the password grants access are selected.
   - The new password is entered and emailed to the beneficiary.

   ManagerPasswordResetEXE
   Is the part of the flow where the request is displayed in a list of requests to an entitled operator. There is no action for the operator except to acknowledge whether the request was completed.
6. Click **ManagerPasswordResetGEN** to display the details of this activity. Under **Activity scope**, you find the following tabs:

Table 16. `Activity scope` tabs of `ManagerPasswordResetGEN`

Tab	Content
Beneficiary	Provides a selection of the type of users for whom the applicant (the User Manager in this case) can reset a password. This affects the list of users displayed in the Users page of the request in Access Requests.
Application	Provides a selection of the type of applications (accounts) accessible to the user for which the applicant can reset a password. This affects the list of accounts displayed in the Accounts page of the request in Access Requests.
Required Data	Provides configuration options for the request, where the account operation is `Change Password`. This affects the contents of the remaining pages of the request, such as: • Whether there are security questions to verify the identity of the beneficiary • If the applicant is requested to enter his/her own password • If the applicant types the new password or has it generated automatically • If the new password is emailed to the beneficiary or communicated by other means • If the beneficiary's email address can be updated on the moment
Email data	Provides the template for the text of the email sent to the beneficiary with the new password. Templates are managed in **Access Governance Core** > **Configure** > **Email**.

You can edit the choices selected in these tabs to better meet your requirements.

7. Click **Ok** or **Cancel** to close the Activity window.
8. Click **ManagerPasswordResetEXE** to display the details of this activity. Remember that the Execution activity of this work flow is nominal. **Activity scope** includes the following tabs:
   - Beneficiary
   - Application
9. Click **Ok** or **Cancel** to close the Activity window.
10. Click **Next** to proceed to the Assign window where the activities are assigned to one or more roles. The window displays the role to which `ManagerPasswordResetGEN` is assigned. In this case the role is `User Manager`. You can add other roles or replace the existing one with the **Actions** > **Add/Remove** buttons. When you add a role, you can choose from the roles that are defined in the Access Governance Core.
11. Click the **ManagerPasswordResetEXE** tab to view the role that this activity is assigned to. In this case, the activity is assigned to the `Operator` role.
12. If you have changed the configuration options, click **Save** and put the workflow back on line. Otherwise, proceed to another process, tab, or close the window.

Results

The User Manager finds the **ManagerPasswordResetGEN** tab in the Access Requests application of Service Center. The User Manager selects this tab to use a wizard that helps create and email a password for another user. Similarly, an Operator can use the **ManagerPasswordResetEXE** tab to view a list of the latest

`ManagerPasswordResetGEN` requests that are submitted and their status.

Related information:

"Accounts" on page 182
You can create and manage user accounts and set user passwords.

Chapter 14. Reconciliation management

Reconciliation synchronizes the accounts and supporting data to the IBM Security Identity Governance and Intelligence central data repository from a managed resource. Reconciliation is required so that the Identity Governance and Intelligence data is consistent and up-to-date with the remote resource.

Reconciliation overview

Reconciliation ensures the accuracy of permissions and accounts data for the managed targets. Reconciliation can be scheduled to run routinely (for example, daily) or initiated by the administrator. The reconciliation schedule is stored in the Identity Governance and Intelligence database.

When the reconciliation schedule is triggered, Identity Brokerage runs a reconciliation through an Identity Brokerage Adapter. It compares the search results of the recent reconciliation with the data that is stored in the target cache. Identity Brokerage stores the delta data and change events, in the Recon Change Event database. Changes are saved in the target cache. These changed events are retrieved and posted back to the Target Administration Console.

During reconciliation, new accounts on the managed resource are created in the Identity Governance and Intelligence repository and assigned to the user based on the adoption policy for the target.

If a match exists between a user login ID and an account, the software creates the ownership relationship between the account and the person. It also verifies that the accounts fit in the constraints of a defined policy. If no match exists, the unmatched accounts are listed as orphaned accounts. The Identity Governance and Intelligence administrator can manually assign the orphan account to a user.

Modified accounts on the managed resource are updated to the Identity Governance and Intelligence repository. Accounts that are removed from the managed resource are also removed from Identity Governance and Intelligence.

You can manage schedules for reconciliation or initiate a reconciliation activity immediately. To determine an ownership relationship, reconciliation compares account information with existing user data that is stored on Identity Governance and Intelligence. It first looks for the existing ownership in Identity Governance and Intelligence. It then applies adoption rules that are configured for the reconciliation.

You can run reconciliation to load accounts and supporting account information, which includes groups, into Identity Governance and Intelligence. Reconciliation inserts accounts from the managed resources into the Identity Governance and Intelligence directory.

Managed target accounts can be excluded from reconciliation on the Identity Governance and Intelligence and on the managed target itself for some adapters.

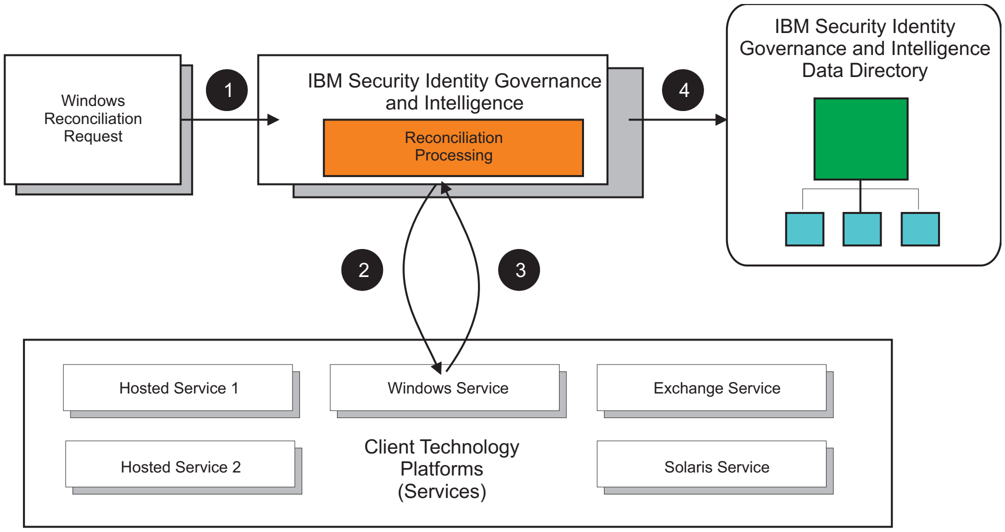
Reconciliation tips

Follow these suggestions for reconciliation:

- Set up reconciliation schedules based on the frequency of data changes.
- Allow adequate time between two reconciliations.
- Avoid unnecessary reconciliations.

Reconciliation process

The following illustration is an overview of the reconciliation process. In this example, the software reconciles Windows Server data.


Windows Reconciliation Request
1
IBM Security Identity Governance and Intelligence
Reconciliation Processing
4
IBM Security Identity Governance and Intelligence Data Directory
2
3
Hosted Service 1
Windows Service
Exchange Service
Hosted Service 2
Client Technology Platforms (Services)
Solaris Service

The numbered steps in the following table correspond to the illustration.

Step	Description
1	An administrator submits a reconciliation request to a system with security that is managed by Identity Governance and Intelligence.
2	The reconciliation request is sent to the selected target.
3	The target collects information from the system and sends the information to Identity Governance and Intelligence.
4	The the information is read and reconciled with the Identity Governance and Intelligence directory with account information from the target.
5	Identity Governance and Intelligence attempts to find the account owner.

Reconciliation timeout and failure threshold

A reconciliation job can hang if the target does not respond to the Identity Brokerage queries in a timely manner. To prevent the reconciliation job from waiting for an indefinite period, set a reconciliation timeout. Another important precaution is to set the reconciliation failure threshold. This setting prevents the reconciliation job from removing all user accounts from a target in Identity Governance and Intelligence in the rare case where a successful reconciliation returns no accounts.

Reconciliation timeout

Reconciliation timeout (`ib.reconciliation.timeout.minutes`) is the duration of the reconciliation.

- You can schedule reconciliation or trigger it on demand from the Target Administration Console.
- You can set the timeout value only for a scheduled reconciliation. For information about setting the timeout value, see “Creating a reconciliation schedule” on page 120. There is no option to modify the default timeout value for reconciliation on demand.
- The default maximum timeout value for reconciliation on demand is 600 minutes.

Reconciliation failure threshold

Reconciliation failure threshold (`ib.reconciliation.failurethreshold`) is the maximum number of local accounts that are deleted from the Identity Brokerage cache at the end of a reconciliation.

- You can configure this property through the IBM Security Identity Governance and Intelligence command-line interface. For information about configuring the property, see Getting and setting the reconciliation failure threshold.
- You can specify any value from 0 to 100, and it is considered as a percentage value.
- If the number of accounts that are deleted from the target exceeds the threshold value that you specified, then no local account or supporting data entries are deleted.

Related tasks:

“Creating a reconciliation schedule” on page 120
You can schedule a reconciliation for account and attribute data or only for supporting data from the managed target.

Related information:

Getting and setting the reconciliation failure threshold

Reconciling accounts immediately on a target

You can initiate a reconciliation activity immediately on a target, rather than scheduling the reconciliation.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a target instance.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:

    a. Type information about the target in the **Search information** field.
    b. Select a target type from the **Target type** list.
    c. Select a status from the **Status** list, and then click **Search**. A list of targets that matches the search criteria is displayed.

       If the table contains multiple pages, you can do the following tasks:

       - Click the arrow to go to the next page.
       - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▸) next to the target to show the tasks what can be done. The tasks depend on the type of target.
6. Click **Reconcile Now**.
7. Click **Submit** to request an immediate reconciliation activity.
8. Optional: To view the results, click **View the status of the reconciliation request**.
9. To prevent the reconciliation from running at the scheduled time, change or delete the scheduled reconciliation.
10. Click **Close**.

Results

A message indicates that you successfully submitted a reconciliation request to run immediately.

Creating a reconciliation schedule

You can schedule a reconciliation for account and attribute data or only for supporting data from the managed target.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a target instance.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
    a. Type information about the target in the **Search information** field.
    b. Select a target type from the **Target type** list.
    c. Select a status from the **Status** list.
5. Click **Search** . A list of targets that matches the search criteria is displayed.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. In the **Targets** table, click the icon (▸) next to the target to show the tasks. The tasks that you can do depend on the type of target.

7. Click **Set Up Reconciliation**.
8. On the Manage Schedules page, click **Create**. The Set Up Account Reconciliation notebook is displayed.
9. On the General page, type information about the reconciliation schedule. To set the maximum timeout value, enter a value in the **Maximum duration (minutes)** field. The default maximum timeout value for reconciliation is 600 minutes.
10. On the Schedule page, select a schedule interval for the reconciliation. The fields that are displayed depend on the scheduling option that you select.
11. Click **OK**.
12. Take one of the following actions:
    - Select another target task and click **Refresh** to refresh the **Targets** table.
    - Click **Close**.

Results

A message indicates that you successfully created a reconciliation schedule.

Changing a reconciliation schedule

After you create a reconciliation schedule, you can change it if necessary.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A reconciliation schedule must exist.

Procedure

To change a reconciliation schedule, complete these steps:

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Type information about the target in the **Search information** field.
   b. Select a target type from the **Target type** list.
   c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▸) next to the target to show the tasks. The tasks that you can do depend on the type of target.
6. Click **Set Up Reconciliation**.
7. On the Manage Schedules page, select the check box next to the reconciliation schedule that you want to modify and click **Change**. The Set Up Account Reconciliation notebook is displayed.

8. Change the information on the General and Schedule pages and click **OK**.
9. Take one of the following actions:
   - Select another target task and click **Refresh** to refresh the **Targets** table.
   - Click **Close**.

Results

A message indicates that you successfully updated an existing reconciliation schedule.

Deleting a reconciliation schedule

After you create a reconciliation schedule, you can delete it if necessary.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A reconciliation schedule must exist.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Type information about the target in the **Search information** field.
   b. Select a target type from the **Target type** list.
   c. Select a status from the **Status** list, and then click **Search**. A list of targets that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▸) next to the target to show the tasks. The tasks that you can do depend on the type of target.
6. Click **Set Up Reconciliation**.
7. On the Manage Schedules page, select the check box next to the reconciliation schedule that you want to delete. Selecting the check box at the top of this column selects all reconciliation schedules.
8. Click **Delete**.
9. On the Confirm page, click **Delete** to delete the selected reconciliation schedule or click **Cancel**.
10. Take one of the following actions:
    - Select another target task and click **Refresh** to refresh the **Targets** table.
    - Click **Close**.

Results

A message indicates that you successfully removed the reconciliation schedule.

Viewing reconciliation requests

You can view the reconciliation requests and their status.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a target instance and schedule reconciliations.

Procedure

To view the status of reconciliation requests, complete these steps:

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Type information about the target in **Search information**.
   b. Select a target type from the **Target type** list.
   c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▸) next to the target to show the tasks. The tasks depend on the type of target.
6. Click **View Reconciliation Requests**.
7. On the View Reconciliation Requests page, specify the search criteria and click **Search**. A list of reconciliation requests is displayed.
8. Optional: Cancel one or more reconciliation requests by selecting the check box next to a request and clicking **Cancel Request**.

Chapter 15. Resources scopes

One of the angle stones of IBM Security Identity Governance and Intelligence Data Model concern the concept of resources scopes. An IGI Administrator can act not only according to the assigned entitlements but also according to the assigned scopes on resources.

IBM Security Identity Governance and Intelligence is a platform that is based on Role Basic Access Control standard.

The access to the resources of the organization depends by the role that you have into the organization.

The role provides you the set of authorizations (the set of entitlements) needed to manage the business processes of the organization.

The role provides you a first level of authorization (what you can do).

Two persons with the same role can access the same set of functions, but can have a different action area according to a different set of resources that are assigned to them.

The assignment of resources provides you a second level of authorization (on objects you that you can manage with your role).

For a clear example, see “Employment and resources” on page 14.

The scope of a user coincides with the set of resources available for that user.

This concept can be declined in different ways, on different modules, through different operations.

The typical question about scope is: "User A has the same role of User B but User B don't see the same elements of User A".

If two users have the same role but different scopes, it's normal to have different views of the state of the system.

Main areas where scopes are involved:

- Scope for Admin Roles
- Scope for Report Designer queries
- Scope for Process Designer activities
- Scope for Certification Campaigns

Scope for Admin Roles

IBM Security Identity Governance and Intelligence provides a set of preset administrative roles.

These roles can be freely used or cloned or modified by the customer.

The customer can build other administrative roles, suitable for covering specific needs.

Through these roles, you can manage the access to different modules of the platform.

Every administrative role must be associated to a scope on following resources:

- **Org Units**
- **Entitlement**
- **Application**
- **Risk**
- **Attribute Hierarchy**

Two users with the same administrative roles but with different scopes on resources, can have a different actions area.

Table 17. Same Role - Different Scopes

Role - Scope		**Description**
User Manager (User A)	Scope on **Org Units**	The User A, in Access Requests workflow, can manage request for users into organizational units that are deployed in the scope (for example, OU1 and OU2). User A can also manage all applications available for the users of the OUs scope.
User Manager (User B)	Scope on • **Org Units** • **Applications**	The User B, in Access Requests workflow, can manage request for users into OU1 and OU2. User B can also manage a set of applications that are deployed in the scope (for example, APP1 and APP2).

The table shows a quick example of "second level of authorization": User B have the same role of User A but can act differently for a different scope on resources.

Thus, User B see only users of OU1 and OU2 involved in APP1 and APP2, while User A see all applications related to users of OU1 and OU2.

In this situation, User B see likely a minor number of users of User A.

For information about assigning the scope to an administrative role, see “Assigning an administrator role to a user” on page 165.

Scope for Report Designer queries

In Report Designer, you can configure a report based on a specific query.

You must associate every query to a specific scope that is a temporary table where is collected data useful for speed-up the run of the query.

For information about the default product scopes, see “Scope” on page 632.

For information about the join of queries to scopes, see “Query” on page 606.

Scope for Process Designer activities

Process Designer module provides a modeler capable of outlining every type of workflow for implementing custom authorization processes.

A workflow is built by a sequence of activities.

Every activity has an associated scope.

Different operating attributes (grouped under the tab **Activity scope**) determine the behavior of an activity.

All these attributes set the scope of the activity, thus the set of data model objects under the control of the activity.

For information about how to model an activity scope, see “Operating attributes” on page 375.

Two different managers with the same role (for example User Manager), associated to the same activity, are associated to the same activity scope.

Thus, they can operate on the same objects.

A clear example of activity scope setting that is related to applications, is shown in the following table:

Table 18. Visibility levels by application

Visibility type	Description
All Applications	All registered applications
Specific Applications	Group of applications that are selected by clicking **Specific Applications**
User owned Applications	Applications that are owned by the user that is involved in the management of the activity.

But if User A see only OU1 and User B see only OU2, they can act, with the same role, in the same activity, on different set of objects.

User A manage only applications that are related to users of OU1 and User B only on applications that are related to users of OU2.

Scope for Certification Campaigns

During the configuration of a Certification Campaign, you can choose different types of campaigns.

Every campaign must be associated to a certain dataset.

During the configuration of a Certification Campaign, several reviewers can share dataset.

For example, if you are considering a campaign on risks, the related dataset can host a subset of users and a subset of risks. If you have a role as Reviewer, you must have a scope S with users and risks as assigned resource.

If both resources are missing, S is an empty set, and the reviewer can't see any certification item when log in to Access Certifier.

For information about modeling a certification campaign, see "Certification campaigns" on page 239.

Chapter 16. Rules introduction

One of the angle stones of IBM Security Identity Governance and Intelligence concern the concept of rule. An IGI Administrator can write rules for different goals. Rules are used for extending the native capabilities of the product.

IBM Security Identity Governance and Intelligence provides many "point and click" functions for configuring the main capabilities.

When is needed an advanced customization of the native capabilities, you can write a rule.

A rule is a piece of Java code that is used for implementing customizations of additive business logic of a specific customer.

Rules can be also scheduled through Task Planner module.

A rule is an element with a high degree of flexibility.

The learning curve for managing rules is slow in the short period.

In the medium or long period, the maintainability and the flexibility of rules represents a real added value for any customer that adopts IBM Security Identity Governance and Intelligence.

A new rule can be deployed without stop and restart the application server.

The following table shows an estimation of how often you need to define a new rule or to update a default rule during the deployment of IBM Security Identity Governance and Intelligence, related to several components.

Table 19. Customization frequency of rules

Component	Customization Frequency
Event Queues	≈ 99%
Enterprise Connectors	≈ 0 - 90%
Access Governance Core	≈ 50%
Task Planner	≈ 50%
Access Requests work flows.	≈ 25%
Access Certifier campaigns.	≈ 2%
	≈ 1%

Note: This estimation is based on previous experiences of deployments of the product.

Rules are contained in a Rules Sequence (also known as Rules Flow).

Sequences of rules are grouped in Rule Classes.

Some classes of rules (system rules classes) have some fixed sequences, as shown in the following table:

Table 20. Rules classes

Rule Class	Module	Fixed Flow(Sequence)	Triggered by
Live Events	Access Governance Core	Yes	Events execution (with exception of creation events)
Deferred Events	Access Governance Core	Yes	Deferred Events execution (with exception of creation events)
Authorization Digest	Access Governance Core	No	Fulfillment of a certification campaign
Advanced	Access Governance Core	No	Not triggered but can be scheduled by a job of Task Planner
Account	Access Governance Core	No	Account creation
Attestation	Access Governance Core	No	Creation of a data set for a certification campaign
Hierarchy	Access Governance Core	No	Building of an attribute hierarchy
Workflow	Process Designer	No	Pre action or post action that is related to a workflow activity
Advanced	Access Risk Controls for SAP	Yes	SAP system operation

A generic fixed sequence is a sequence that is provided by default.

This type of sequence is available after the installation of the product; it cannot be modified and must be used by design.

Chapter 17. Target type administration

Target integration automates data collection from distributed target systems and reflects changes that are initiated from Identity Governance and Intelligence. Target systems are repositories for user account information.

Overview

A *target type*, also called an *adapter profile*, is a category of related targets that share schemas. It defines the schema attributes that are common across a set of similar managed resources.

Target types are templates that are used to create targets for specific instances of managed resources. For example, if you have several Lotus® Domino® servers that users need access to, you might create one target for each server by using the Lotus Domino target type.

A target type is defined in the target definition file of an adapter, which is a Java™ Archive (JAR) file that contains the profile. The target type for an adapter is created when the adapter profile is imported.

Target type administration tasks

You can do the following tasks from the Target Administration Console:

Table 21. Target type administration tasks

Task	Refer to
Import target definition files, also called adapter profiles.	"Importing target types (adapter profiles)" on page 132
Import HR feed adapter profiles as target types.	"Importing HR feed adapter profiles" on page 134
Map target type account attributes to Identity Governance and Intelligence user attributes.	"Importing the attribute map for a target type" on page 136
Define account defaults for a target type by mapping to a user attribute directly or by using JavaScript.	"Adding account defaults to a target type" on page 139
Change account defaults for a target type.	"Changing account defaults for a target type" on page 140
Remove account defaults from a target type.	"Removing account defaults from a target type" on page 141

Target definition file or adapter profile

A *target definition file*, also called an *adapter profile*, defines the type of managed resource that IBM Security Identity Governance and Intelligence can manage.

The target definition file creates the target types for IBM Security Identity Governance and Intelligence.

The target definition file is a Java archive (JAR) file that contains the following information:

- Target information, including definitions of the account provisioning operations, such as add, delete, suspend, or restore.
- Target provider information, which defines how IBM Security Identity Governance and Intelligence communicates with the managed resource.
- Schema information, including the LDAP classes and attributes.
- Account and target forms and the label for the attributes for creating targets and requesting accounts on those targets. They are displayed in the user interface.

Importing target types (adapter profiles)

As an administrator, you can import a target definition file, which creates a target type in Identity Governance and Intelligence.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

The file to be imported must be a Java archive `.JAR` file. You can create a target type for an adapter that provides a `.JAR` file.

About this task

Target definition files are also called adapter profile files, which are provided with the various Identity Brokerage Adapters. The adapter profile is required because it defines the types of resources that the Identity Governance and Intelligence server can manage.

The adapter profile is used to create an adapter service on the Identity Governance and Intelligence server and to establish communication with the adapter. If the adapter profile is not installed, you cannot manage the targets. Import the adapter profiles to create target definitions for the targets.

This task can be completed from the Target Administration Console. To import a target type, complete these steps:

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration Console is displayed.
3. From the navigation tree, select **Manage Target Types**. The Manage Target Types page is displayed.
4. On the Manage Target Types page, click **Import**. The Import Target Type page is displayed.
5. On the Import Target Type page, complete these steps:
   a. In the **Target Definition File** field, click **Browse** to locate the file. For example, if you are installing the IBM Security Identity Governance and

Intelligence adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file. The adapter profiles are in the target cache.

   b. Click **OK**. A message indicates that you successfully imported a target type.

6. Click **Close**.

Results

The import occurs asynchronously, which means it might take some time for the target type to load into IBM Security Identity Governance and Intelligence from the properties files and to be available in other pages. On the Manage Target Types page, click **Refresh** to see the new target type. If the target type is not displayed in a reasonable amount of time, check the log files to determine why the import failed.

What to do next

When the adapter profile is successfully imported, you need to import the attribute mapping definition file. See “Importing the attribute map for a target type” on page 136.

Next, configure the account defaults for the target type. See “Adding account defaults to a target type” on page 139.

After the target type is imported and configured, create a target that uses the adapter profile. See “Creating targets” on page 144.

If you cannot create a target with the adapter profile or open an account on an existing target, the adapter profile was not installed correctly during the import. You must import the adapter profile again.

Identity Adapters

⇨ http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Before you begin

Before you complete this task, 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

About this task

The **USER_ADD** flow process does not include the **Generate Unique UserID** rule by default. You must manually add the **Generate Unique UserID** rule before you can successfully import HR feed data.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Click **Configure** > **Rules** > **Rules**.
4. In the **Rules** tab on the left pane, complete the following fields:
   a. In the **Rule Class** field, select **Live Events**.
   b. In the **Queue** field, select **IN**.
   c. In the **Rule Flow** field, select **USER_ADD**.
5. In the **USER_ADD** flow process, expand and select the **User Add default group** folder for the rule group.
6. In the right pane, expand **Rules Package**.
7. In the **Rules Package** pane, select **Generate Unique UserID**.
8. From the **Actions** menu, click **Add**. In the left pane, **Generate Unique UserID** is displayed in the rule group that is named **User Add default group**.
9. In the left pane, move **Generate Unique UserID** so it is located after **Create OrgUnit From User Data** and before **Create User**.
10. Restart the IBM Security Identity Governance and Intelligence server.
    a. On the **Appliance Dashboard** of the IBM Security Identity Governance and Intelligence virtual appliance console, locate the **Server Control** widget.
    b. Select **Identity Governance and Intelligence server**.
    c. Click **Restart**. For more information, see Viewing the server control widget.

What to do next

After you add the **Generate Unique UserID** rule, complete these procedures:

- Import the adapter profile. For more information, see "Importing HR feed adapter profiles."
- Create a target. For more information, see "Creating targets to support HR feed" on page 146.
- Reconcile the user data. For more information, see "Reconciling accounts immediately on a target" on page 119.
- Ensure that the reconciliation process is complete. For more information, see "Viewing reconciliation requests" on page 123.

Rules
Rules are used to manage different types of events or for the automation of particular policies.

Importing HR feed adapter profiles

As an administrator, you can import an HR feed adapter profile, which creates a target type in Identity Governance and Intelligence.

Before you begin

For HR feed profiles, you must first configure the rule for the unique user ID. For more information, see "Configuring the rule for the unique user ID" on page 133.

The adapter profile to be imported must be a Java archive `.JAR` file. You can create a target type for an adapter that provides a `.JAR` file. For example, you can import the profile for PeopleSoft or SAP adapters.

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

About this task

Target definition files are also called adapter profile files, which are provided with the various Identity Brokerage Adapters. The adapter profile is required because it defines the types of resources that the Identity Governance and Intelligence server can manage.

The adapter profile is used to create an adapter service on the Identity Governance and Intelligence server and to establish communication with the adapter. If the adapter profile is not installed, you cannot manage the targets. Import the adapter profiles to create target definitions for the targets.

Complete this task from the Target Administration Console. To import a target type, complete these steps:

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration Console is displayed.
3. From the navigation tree, select **Manage Target Types**. The Manage Target Types page is displayed.
4. On the Manage Target Types page, click **Import**. The Import Target Type page is displayed.
5. On the Import Target Type page, complete these steps:
   a. In the **Target Definition File** field, click **Browse** to locate the file. For example, if you are installing the IBM Security Identity Governance and Intelligence adapter for PeopleSoft, locate and import the `PeopleSoftHRProfile.jar` file. The adapter profiles are in the target cache.
   b. Click **OK**. A message indicates that you successfully imported a target type.
6. Click **Close**.

Results

The import occurs asynchronously, which means it might take some time for the target type to load into IBM Security Identity Governance and Intelligence from the properties files and to be available in other pages. On the Manage Target Types page, click **Refresh** to see the new target type. If the target type is not displayed in a reasonable amount of time, check the log files to determine why the import failed.

What to do next

When the adapter profile is successfully imported, you need to import the attribute mapping definition file. See "Importing the attribute map for a target type" on page 136.

After the target type is imported and configured, create a target that uses the adapter profile. See "Creating targets to support HR feed" on page 146.

If you cannot create a target with the adapter profile or open an account on an existing target, the adapter profile was not installed correctly during the import. You must import the adapter profile again.

Related tasks:

"Creating targets to support HR feed" on page 146
Create an instance of a target from an HR feed profile, such as PeopleSoft or SAP.

Identity Adapters

➡ http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm

Importing the attribute map for a target type

You can map the Identity Brokerage Adapters account attributes with the Identity Governance and Intelligence system attributes.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

If the adapter package contains a mapping definition file and is specified as a requirement in the guide, complete this task after you import the target type (adapter profile). The imported file must be a DEF file. For more information, see these topics:

- "Importing target types (adapter profiles)" on page 132
- "Importing HR feed adapter profiles" on page 134

About this task

The attribute mappings for all supported adapters are configured and require no further action.

This task is required for new and custom adapters. See the *Development and Customization Guide* at http://www-01.ibm.com/support/docview.wss?uid=swg21687732 for instructions.

Note: The following information applies to HR feed adapters:

- The HR adapter packages include two attribute mapping files: one for accounts and one for groups.
- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- Attribute mapping changes might take up to 10 minutes to take effect after they are imported.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, select **Manage Target Types**.

4. In the **Target Type** table, click the icon (▸) next to the target type to show the available tasks. The tasks that you can do depend on the type of target.
5. Click **Attribute Mapping**.
6. On the Import Attribute Mapping page, click **Browse** to locate the file. For example, if you are installing the IBM Security Identity Governance and Intelligence adapter for a Windows server that runs Active Directory, locate and import the `ADprofileMapping.def` file. Or, for example, if you are using a PeopleSoft adapter profile, locate and import the `PeopleSoftHRProfileMapping.def` file.
7. Click **OK** to import the file. The import occurs asynchronously. It might take some time for the target type to load from the properties files and to be available in other pages.

What to do next

After the target type is imported and configured, create a target that uses the adapter profile. See "Creating targets" on page 144. For information about HR feed targets, see "Creating targets to support HR feed" on page 146.

Identity Adapters

http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm

Account defaults on a target type

You can define default values for account attributes either on a target or target type. This step is required only for required attributes, which are indicated in the user interface with an asterisk (*). This step does not apply to HR feed adapter profiles.

Types of account defaults

Target type account defaults
When account defaults are defined at the *target type level*, they apply to all targets of that type. However, you can override a target type default by defining an account default at the *target level*.

Target account defaults
These defaults are initially inherited from the target type account defaults, but they become local to the target as soon as it is changed. When they become local account defaults, you can change or remove them. Changes and removals do not affect the target type account defaults.

You must specify the account defaults for the required attributes of the target type. The required attributes are indicated by an asterisk (*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP.

Options for defining default values for account attributes

Basic You can hardcode default values for an account attribute.

Advanced
You can code JavaScript to retrieve data from Identity Governance and Intelligence objects and set the value for an account attribute. As a starting point, you can create a basic account default and then use the advanced option to edit the generated JavaScript.

For account defaults, you can use the JavaScript objects *subject* and *service*, where *subject* represents a user, and *service* represents a target.

The available JavaScript APIs are:

- *subject*.name returns the user name.
- *subject*.getProperty(***attributeName***) returns the user attribute value. See the list below of user attribute names.
- *service*.name returns the target name.

The following example shows the JavaScript for the **Gecos** (comments) attribute.

```
return "Account for "+ subject.name+" on "+service.name;
```

User attribute names that can be passed to the API

Below gives the list of the user attribute names you can pass to API *subject*.getProperty():

Table 22. User attribute names for use with the API

User Attribute Name	User Attribute Label
ad_ou	Active directory OU
address	Address
eraliases	Aliases
birth_country	Country of birth
locality	City
country	Country
description	Description
dn	Distinguished name
mail	E-mail address
givenname	First name
cn	Full name
sex	Gender
last_mod_user	Last Modified By
surname	Last Name
erlastoperation	Last Operation
erlocale	Locale
ownercode	Owner User ID
phone_number	Phone Number
place_of_birth	Place of Birth
ersharedsecret	Shared secret
cod_fisc	SSN/Fiscal Code
nation	State
eruri	Uniform Resource Identifier
ername	User ID
zipcode	Zip Code

Table 22. User attribute names for use with the API (continued)

User Attribute Name	User Attribute Label
attr1 ~ attr15	Custom user attribute, which can be mapped to any user data. To find out which user data **attr<*n*>** is mapped to, go to the Identity Governance and Intelligence Administration Console. Then select the Access Governance Core module. Next, select **Settings** > **Core Configurations** > **User Virtual Attributes**. Select the **UserErc** database, and then select the **Attribute Mapping** tab. For example, **attr3** is mapped to **Education**.

Adding account defaults to a target type

You can add account defaults to a target type. This task is required only for the attributes in the user interface that are marked with an asterisk (*).

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

The target type must exist. If it does not exist, you must import the profile for the target type. See "Importing target types (adapter profiles)" on page 132.

About this task

You can add default values for attributes. When you create a target instance from this target type, the account defaults for the target type are copied to the target.

You must specify the account defaults for the required attributes of the target type. The required attributes are indicated by an asterisk (*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Target Types**.
4. In the **Target Types** table, click the icon (▸) next to the target type and then click **Account Defaults**.
5. On the Select Default Attribute page, click **Add**.
6. On the Select an Attribute page, select an account attribute. Take one of the following actions:
   - Add a default value.
     a. Click **Add**.
     b. Complete the appropriate fields, which vary depending on the type of target.

   c. Click **OK**. The attribute default is added.

- Add a script that specifies a default value.
   a. Click **Add (Advanced)**.
   b. Type the JavaScript code in the **Script** field. For account defaults, you can use the JavaScript objects *subject* and *service*, where:
      - *subject*`.name` returns the user name.
      - *subject*`.getProperty(`***attributeName***`)` returns the user attribute value. See the list below of user attribute names.
      - *service*`.name` returns the target name.

      The following example shows the JavaScript for the **`Gecos`** (comments) attribute.

      ```
      return "Account for "+ subject.name+" on "+service.name;
      ```

      For information about user attribute names that can be passed to the *subject*`.getProperty()` API, see "Account defaults on a target type" on page 137.
   c. Click **OK**.

7. On the Select Default Attribute page, finish adding attribute defaults to the target type.
8. Click **OK** to save the changes and to close the page.
9. Add more account defaults or click **Close**.

Results

A message indicates that you successfully saved the account defaults on the target type.

Changing account defaults for a target type

You can change the account defaults for a target type.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Target Types**.
4. In the **Target Types** table, click the icon (▸) next to the target type and then click **Account Defaults**.
5. On the Select Default Attribute page, select the check box next to the attribute that you want to modify and take one of the following actions:

   Note: The template value for the attribute is updated in the list on the Select an Attribute page.
   - Changes the default value for the selected attribute.

    Note: If you select this option when an attribute currently has a scripted default value, the existing script is overwritten with the template value that you specify.

    a. Select **Change**.
    b. Complete the appropriate fields, which vary depending on the target type.
    c. Click **OK**.

  - Add or change the script that specifies a default value for the selected attribute.
    a. Select **Change (Advanced)**.
    b. Type the JavaScript code in the **Script** field.
    c. Click **OK**.

6. On the Select Default Attribute page, finish changing attribute defaults for the target type.
7. Click **OK**.
8. Change more account defaults or click **Close**

Results

A message indicates that you successfully saved the account defaults on the target type.

Removing account defaults from a target type

You can remove account defaults from a target type.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Target Types**.
4. In the **Target Types** table, click the icon (▸) next to the target type and then click **Account Defaults**.
5. On the Select Default Attribute page, select the check box next to the attribute that you want to remove and click **Remove**. Selecting the check box at the top of this column selects all attributes. The attribute default is removed from the list on the Select an Attribute page.
6. On the Select Default Attribute page, finish removing attributes from the target type.
7. Click **OK**.
8. Remove more account defaults or click **Close**.

Results

A message indicates that you successfully removed the account defaults from the target type.

Chapter 18. Target administration

A *target* represents a user repository for a resource, such as an operating system, a database application, or another application that IBM Security Identity Governance and Intelligence manages. For example, a managed resource might be a Lotus Notes® application, and a service can be defined for a Lotus Notes User Repository.

Overview

Targets are created from target types, which represent a set of managed resources that share similar attributes. For example, a default target type that represents Linux systems is one of the target types that is installed by default when you install IBM Security Identity Governance and Intelligence. Target types are also installed when you import the target definition files for the adapters for those managed resources.

Most targets provide an interface for provisioning accounts to users, which usually involves some workflow processes that must be completed successfully. Users access these targets by using an account on the target.

A *target owner* identifies the person who owns and maintains a particular target.

A user's profile is represented as an *account*.

Target administration tasks

Use the Target Administration Console to do these tasks:

Table 23. Target administration tasks

Task	Refer to
Create targets.	“Creating targets” on page 144
Modify targets.	“Changing targets” on page 147
Delete targets.	“Deleting targets” on page 148
Schedule an account reconciliation.	“Creating a reconciliation schedule” on page 120
Initiate an immediate account reconciliation.	“Reconciling accounts immediately on a target” on page 119
View reconciliation status.	“Viewing reconciliation requests” on page 123
Define account defaults for a target by mapping to a user attribute directly or by using JavaScript.	“Adding account defaults to a target” on page 151
Change account defaults for a target.	“Changing account defaults for a target” on page 152
Remove account defaults from a target.	“Removing account defaults from a target” on page 153
View the connection status of a target.	“Viewing the target connection status” on page 154
Test the target connection.	“Testing the target connection” on page 155
Import target definition files, also called adapter profiles.	“Importing target types (adapter profiles)” on page 132

Table 23. Target administration tasks (continued)

Task	Refer to
Define account defaults for a target type (adapter profile) by mapping to a user attribute directly or by using JavaScript.	"Adding account defaults to a target type" on page 139
Change account defaults for a target type.	"Changing account defaults for a target type" on page 140
Remove account defaults from a target type.	"Removing account defaults from a target type" on page 141

Target prerequisite

A target might have another target that is defined as a target prerequisite. Users can receive a new account only if they have an existing account on the target prerequisite. For example, Target B has a target prerequisite of Target A. If a user requests an account on Target B, the user must first have an account on Target A to receive an account on Target B.

Target status

The IBM Security Identity Governance and Intelligence server tracks its ability to make remote connections and send provisioning requests to adapters on a per target basis. This ability is reflected in the Status for each target on the Manage Targets panel. On this panel, you can also search for targets with a specific status.

The value options in the **Status** list contain status values for each target:

Active Targets that function with no known issues.

Failed Targets that encountered a problem. For example, a connection test might fail or a request was not completed on an endpoint because of a problem with making a remote connection.

Unknown
Targets that never attempted a connection test or never received and processed a request.

Creating targets

Create an instance of a target from a target type, such as the Linux profile or another adapter profile that you installed.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can create a target in IBM Security Identity Governance and Intelligence, you must create a target type. Alternatively, use one of the target types that were automatically created when you installed Identity Governance and Intelligence. You can create a target type by importing the adapter profile. Alternatively, you can add new schema classes and attributes for the target to your LDAP directory. Before you can create a target for an adapter, the adapter must be installed, and the adapter profile must be created.

About this task

The target name and description that you provide for each target are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

To create a target instance, complete these steps:

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration Console is displayed.
3. From the navigation tree, click **Manage Targets**. The Select a Target page is displayed.
4. On the Select a Target page, click **Create**. The Create a Target wizard is displayed.
5. On the Select the Type of Target page, select a target type and click **Next**.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On General Information page, specify the values for the target instance. The content of the General Information page depends on the type of target that you are creating. The creation of some targets might require more steps. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide* for the more information.
7. On the Users and Groups page, which is displayed only for LDAP targets, complete the required fields.
8. On the Authentication page, which does not display for every target type, complete the required fields.
9. On the Dispatcher Attributes page, specify information about the dispatcher attributes and click **Next** or **OK**. The Dispatcher Attributes page is displayed only for IBM Security Directory Integrator based targets.
10. On the Status and Information page, view information about the adapter and managed resource and click **Next** or **Finish**. The adapter must be running to obtain the information.
11. Optional: On the Application Information page, type a name and description for the application, and then click **Finish**.
12. Optional: Click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**. If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the target instance for a specific target type.

What to do next

Specify the account defaults for the target attributes. The required attributes are indicated by an asterisk (*). Provisioning fails for required attributes that are not defined. For example, LDAP requires the attributes **`Full name`** and **`Last name`**. For more information, see "Account defaults on a target" on page 149.

Select another target task, or click **Close**. When the Select a Target page is displayed, click **Refresh** to refresh the **Targets** table and display the new target instance.

Creating targets to support HR feed

Create an instance of a target from an HR feed profile, such as PeopleSoft or SAP.

Before you begin

For HR feed profiles, you must first configure the rule for the unique user ID. For more information, see "Configuring the rule for the unique user ID" on page 133.

Before you can create a target to support HR feed in IBM Security Identity Governance and Intelligence, you must create a target type. You can create a target type by importing the adapter profile into Identity Governance and Intelligence. Alternatively, you can add new schema classes and attributes for the target to your LDAP directory. Before you can create a target for an adapter, the adapter must be installed, and the adapter profile must be created.

About this task

The target name and description that you provide for each target are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

To create a target instance for HR feed, complete these steps:

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration Console is displayed.
3. From the navigation tree, click **Manage Targets**. The Select a Target page is displayed.
4. On the Select a Target page, click **Create**. The Create a Target wizard is displayed.
5. On the Select the Type of Target page, select an HR feed target type, such as **HR feed PeopleSoft Profile** or **SAP HR Feed Profile**, and click **Next**.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. Complete the fields on the tabs that are available for your target instance. The content of the tabs depends on the type of target that you are creating. The creation of some targets might require more configuration steps because each profile (adapter) is unique. See the adapter's *Installation and Configuration Guide*

for the more information. For example, if you are creating a PeopleSoft target, complete the fields in these tabs and click **Next**:

- **PeopleTools Profile**
- **PS Connection**
- **Dispatcher Attributes**
- **Status and information**

7. Click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

Results

If the connection is successful, a message is displayed, indicating that you successfully created the target instance for a specific target type. If the connection fails, contact the analyst who is responsible for the system on which the managed resource runs.

What to do next

Set up the reconciliation schedule, or run a reconciliation operation now. For more information, see Chapter 14, “Reconciliation management,” on page 117.

Select another target task, or click **Close**. When the Select a Target page is displayed, click **Refresh** to refresh the **Targets** table and display the new target instance.

Related tasks:

“Importing HR feed adapter profiles” on page 134
As an administrator, you can import an HR feed adapter profile, which creates a target type in Identity Governance and Intelligence.

Changing targets

You can change the information for a target instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can change a target in IBM Security Identity Governance and Intelligence, you must create a target instance.

About this task

You must specify the password when you test the target connection.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Option. Click **Refresh** to update the **Targets** table

b. Type information about the target in the **Search information** field.

c. Select a target type from the **Target type** list.

d. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

5. In the **Targets** table, select the check box next to the target that you want to change and then click **Change**.
6. Change the values for the target instance and click **OK**. The changes that you can make to the target depends on the type of target. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide*.
7. Select another targets task or click **Close**.

Results

A message is displayed, indicating that you successfully changed the target instance.

Deleting targets

Delete target instances when necessary. For example, you might delete a target instance for an obsolete application.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can delete a target in IBM Security Identity Governance and Intelligence, a target instance must exist.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Option. Click **Refresh** to refresh the **targets** table.
   b. Type information about the target in the **Search information** field.
   c. Select a target type from the **Target type** list.
   d. Select a status from the **Status** list.
   e. Click **Search**. A list of targets that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, select the check box next to the target that you want to remove and click **Delete**. Selecting the check box at the top of this column selects all target instances.

6. On the Confirm page, click **Delete** to remove the selected target instance or click **Cancel**. The targets are removed automatically from all policies that currently reference them. If all targets referenced by a policy are deleted by this operation, the entire policy is also deleted. All accounts that are related to that target are also deleted. However, they are not de-provisioned from the managed resource.
7. Select another targets task, or click **Close**.

Results

A message indicates that you successfully deleted the target instance.

Account defaults on a target

You can define default values for account attributes either on a target or a target type. This step is required only for the attributes in the user interface that are marked with an asterisk (*). This step does not apply to HR feed target instances.

Types of account defaults

Target type account defaults
When account defaults are defined at the *target type level*, they apply to all targets of that type. However, you can override a target type default by defining an account default at the *target level*.

Target account defaults
These defaults are inherited from the target type account defaults, but they become local to the target as soon as it is changed. Local account defaults can be changed or removed. Changes and removals do not affect the target type account defaults.

You must specify the account defaults for the required attributes of the target. The required attributes are indicated by an asterisk (*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP.

Options for defining default values for account attributes

Basic You can hardcode default values for an account attribute.

Advanced
You can code JavaScript to retrieve data from Identity Governance and Intelligence objects and set the value for an account attribute. As a starting point, you can create a basic account default and then use the advanced option to edit the generated JavaScript.

For account defaults, you can use the JavaScript objects *subject* and *service*, where *subject* represents a user, and *service* represents a target.

The available JavaScript APIs are:

- `*subject*.name` returns the user name.
- `*subject*.getProperty(***attributeName***)` returns the user attribute value. See the list below of user attribute names.
- `*service*.name` returns the target name.

The following example shows the JavaScript for the **Gecos** (comments) attribute.

```
return "Account for "+ subject.name+" on "+service.name;
```

User attribute names that can be passed to the API

Below gives the list of the user attribute names you can pass to API *subject*.getProperty():

Table 24. User attribute names for use with the API

User Attribute Name	User Attribute Label
ad_ou	Active directory OU
address	Address
eraliases	Aliases
birth_country	Country of birth
locality	City
country	Country
description	Description
dn	Distinguished name
mail	E-mail address
givenname	First name
cn	Full name
sex	Gender
last_mod_user	Last Modified By
surname	Last Name
erlastoperation	Last Operation
erlocale	Locale
ownercode	Owner User ID
phone_number	Phone Number
place_of_birth	Place of Birth
ersharedsecret	Shared secret
cod_fisc	SSN/Fiscal Code
nation	State
eruri	Uniform Resource Identifier
ername	User ID
zipcode	Zip Code
attr1 ~ attr15	Custom user attribute, which can be mapped to any user data. To find out which user data **attr<*n*>** is mapped to, go to the Identity Governance and Intelligence Administration Console. Then select the Access Governance Core module. Next, select **Settings** > **Core Configurations** > **User Virtual Attributes**. Select the **UserErc** database, and then select the **Attribute Mapping** tab. For example, **attr3** is mapped to **Education**.

Adding account defaults to a target

You can add default values for attributes. When you create an account for a target, the default values are provided. This task is required only for the attributes that are marked with an asterisk (*) in the user interface.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create a target instance before you begin this task.

About this task

Defaults are inherited from the target type account defaults, but they become local to the target as soon as they are changed. Local account defaults can be changed or removed. Changes and removals do not affect the target type account defaults.

A message indicates whether account defaults are already defined on the target type. If you click **OK**, the account defaults for the target type are copied to the target. You can either change the account defaults or remove them from the target. Changes and removals do not affect the account defaults on the target type.

You must specify the account defaults for the required attributes of the target. The required attributes are indicated by an asterisk (*). Provisioning fails if the required attributes are not defined. For example, the attributes *Full name* and *Last name* are required for LDAP.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Type information about the target in the **Search information** field.
   b. Select a target type from the **Target type** list.
   c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▸) next to the target to show the tasks that can be done. The tasks depend on the type of target.
6. Click **Account Defaults**.
7. On the Select Default Attribute page, click **Add**.
8. On the Select an Attribute page, select an account attribute.
9. Choose one of the following options to add the attribute default to the list on the Select an Attribute page:
   - Add a default value.
     a. Click **Add**.

    b. Complete the appropriate fields, which vary depending on the type of target.
    c. Click **OK**.
  - Add a script that specifies a default value.
    a. Click **Add (Advanced)**.
    b. Type the JavaScript code in the **Script** field. For account defaults, you can use the JavaScript objects *subject* and *service*, where:
       - `subject.name` returns the user name.
       - `subject.getProperty(attributeName)` returns the user attribute value. See the list below of user attribute names.
       - `service.name` returns the target name.

       The following example shows the JavaScript for the **Gecos** (comments) attribute.

       ```
       return "Account for "+ subject.name+" on "+service.name;
       ```

       For information about user attribute names that can be passed to the `subject.getProperty()` API, see "Account defaults on a target" on page 149.
    c. Click **OK**.

10. On the Select Default Attribute page, click **OK** when you finish adding attribute defaults to the target instance.
11. Add another account default or click **Close**.

Results

A message indicates that you successfully saved the account defaults on the target.

Changing account defaults for a target

You can change the account defaults for a target instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create account defaults for the target or target type before you begin this task.

About this task

You can change the default values for attributes. The changed default values do not affect existing accounts; they are used for new accounts that are created on the target.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Type information about the target in the **Search information** field.

   b. Select a target type from the **Target type** list.
   c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▸) next to the target to see the tasks that can be done on the target. The tasks that you can do depend on the type of target
6. Click **Account Defaults**.
7. On the Select Default Attribute page, select the check box next to the attribute that you want to modify
8. Choose one of the following options to update the template value on the Select an Attribute page:
   - Change the default value.

     Note: If you select this option when an attribute currently has a scripted default value, the existing script is overwritten with the template value that you specify.
     a. Click **Change**.
     b. Complete the appropriate fields, which vary depending on the type of target.
     c. Click **OK**
   - Adds or change a script that specifies a default value for the selected attribute.
     a. Click **Change (Advanced)**.
     b. Type the JavaScript code in the **Script** field.
     c. Click **OK**
9. On the Select Default Attribute page, click **OK** when you finish changing attribute defaults.
10. Select another account default task or click **Close**.

Results

A message indicates that you successfully saved the account defaults on the target.

Removing account defaults from a target

You can remove account defaults from a target instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create account defaults for the target before you begin this task.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.

2. From the Administration Console, select **Target Administration**.
3. From the navigation tree, click **Manage Targets**.
4. On the Select a Target page, complete these steps:
   a. Type information about the target in the **Search information** field.
   b. Select a target type from the **Target type** list.
   c. Select a status from the **Status** list and then click **Search**. A list of targets that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Targets** table, click the icon (▸) next to the target to show the tasks that can be done on the target, and then click **Account Defaults**. The tasks that you can do depend on the type of target.
6. On the Select Default Attribute page, select the check box next to the attribute that you want to remove. Selecting the check box at the top of this column selects all attributes.
7. Click **Remove**. The attribute default is removed from the list on the Select an Attribute page.
8. On the Select Default Attribute page, finish removing attributes from the target instance and click **OK**.
9. Select another account default task or click **Close**.

Results

A message indicates that you successfully removed the account defaults from the target.

Viewing the target connection status

You can view the connection status for the targets that you own on Target Administration Console.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can view a target's connection status, a target instance must exist.

Procedure

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. To view the details for each target connection, expand **Target Connection Status** (▸).
4. Optional: Change the target configuration and test the connection.
   a. Click the target name.
   b. On the Change Target page, change the settings.
   c. Click **Test Connection**.

Testing the target connection

You can test the connection for the targets that you own.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can test a target's connection, a target instance must exist.

About this task

Note: You also can test the target connection when you create or change a target with **Manage Targets** task.

If you modify a target, you must specify the password when you test the connection.

The Target Administration Console shows the connection status for all the targets that you own.

Procedure

To test the target connection, complete these steps:

1. On the Appliance Dashboard, select **Identity Governance and Intelligence Administration Console** from the **Quick Links** widget.
2. From the Administration Console, select **Target Administration**.
3. On the Welcome page, expand the **Target Connection Status** twistie (▸) to view the details for each target connection.
4. Click the target name.
5. Click **Test Connection**. A message indicates whether the connection is successful.
6. If necessary, change the target's configuration and test the connection again.

Chapter 19. Target management using Enterprise Connectors

Enterprise Connectors enable the connection between the Access Governance Core and the target system. It provides connectors that keep the Access Governance Core repository synchronized with the target system. The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications.

A connector consists of the following drivers and engine that allows it to communicate with the target system, transform, and map the data to Identity Governance and Intelligence:

- IDEAS driver

  A built-in and default driver that interfaces between the connector core and Identity Governance and Intelligence.
- Target driver

  A driver that hosts all the configuration settings, including connection parameters that are required to communicate to the target system, alike to the Identity Brokerage Adapter.
- Connector core

  The engine that performs the execution of a connector.

Identity Governance and Intelligence include out-of-the-box target drivers to support the following target systems:

- Active Directory
- CSV
- IDEAS
- JDBC
- LDAP
- SAPHR
- SAPR3
- UNIX
- WorkGroup
- XLS
- XML

Use Enterprise Connectors to integrate with target systems that the Identity Brokerage does not support. Enterprise Connectors cover connectors or target types that are not available in the Identity Brokerage Adapters, such as HR systems and CSV files.

To manage target systems by using Enterprise Connectors, the administrator must use the following modules in the Administration Console:

Enterprise Connectors

Use this module to configure a connector to monitor the connector or reconciliation status to view the connector history and the attributes in the IDEAS driver, and to configure the mapping rules.

Task Planner

Use this module to execute the connector *read to*, *write from*, or *reconciliation* external schedules that are configured in the Enterprise Connectors module.

Identity Governance and Intelligence include an out-of-the-box **Connectors** task schedule, which contains the following jobs:

ConnectorPolling4Connect
Job to process a connector *read to* or *write from* schedule.

ConnectorPolling4Reconciliation
Job to process a connector *reconciliation* schedule.

Access Governance Core

When the connector *read to*, *write from*, or *reconciliation* actions are executed, events are created and rules are applied. Enterprise Connectors use the events and rules in Access Governance Core to complete the processing of data from the target system into Identity Governance and Intelligence. Use this module to manage the target accounts and event markers to be associated with the connector during configuration.

Business Managers use the Access Requests module to review user access requests. The status of the request depends on whether the connector successfully synchronized the user entitlement with the target system.

Configuring a connector

The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications. Configure a connector to keep the Access Governance Core repository synchronized with the target system. Configuring a connector mainly involves creating a new connector profile, and specifying and configuring a target driver and channel.

1. Navigate to **Enterprise Connectors** > **Manage** > **Connectors**.
2. Click **Actions** > **Add**.
3. Select the **Connector Details** tab to create a new connector profile.
   a. Assign a name and description for the connector.
   b. Select the target system type and its corresponding target driver.
   c. (Optional) Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
   d. (Optional) Select **History ON** to save and track the connector usage.
   e. Select and set the connector properties in **Global Config**.
   f. Click **Save**.
   g. Enable the channel mode to synchronize the data between the target system and Identity Governance and Intelligence. Depending on the selected channel, the corresponding **Channel** tab is displayed.

      Enable write to channel
      Propagates every change in the Access Governance Core repository into the target system.

      Enable read from channel
      Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

Enable reconciliation
Synchronizes the modified data between the Access Governance Core repository and the target system.

4. Select the **Driver Configuration** tab to set the target driver's properties that are required to communicate to the target system, such as connection details, and data transmission format.

   The **Events Marker** represents the target system that is linked by the target driver as the sender or recipient of events to or from Identity Governance and Intelligence. Event markers are defined in the Access Governance Core module **Manage** > **Accounts**. Each marker is closely associated to the account that is linked with an application. With an exception for the IDEAS event marker, an event marker cannot be associated with more than one target driver.
5. Select the **Driver Attributes List** tab to view the list of attributes that are retrieved from the target system. This list provides the meta-object that represents the target object to use during the mapping.
6. In the **Channel** tab, configure the enabled channel mode.
   - Map the attributes, if available. Set the mapping from the target object fields and the Identity Governance and Intelligence object fields. See “Mapping attributes.”
   - Define the **Pre Mapping Rules**, **Post Mapping Rules**, **Response Rules** if applicable. See “Managing Pre Mapping Rules, Post Mapping Rules, or Response Rules” on page 160.
7. After the configuration, go to the **Connector Details** tab and click **Enabled** to allow the connector to be scheduled in the target system.

Importing and exporting connector definition files

Import or export the connector definition file as an XML file to reuse objects from one environment to another. For example, you can test the connector from the test environment and then export and import it to the production environment.

The XML file name format is

```
ConnectorName.dd_mm_yyyy hh.mm.ss.xml
```

1. Navigate to **Enterprise Connectors** > **Manage** > **Connectors**.
2. Select a connector.
3. To import the file, click **Actions** > **Import**. The Import connector XML dialog is displayed.
4. To export the file, click **Actions** > **Export**.
5. Browse for the file.
6. Click **OK**.

Mapping attributes

Mapping attributes is necessary to synchronize the data objects between the Identity Governance and Intelligence Access Governance Core repository and the target system.

1. Navigate to **Enterprise Connectors** > **Manage** > **Connectors**.
2. In the **Channel** tab, click **Mapping**. The **IDEAS Objects** dialog is displayed.
3. Select the Identity Governance and Intelligence data object to match with the target system and click **OK**. The list of attributes from the Access Governance Core repository and from the target system are displayed.

4. In the **IDEAS** or **TARGET** pane, select the check box and click the **Source** button that corresponds to the attribute to be mapped.
5. In the **IDEAS** or **TARGET** pane, click the **Destination** button that corresponds to the attribute to be mapped. The mapped attributes are displayed in the **IDEAS** or **TARGET** pane, depending on whether **Channel-Write To** or **Channel-Read From** is enabled.

Managing Pre Mapping Rules, Post Mapping Rules, or Response Rules

Use **Pre Mapping Rules** to manage data that are coming from the target system before mapping the data to an Identity Governance and Intelligence attribute.

Use **Post Mapping Rules** to manage data from the target system after mapping the data to an Identity Governance and Intelligence attribute.

Use **Response Rules** to manage data that are coming in to Identity Governance and Intelligence as feedback from the target system. The Response Rules section shows the outcome of the action that is run on the target, so you can view the status of the target after the completion of a particular action. To learn the result of an operation, you need a rule that handles the results of the procedure. This type of rule helps you control the objects that are addressed by the rule.

1. Navigate to **Enterprise Connectors** > **Manage** > **Connectors**.
2. Select a connector from the list.
3. In the **Channel** tab, click **Pre Mapping Rules**, **Post Mapping Rules**, or **Response Rules**, whichever is applicable.
4. To import existing rules
   a. On the left pane, click **Actions** > **Import**.
   b. On the Import Rule Class/Flow window, select whether to import **Rule Class** or **Rule Flow**.
   c. Specify whether to preserve the old data.
   d. Browse for the file.
   e. Click **OK**.
5. To define a new rule
   a. On the right pane, click **Actions** > **Create**.
   b. Specify a rule name and description.
   c. Use the **Functions** to set the conditions and actions' structure.
   d. Select the events, operations, variables, and other required Java objects from **Ideas** > **Bean** or **Ideas** > **Action** subfolders.
   e. Click **Actions** > **Add**.
   f. Click **Save**.

   Example of a Pre Mapping Rule `parse DATE_OF_BIRTH`

```
when
  event : Event(  )
then

        String attributeName = "DATE_OF_BIRTH";

        DataBean dBean = event.getBean();
        String dateString = (String) dBean.getCurrentAttribute(attributeName);

        if (dateString != null) {
                SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");

                try {
                    Date date = format.parse(dateString);

                    dBean.setCurrentAttributeValue(attributeName, date);
                } catch (Exception e) {
                    log.error("DATE_OF_BIRTH wrong fromat");
                    dBean.stripCurrentAttribute(attributeName);
                }
            }
```

Scheduling the *read to* or *write from* functions

The *read to* function is required to import data from the target system to the Access Governance Core repository.

The *write from* function propagates every change in the Access Governance Core repository into the target system.

To view or set the schedule for the **read to** or **write from** between the connector and the target system, complete these steps:

1. Navigate to **Enterprise Connectors** > **Monitor** > **Connector Status**. Only the enabled connectors in **read to** or **write from** mode are displayed.
2. Select the connector.
3. In the **Connector Status Details** tab, select the preferred scheduling option.

   Local Scheduling
   If selected, set the scheduling details such as **Frequency** and **Date**, and whether to run the schedule immediately.

   External Scheduling
   If selected, the schedule is configured and run through Task Planner.
4. Click **Save**.

Scheduling the *reconciliation* function

The *reconciliation* function is required to synchronize the modified data between the Access Governance Core repository and the target system. To view or set the schedule for the **reconciliation** between the connector and the target system, complete these steps:

1. Navigate to **Enterprise Connectors** > **Monitor** > **Reconciliation Status**. Only the enabled connectors in **reconciliation** mode are displayed.
2. Select the connector.
3. In the **Reconciliation Status Details** tab, select the preferred scheduling option.

   Local Scheduling
   If selected, set the scheduling details such as **Frequency** and **Date**, and whether to run the schedule immediately.

   External Scheduling
   If selected, the schedule is configured and run through Task Planner.
4. In the **Advanced Settings**, select the reconciliation mode and the data to use.
5. Click **Save**.

Viewing the connector history

To view the status history of the scheduled *read to*, *write from*, or *reconciliation* jobs, complete these steps:

1. Navigate to **Enterprise Connectors** > **Monitor**.
2. Select **Connector Status** or **Reconciliation Status**, where applicable.
3. Select the connector name.
4. Click **Connector History**.

Viewing the attributes

To view the list of attributes for each data object managed in Identity Governance and Intelligence, complete these steps:

1. Navigate to **Enterprise Connectors** > **Settings** > **IDEAS Driver**.
2. Click on one of the listed items and expand it.

Viewing and scheduling the connector *read to*, *write from*, or *reconciliation* jobs

1. Navigate to **Task Planner** > **Manage** > **Tasks**.
2. Click **Connectors**.
3. Click **Jobs** to view the available jobs, and click **Actions** to add, remove, or sort the job priority.

   ConnectorPolling4Connect

   Job to process a connector *read to* or *write from* schedule.

   ConnectorPolling4Reconciliation

   Job to process a connector *reconciliation* schedule.
4. Click **Scheduling** to set the iteration number, frequency, and start date of the job.

Chapter 20. User administration

Identity Governance and Intelligence administrators use the Administration Console to do user administration tasks, such as adding users to the system.

User administration tasks

Use the Administration Console to do these tasks:

Table 25. User administration tasks

Task	Refer to
Add a user to the system	"Adding a user"
Configure user access	"Configuring user access to Service Center applications" on page 164
Assign an administrator role to a user	"Assigning an administrator role to a user" on page 165
Extend the UserErc table with extra columns to import more user data from another system	"Adding columns to the UserErc table" on page 165
Populate the data model	"Creating a bulk load operation" on page 89

Related information:

"Users" on page 175
You can define and manage users and items that are associated to them, such as entitlements, resources, accounts, rights, mitigations, events, and activities.

Adding a user

Complete this task to register a new user into the Identity Governance and Intelligence data model.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Manage** > **Users**.
4. In the **Users** tab, click > **Actions** > **Add**.
5. In the **Details** tab, define a basic User profile. Specify information in the following fields and in the other fields, if applicable. See the related help topic for the options and their descriptions.
   - First Name
   - Last Name
   - Master UID
   - OU Master
6. Click **Save**.
7. In the Password window, create the password for the User.
8. Click **Ok**.

Related information:

"Users" on page 175
You can define and manage users and items that are associated to them, such as entitlements, resources, accounts, rights, mitigations, events, and activities.

Configuring user access to Service Center applications

Complete this task to enable Users to access the Application in Service Center. These Applications must be properly configured. Users must have the right Roles to access one or more Application.

About this task

Being authorized to access an Application does not imply that you can run every task available within that Application. For example, you can have the Entitlement to work with Access Certifier. However, if no configured campaigns exist, then you cannot run any campaign review in this module.

Procedure

1. Create a User. See "Adding a user" on page 163.
2. Log in to the Service Center. Use the credential of the User that you created. No applications are displayed in the Service Center landing page.
3. Assign a Role to the User. See "Assigning an administrator role to a user" on page 165.

Option	Description
User Manager	The user can view and access the following applications: • Reports • Access Certifier • Access Requests **Note:** A diagnostic message is displayed when the Access Requests application is not correctly configured.
Application Manager	The user can view and access the following applications: • Business Activity Mapping • User-account matching **Note:** In particular, because the applications are linked to an account, the accounts that can be managed in User-account matching depend on the application scope.
Risk Manager	This role is required to manage several activities in the Access Requests workflows.
Employee	This role is required to manage several activities in the Access Requests workflows.
Reviewer Supervisor	This role is required in Access Certifier.
Redirection Approver	This role is required to manage authorization requests that are redirected by the user with the role that was assigned in Process Designer. The users to whom the request can be redirected have this role and are specified in the **Redirect Scope** tab of the underlying WorkFlow process activity.

4. Log in to the Service Center. Use the credential of the User you created. All applications are displayed in the Service Center landing page.

Related information:

"Admin roles" on page 249
Admin roles are used to manage IBM Security Identity Governance and Intelligence applications.

Assigning an administrator role to a user

Complete this task to assign an administrator role to a User.

About this task

A set of default administrative roles are provided at installation to help ease the configuration of the other Identity Governance and Intelligence features. New roles can be added and the role structure can be modified. However, the modification of administrative roles must be done by an expert administrator.

Procedure

1. Log in to the Administration Console.
2. Click **Access Governance Core**.
3. Select **Configure** > **Admin Roles**.
4. In the **Flat View** tab, select one of the administrator roles.
5. Access the **Users** tab, click **Actions** > **Add**.
6. In the Add Users window, select one of the registered users and click **OK**.
7. Optional: In the Date Selection window, set the validity period of the assignment and click **OK**.
8. In the Resources window, define the scope specified for the selected administrator role by selecting entries from the table and selecting the **Add** and **Remove** icons.
9. Click **OK**.

Related information:

"Resources" on page 236
Describes how to manage resources.

Adding columns to the UserErc table

You can extend the UserErc table with extra columns to import additional user data from another system.

Before you begin

This task consists of two steps:

1. Adding the columns in the USER_ERC table in the Identity Governance and Intelligence database.
2. Mapping the new attributes in the UserErc repository in Access Governance Core.

To complete this task, you must be an Identity Governance and Intelligence administrator.

About this task

The UserErc repository contains user data that is imported from an external system through an Identity Governance and Intelligence enterprise connector. The columns of the repository are mapped in the users table of the Access Governance Core database. The columns follow the specifics that are defined through user virtualization in Access Governance Core.

The attributes of the UserErc repository correspond to the columns of the USER_ERC table in the database. If you need extra columns to take in external data, follow this procedure.

Procedure

1. Add the new column to the USER_ERC table in the database.

   On Oracle:

   a. Use `sqlplus` to connect to user IGA_CORE.

   b. Run the following command:

   ```
   alter table USER_ERC add new_column_name VARCHAR2(512 CHAR);
   ```

   where *new_column_name* is the name of the column you are adding. For example, to add column HIRED_ON, run:

   ```
   alter table USER_ERC add HIRED_ON VARCHAR2(512 CHAR);
   ```

   On DB2:

   a. Use `clpplus` to connect to user `igacore`.

   b. Run the following command:

   ```
   alter table USER_ERC add new_column_name VARCHAR(512);
   ```

   where *new_column_name* is the name of the column you are adding. For example, to add column HIRED_ON, run:

   ```
   alter table USER_ERC add HIRED_ON VARCHAR(512);
   ```

2. Log in to the Administration Console.
3. Select **Access Governance Core**.
4. Select **Settings** > **User Virtual Attributes**
5. Select the **UserErc** repository in the left pane, and click **Attribute Mapping** in the right pane.
6. Click **Actions** > **Add**. The Select attribute to add window is displayed.
7. Scroll down, select the attribute name that corresponds to the column you added in the USER_ERC table, and click **Ok**. The new attribute is added on top of the **Name** column in the Attribute Mapping pane.
8. Proceed to add a label and to complete the mapping for the new attribute.

Results

The new attribute is displayed with the user external data in the **Manage** > **Users** window of Access Governance Core.

Related information:

"User virtual attributes" on page 325
Access Governance Core supports a policy for linking user data from external sources. This policy is called virtualization.

Chapter 21. Introduction to Access Governance Core

Access Governance Core (AG Core) is the central IBM Security Identity Governance and Intelligence module, dedicated to the implementation of the authorization processes.

It creates a centralized authorization system based on the role-based access control (RBAC) model, as defined by the Standard ANSI/INCITS 359-2004.

The key consideration is a user's role within an organization. Based on that role, the user is assigned the authorization to use specific organization resources and functions.

The Access Governance Core assigns to users, specific authorization profiles and oversees the management their lifecycles.

Access Governance Core provides a modeler that systematically outlines the current structure of an organization's organizational and technical components. The outline or organizational description is called a realm. It is implemented by a database that literally photographs how the company is structured, in terms of its organization units, users, resources, and applications.

Based on this description, an authorization profile is built for each user within the organization. The profile determines what a user can do within the realm, what resources can be accessed, and what operations can be performed on these resources.

The definition of an authorization profile intrinsically introduces rules that control the visibility of objects that are described in the realm. It makes only those applications, functions, and resources that are outlined in the user's profile accessible to the user.

A special feature in the Access Governance Core allows for multi-Realm management. You can define the management of multiple organizations and maintain their separate contexts that relate to different realms.

The Access Governance Core flexible architecture can integrate easily within existing IT architectures. Its scalable functions allow it to manage its progressive introduction within the host system.

AG Core Architecture

To understand the AG Core architecture, study the following outline. It specifies the essential highlights of each component module.

The AG Core comprises the following elements:

- Administration Module
- Security API
- WSDL Interface
- EJB Layer
- DAO Layer

- DB (Identity Repository)

Administration Module

The Administration module allows the complete management and configuration of AG Core. It is used to outline the Realm. It populates the organizational model under examination and defines entitlements for users who are a part of it.

The Administration realm, REALM 0, is always present. It contains the list of all administrators and their relative authorizations.

One or more administrators can be defined inside each realm. Each administrator can have a different degree of visibility to the entire realm or just one part of it, and a different set of functions to manage. The interface is multilingual.

Security API

Security APIs provide tools for implementing a set of security services that cut across the entire AG Core architecture. They can be employed within any application client, serving to access the AG Core and its prerogatives.

Specifically, security APIs allow for the implementation of authentication policies that present varying degrees of resistance, based on different outlines that define the required security level.

Traditional authentication outlines are available that are based on a user name and password or advanced ones that are based on compliant smart cards PKCS11 and digital certificates X.509.

Available Java classes enable the management of the following security items:
- The authentication phase
- The security contexts that are related to entities that are logging on AG Core
- The security tokens that are involved in AG Core transactions
- The SAML communication standard.

WSDL Interface

This part of the architecture allows for a set of web services to be exposed externally, which implements the same methods made available by the Security APIs.

Due to the nature of this technology, based on standards such as SOAP and XML, these services are available from any client web service consumer, without any platform limitations.

The APIs are available in both JAVA and .NET versions.

EJB Layer

AG Core is entirely developed by using J2EE-EJB technology. To optimize performance, EJB–stateless sessions were employed. However, it is impossible to trace users who are calling an EJB method or to know whether they are authorized to do so. Management of these sessions is not possible.

The solution to the problem is the use of an XML token. It is signed and even encoded in some of its parts that contain a definition of the permission user. The token is created during the login phase, by using security APIs, and is populated with data from the user who requested access. After it signed and eventually encoded, the token is given back to the caller application.

Every EJB method that differs from the login requires a token as a parameter.

The EJB reads from the token all the information that is related to the user caller. It returns the value of the method only after it ascertains that the user is authorized for the specified operation, and that the token was not modified. This security service on the EJB layer is requested when the product is installed on devices that are inadequately protected by network systems, and are exposed to external attacks.

When Access Governance Core is set up in an area that is highly protected and deemed secure, this application security mechanism can be disabled. Disabling this mechanism maximizes performance.

DAO Layer

The DAO layer allows for the uncoupling of the business logic application (EJB) and the physical structure of the database. The interrogation logic of the database is rendered independent from the underlying database management system (DBMS), for example Access, ISAM, or SQL-DB.

Database

From a logic viewpoint, the IBM Security Identity Governance and Intelligence Core database can be laid out in two main sections:

- The first section contains information for managing the realms and data for the AG Core configuration;
- The second section contains as many copies as the number of realms, the different organizations that are being managed. REALM 0 is used to define the administrators, and the authorizations that are related to them.

Each realm in the second section can be outlined and logically split into three main areas:

A description of the organization of the company

The set of applications and functions that can be provided

The resources to be accessed.

Each of these three areas can be represented by an Entities-Relations diagram that describes the tables physically present on the database, and the relationships between them.

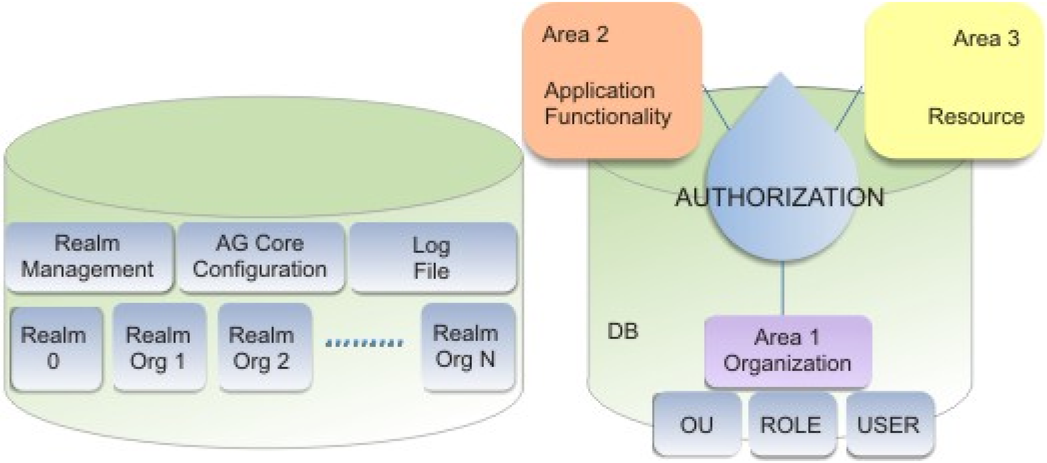


Figure 45. Logic architecture of the AG Core database

The DB is populated:

- According to indications of the realm administrator, through the administration console
- For a database with pre-existing data, the data can be transferred directly to the AG Core database, by using a set of batch procedures.

Managing the Administration Realm

The AG Core distinguishes between an administration realm and other operating realms, which can conceptually be seen as complementary components of the general model.

These realms are identified by a name that is assigned to them by the administrator. For instance, the administration realm for a regional name healthcare unit might be named `REALM_RNHCU`. An operating realm is sometimes referred to as just a realm.

The administration realm structure is identical to that of a generic realm. It comprises an application area, organizational area, and a resources area. However, it is managed differently than a generic realm since the administration realm allows for the complete management of administrators that belong to other realms.

All administrator users from other realms must be profiled in the administration realm and assigned the necessary functions to access and use the Access Governance Core. This phase represents the main point of the definition of the administration realm application area. The administrators can be assigned only a subset of the management functions that are expressed by the console, or accessible resources, or both. This subset can be customized at a single administrator level dependent upon on the privileges that are granted in a realm or subtree of the realm. The functions can be assigned either when the Access Governance Core is installed and configured, or afterward, during natural management and fine-tuning phases during the lifecycle of an organization.

The organizational area lists groups of administrators that are authorized to manage their related realms. Groups of administrators must be defined for the realms, and each of these groups is then defined within its relative OU.

Realms to be administered are represented as resource types in the administration realm. The different realms are created during the installation phase through SQL scripts.

Product Administration

During the AGCore installation procedure, an administration realm is created, along with its related super administrator, who is responsible for defining the initial customizations. In addition, the first operating realm is also created.

The super administrator can create other realms and administrator groups.

Note: All operations that are supplied by the AGC for the generic profiling of users are also used for the profiling of administrators.

Accessing the administration realm, you can manage:
- Administrators
- Realms
- Visibility or scope
- Administration roles

Administrator

An Administrator is a user that is registered as a member of an administration realm. The AG Core super administrator is created during the installation phase, whereas the other administrators must be created later. Administrators have administration privileges on their related realms.

A special category of users exists that can access privileges are assigned to the administrative realm to support the tasks of the super administrator, even in delegated mode.

Realms

Realms are configured as resource types of a particular resource family, the realms family.

In general, the administration realm includes the following content:
- A resource family called Realms.
- The number of types that belong to the realms family is the same as the number of realms that are installed. The name of the type, `TypeName` *k*, coincides with the name assigned to the realm.
- For each type, a resource that coincides with the root OU for the realm that is defined by the type. The link is implemented through the field scope, in which the root name of the realm must be entered.
- After the root OU is defined, as many other resources can be added as there are organizational units in the realm. These resources can target any OU that differs from the root, to implement the concept of limited scope.

The following figure illustrates the presence of *N* types that belong to the realms family.

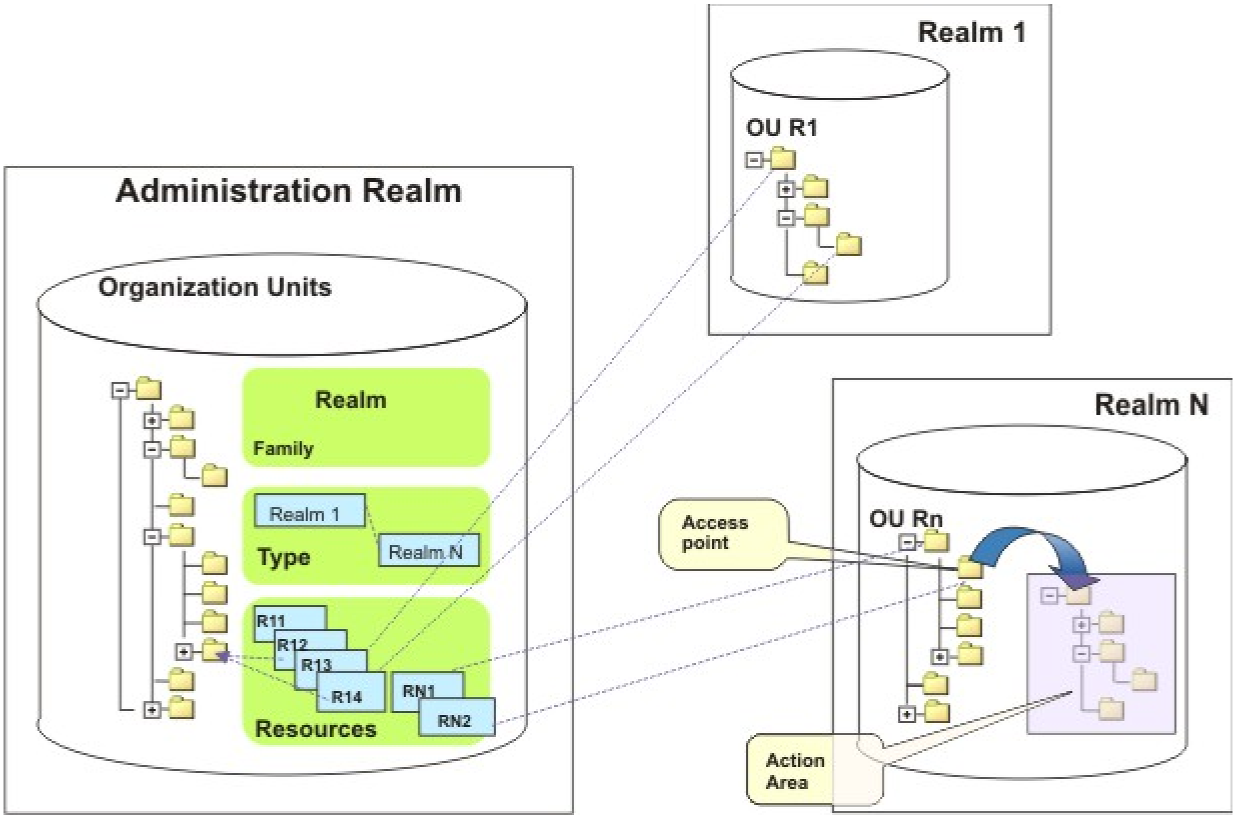


Figure 46. Operating realms as resources of the administration realm

Resources are specified for each type. Four resources are defined for realm type 1.

R11

R12

R1

R14

Two resources are defined for realm type N

RN1

RN2

Realm types 2 - *N*-1 are not visualized. The resource RN2 is an access point to the OU linked by the arrow. The subtree is visualized in the frame labels as **Action Area**.

Visibility

A generic OU in the realms tree defines a level of visibility. This visibility can be implemented by constructing an access point, scope, to the organizational structure of the realm.

Each administrator can access the organizational subtree of the realm, whose root coincides with the access point.

There can be more than one access point for every realm. Each administrator can access only one access point.

Functions that can be assigned in administration realm

The following table provides a list of all available functions on the Access Governance Core in the Administration Realm.

These functions cannot be modified, and can be assigned to roles only:

Table 26. Assignable functions

Functions	Description
CHANGE_USER_PWD	Change the user's password.
MODIFY_REALM_SETTINGS	Create, delete, and edit realm settings.
FIND_REALM_SETTINGS	Find realm settings.
MODIFY_USER	Create, delete, and edit user information.
FIND_USER	Find user information.
MODIFY_ORGUNIT	Create, delete, and edit organization units.
FIND_ORGUNIT	Find organization units.
MODIFY_ENTITLEMENT	Create, delete, and edit entitlements.
FIND_ENTITLEMENT	Find entitlements.
MODIFY_USER_ENTITLEMENT	Create, delete, and edit positions or employment of a user.
FIND_USER_ENTITLEMENT	Find positions or employment of a use.
MODIFY_ORGUNIT_ENTITLEMENT	Create, delete, and edit entitlements of an OU.
FIND_ORGUNIT_ENTITLEMENT	Find entitlements of an OU.
MODIFY_RESOURCE	Create, delete, and edit resources.
FIND_RESOURCE	Find resources.
MODIFY_ORGUNIT_RESOURCE	Create, delete, and edit resources of an OU.
FIND_ORGUNIT_RESOURCE	Find resources of an OU.
MODIFY_REALM_SETTINGS	Edit a realm configuration.
MODIFY_USER_ACCOUNT	Edit a user's account, for example, disable user, force change password, reset the last login, or reset login errors.
FIND_USER_ACCOUNT	Find data relative a user's account.
MODIFY_DELEGATED	Create, delete, and edit delegated users.
FIND_DELEGATED	Find delegated users.
MODIFY_ROLE_POLICY	Create, delete, and edit role policies.
FIND_ROLE_POLICY	Find role policies.
MODIFY_SERVICES	Create, delete, and edit services.
FIND_SERVICES	Find services.
MODIFY_USER_RESOURCES	Create, delete, and edit user resources.
FIND_USER_RESOURCES	Find user resources.
MODIFY_USER_SERVICES	Create, delete, and edit user services.
FIND_USER_SERVICES	Find user services.
MODIFY_ENTITLEMENT_SERVICES	
FIND ENTITLEMENT_SERVICES	

Table 26. Assignable functions (continued)

Functions	Description
MODIFY_APPLICATION	Create, delete, and edit applications.
FIND_APPLICATION	Find applications.

A default role, product administrator, in the administration realm is assigned all the functions previously described. Other administrative roles with limited functions can be created for administrators to whom only a subset of functions must be assigned.

Administration realm resources coincide with the access points for the realms to be administered. The realms coincide with resource types.

The resources that are access points for the roots of their realms are created automatically during the Access Governance Core installation. They are created by the SQL scripts that create the realms. The same process occurs for all the resource types that define the realms.

More Resources can be added manually, through the web console, where you might want to delegate the management of special subtrees in the realm to specific administrators. The resources represent organizational units that are roots of the subtree, whose management must be delegated.

The name of each resource type coincides with the name of the realm it represents.

The name of each resource identifies an access point, but doesn't need to coincide with the name of the OU whose subtree is being accessed. The specific selection of the OU is made by entering the OU name in the scope field in the resources data.

To be assigned to an administrator, a resource must first be assigned to the administrator's OU.

Two options are available for assigning resources to OUs:

Inheritability
If a resource represents the access point to a realm, is assigned to an OU, all administrators with a role in OU inherit the access privileges of the realm.

Hierarchy
Every resource that is assigned to the OU selected is automatically assigned to all child OUs of the OU.

The two options are not mutually exclusive.

If you decide not to use the inheritability option, the resources must then be assigned manually to users in the OU. However, different resources can be assigned to different users. This type of assignment is known as prompt.

Two administrators on Realm N represent two users who can potentially operate in the entire Realm N. By using prompt, you can assign them two different resources that provide them with two different access points. They act in different operating areas or subtrees in Realm N.

All resources for the administration OU are assigned through inheritability. Each resource that corresponds to each realm root is assigned to the administration OU with the restriction that each user in the administration OU has visibility to all the realms.

It is possible to define groups of administrators in the administration realm.

By creating an OU for each group and then by assigning resources to the defined OUs by inheritability, each user in the group acquires properties specific to the group. Every user that joins the OU inherits the resources of the OU, and has the same access privileges as all the other users in the OU.

Two resources that represent different scopes must not be assigned to the same user on the same realm. Creating two different access points on the same realm for the same administrator creates a conflict.

Two resources that represent different scopes must not be assigned through inheritability to the same OU on the same realm. The only way to create two different access points on the same Realm is to use prompt to assign the resources. One resource is assigned to one administrator and the other resource is assigned to the other administrators.

Manage

You can manage the main entities in the Access Governance Core module.

- “Users”
- “Groups” on page 193
- “Roles” on page 201
- “Applications” on page 209
- “Accounts” on page 225
- “Resources” on page 236

Users

You can define and manage users and items that are associated to them, such as entitlements, resources, accounts, rights, mitigations, events, and activities.

The pane on the left lists the defined users and a number of attributes. Click **Filter** button to list only specific users. The following fields are available to narrow your search:

Table 27. Available filters to list users.

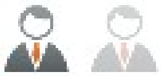
Filter	Description
User Type	Click the arrow and select one of the users types listed. The user type is defined in your security model.
UME	Flag this check box if the users you are searching have more than one account on the same target system.
Search Identity	Enter the name, the surname, or the master UID of the user.

Table 27. Available filters to list users. (continued)

Filter	Description
Associated	If checked, the search result shows only users that are associated with a Group. If not checked, the search result shows only users that are not associated with any Group (for example, when a user is in the database but not yet associated with any Group). **Note:** A user search that is run before the user is associated to an OU identifies the user only if the **Associated** check box is not checked.
Groups	Click ... **Browse** to choose the Group of the user.
Hierarchy	If this check box is flagged, the search starts from the root Organization Unit that is selected in the **Groups** field and is run on all the hierarchy.

Users are displayed in the Users list with the following symbols:

User enabled/disabled



UME User enabled/disabled

AG Core can manage various active access keys to applications that are assigned to the same user on a target system.

User name and password are typical examples. Such credentials are typically the registration and administration keys that are managed as multiple keys assigned to the same user.

A user who is associated to two or more access keys is called a User Multiple Entry (UME) User.

In the left frame, click **Actions** to run the following tasks on a selected user (excepting **Add**):

Table 28. Available actions on a selected user.

Action	Description
New UME	Defines an extra access key for a selected user. As you select this action, the Details pane for the user is displayed in `edit` mode, where you can enter a new Master UID. The current MASTER UID is displayed as the Parent UID.

Table 28. Available actions on a selected user. (continued)

Action	Description
Show UME	Lists the selected user in multiple rows (one row per access key defined) in the Users list on the left. The Details views corresponding to the rows that follow the first row, list the first Master UID of the user as the Parent UID. Click **Search** to refresh the Users list when you are done.
Fulfillment	Displays an Entitlements Details window with a list of External roles that are defined for a selected user. For every permission granted to the user, you can verify the status, the date, and the party who granted the permission.
Add	Adds a user to the AG Core repository. When you add a user, the **Master Account**, is automatically created. See Accounts.
Remove	Removes a user from the AG Core repository.

For information about the procedure, see "Adding a user" on page 163.

The content of the right frame changes depending on the tab that is selected in the upper side of the frame. When you click **Manage** > **Users**, the **Details** tab is shown by default. Under this tab are two distinct accordion panes (click the title bar to expand each pane):

Details
: As you select a user, shows the user's data that is defined in the AG Core database.

Data
: Displays data (about the selected user) that is contained in external repositories.

You can view or modify the following details for a selected user in the Details pane:

Table 29. User details

Detail	Description
User Type	Indicates the type of the User. Click ⋯ **Browse** to view the choices that are provided in the User Types window. This data can be used to indicate the level of the user, such as user manager or security officer. For external users, it indicates the type of relationship with the organization, for example business partner, customer, or supplier.
OU Master	The Organization Unit to which the user belongs.

Table 29. User details (continued)

Detail	Description
Master UID	The Univocal identifier of the user.
System UID	*To be defined.*
Identity UID	*To be defined.*
Account Expiration	Indicates the expiration date of the User account. It is entered automatically based on the settings that are defined in the Accounts section. It can be modified by the Administrator.

Note: The **User details** pane contains other user information such as: name, email, phone number, the Distinguished Name, SSN/Fiscal Code, gender, date and place of birth, address, city, state, country, and ZIP/Postal Code.

If you update the details, click **Save** for confirming the updates.

You can transfer a user from one OU to another, or assign a newly registered user to an OU.

The entitlements that are aggregated to the user during the transfer process are automatically managed.

Selecting **OU Master**, click the ellipsis (...) to display the User Transfer window where, in **View** tab, you can select an OU and then click **Actions** > **ToggleMngr** > **OK** to assign the user to the selected OU.

If you click OK on a confirmation window, you are presented with the following choices:

Assign only default entitlements
The user loses all previously assigned permissions and receives only the default entitlements in the new OU.

Assign all compatible entitlements
The user loses all permissions that are not associated with the new OU. However, the user maintains the entitlements that are common to the two OUs. At least, the user is assigned the default entitlements of the new OU.

The other tabs that you can click are:
- Entitlements
- User Resources
- Accounts
- Rights
- Mitigation
- Events
- Activities

Related tasks:

"Adding a user" on page 163
Complete this task to register a new user into the Identity Governance and Intelligence data model.

Entitlements

Use the **Entitlements** tab to assign or delegate entitlements.

In the **Entitlement** tab you can select two accordion panes:

- **Assigned**
- **Delegated**

The **Assigned** pane shows the entitlements that are permanently assigned to the user in two modes:

- A tree view where the entitlements are listed hierarchically by application (displayed by selecting **View**).
- A plain list of the entitlements that are ordered by name (displayed by selecting **Search**).

You can filter entitlements, according to filters indicated in the following table.

Table 30. Entitlement filters

Filter	Description
Group	The name of a specific group that is hosted by the hierarchy
Type	The entitlement type. It can be one of the following • Permission • IT Role • Business Role • External Role
Application	The application name.
Name or Code	Entitlement name/code.

Click **Actions** to display the following items:

Add Delegated
Adds the entitlements of a selected user in the left frame to another user that acts as the delegate of the selected user.

View Delegated
Shows all the delegated users of the user that was selected in the left frame.

Hierarchy
Shows information about the hierarchical structure of the selected entitlement.

Fulfillment
Shows the information that is related to the status of fulfillment of the selected entitlement.

Add
Adds an entitlement to the selected user.

Remove
Removes an entitlement from the selected user. You can use the [Ctrl] or [Shift] keys for multiple selections.

Note:

If you remove the association with a Business Role (IT Role) that hosts a required attribute permission, a specific sequence of actions is performed by the system:

1. The attribute permission is published (if not previously published).
2. The attribute permission is added, if not already present, to the organizational unit of the user, in visibility violation (if already present, the visibility violation attribute is absent).
3. Assign the attribute permission directly to the user.

A *required* attribute permission, directly associated to a user, cannot be removed (a diagnostic message is shown through the user interface).

The entitlements that are assigned to the selected user are listed according to the entitlement properties described in the following table.

Table 31. Entitlement properties

Property	Description
VV	An entitlement is in VV when it is not associated to the OU but you assign it to a specific user of that OU. The entitlement is not available to the other users of the OU.
Name	Entitlement name.
Application	Application name that is related to the selected entitlement.
Group Name	Name of a specific group that is hosted by the hierarchy indicated in the column **Hierarchy**
Group Code	Code of a specific group that is hosted by the hierarchy indicated in the column **Hierarchy**
Hierarchy	Name of the Attribute Group Hierarchy which involving the Entitlement
Start/End Date	The start or end date of the entitlement validity period.
Creation Date	The date that the entitlement was assigned to the selected user.
Originator	The code that indicates who assigned the entitlement to the selected user.
Delegator Code	The code of the user that is the delegator.

The assignment of an entitlement to a user can have an optional validity period.

If this period is set, the entitlement is valid after the start date and remains valid up to end date, when the assignment expires.

These dates can be set during the assignment.

The effective assignment of the entitlement to the user is realized by a scheduled task.

For an Add operation, you can add only the entitlements that are assigned to the Group Name entity of the selected user.

When a user is assigned to an OU where is set a default entitlement, the system automatically assigns this default entitlement to the user (a green icon indicates the assignment).

When you move a user from OU A to OU B, the current behavior (managed by default rules), is to keep in OU B all entitlements held by the user in OU A.

If one or more entitlements of the user in OU A are not available into OU B, system assigns these entitlements in OU B marked as VV.

The **Delegated** pane shows the entitlements that were temporarily assigned (delegated) by another user. It displays two panels: the left one shows the identity of the delegator, while the right one shows the properties of the entitlement.

Related tasks:

"Assigning an entitlement to a user" on page 101
Complete this task to associate a new entitlement to a user.

User Resources

You can add resources to users.

A Resource is assigned to the employment of the user, through the user's entitlements.

Resources can be aggregated to a selected user in two ways:

Inherited
When a user is aggregated to an OU, the user inherits all the resources that are assigned to the OU.

Assigned
When a set of resources is assigned to an employment of a user, the user is assigned all of the resources that were assigned to the employment.

When a user is selected in the left frame, the right frame displays the following options:

- To view the resource that is already assigned to the user
- To add new resources
- To remove resources
- To check conflicts on a set of entitlements that is aggregated to a user
- To view the entitlement hierarchy.

A set of ***Resource***accordion panes is displayed that directly refers to the entities of the IBM Security Identity Governance and Intelligence Data Model:

- **External**
- **OU**
- **Entitlement**
- **Application**
- **Resource Type**
- **Resource Family**
- **Risk**
- **Attribute Hierarchy**

Resources Accordion panes

Every accordion pane has two frames.

In the left frame, you can view the user's entitlements. You can filters and search by clicking the **Filter/Hide Filter** button. You can search for entitlements by **Type**, the entitlement type, and by **Name**, the entitlement name, filters.

The **Actions** menu of the left frame, has two buttons, **Parents** and **Conflicts.**

Click **Parents** to open the Entitlement Hierarchy window that shows the hierarchy of the selected entitlement.

Clicki **Conflicts** to open the Conflict info window opens that shows the Risk tree in the **Risk info** tab. You can define Mitigation actions from the **Mitigation** tab.

To view the resources, click the **Inherited Resources** tag or on **Assigned Resources** tag in the entitlements list. The results are listed in the right frame.

Note: The inherited resources cannot be removed.

From the right frame, click the **Filter/Hide Filter** button, to filter and search resources according to the filters in the following table.

Table 32. Resources filters

Filter	Description
Family	Family of the resource.
Type	Type of resource.
Name	Name of the resource.

The **Actions** menu of the right frame, has two buttons, **Add** and **Remove**.

Click **Add** to open the Entity Resources window that shows the list of available resources. Select the resources that you want to add. You can use the [Ctrl] or [Shift] keys for a multiple selection. Click **Ok** in the window to complete the operation.

To remove an assigned resource, select the resource. Click **Remove** in the Remove Resources window. Click **Ok** to complete the operation.

Accounts

You can create and manage user accounts and set user passwords.

When a new user is entered, an account that is named `Ideas` is automatically created for this user in AG Core.

Select **Manage** > **Account** to get information on accounts.

The Accounts pane displays the list of accounts that are available to the selected user.

Every account is identified by `Configuration Name – ID Code`.

After the selection of an account, you can click **Actions** to perform one of the following actions:

Details
Provides information on the selected account.

Change Date
Displays a calendar where you can change the expiration date of the account.

Force Pwd
Forces a password change.

Suspend/Restore
Displays the Account Suspending Code window where you can suspend or restore an account.

Change Pwd
Enables the Password change action for the selected user.

Reset Login
Resets the login to the selected account.

Add Creates a User - Account association.

Remove
Removes an account that is associated with the selected user.

Accounts have expiration dates. The administrator can also suspend accounts before they expire.

The **Account Suspension Code** shows fields that describe the reasons for suspending and account:

- **Technical**
- **Security**
- **Terminated**
- **Authoritative**
- **Expire**
- **Maintenance**

Every reason has a severity that ranges 1 - 9. The severity degree can be customized based on the policies of the organization.

Accounts can be suspended for more than one reason. They are restored when all fields are reset to zero.

CAUTION:
The suspension of the Ideas master account automatically affects all of the other accounts of a user.

Click **Actions** > **Details** to see the following data:

Table 33. Account details.

Detail	Description
Applications	Applications that are associated with the account configuration
Master UID	Identifies the user on the AG Core module

Table 33. Account details. (continued)

Detail	Description
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see **Manage** > **Account**). These policies are applied for all the users that are associated to the account that expired.
Last Login	Date of the last login
Last Login Error	Date of the last login error
Number of Login Errors	Number of consecutive login errors. This value is reset to zero when a correct login is made.
Last Password Change	Date of the last password change
First Name	User name
Last Name	User surname
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user
Display Name	Personal data of the user as referred by **Master UID** .
Identity UID	Data incoming from a Target system and associated to the user who is referred by **Master UID** .
Account Attributes	A variable subset of account attributes. This subset is configured in **Manage** > **Accounts** > **Account Attributes**.

Note: In some views, only a subset of the data that is indicated could be shown.

Related concepts:

Chapter 13, “Password administration,” on page 109
Identity Governance and Intelligence administrators use the Administration Console to do password administration tasks, such as configuring the password service and changing account passwords for users.

Rights

Rights are extra attributes that are related to the permissions.

In the **Rights** tab, you can modify the value of the rights that are already assigned to a user selected in the **Users** tab.

The “Rights” on page 18 are defined by the **Key** and **Value** attributes.

Rights can be either of the following types:

- Single-value.
- Look up single-value.
- Multi-value.
- Look up multi-value.

Access Governance Core > **Configure** > **Rights Lookup** provides the setting of the lookup.

Rights are assigned to a user through the assignment of an entitlement, if the entitlement holds permissions joined to rights.

The value of the right can be set during the assignment of the entitlement.

This operation can be made mainly:

- During an authorization workflow (Access Request module)
- Through the run of rules (Rule Engine)
- When a permission is assigned to an entitlement. It is assigned to all users that hold the entitlement. Of course, the value of the right can vary for every user.
- Through a specific bulk load (see Insert Application Access).

The value of the right is set during the assignment phase.

Moreover, the values of a right can be also **fixed** or **restricted**. This last one only if you consider a right multi-value with lookup. These properties can determine dynamically the value of a right when you have the same right (R1) joined to two distinct entitlements (E1 and E2) that are assigned to the same user.

The following table shows the setting of a single right R1, joined to two entitlements E1 and E2, when these two entitlements are contextually assigned to a user.

Table 34. Functions

Right class	E1 (R1)	E2 (R1)	FIXED	RESTRICTED
Single value (SV)	V1	V2	VI XOR V2	Not applicable
Multiple value (MV)	V1, V2	V2, V3, V4	Union = (V1, V2, V3, V4)	Not applicable
SV with Lookup	**V1**, V2, V3, V4, V5, V6	V1, **V2**, V3, V4, V5, V6	VI XOR V2	Not applicable
MV with Lookup	**V1**, V2, **V3**, V4, V5, V6	V1, **V2**, V3, V4, V5, **V6**	Union = (V1, V2, V3, V6)	Any possible subset of Union.

The values in the table are an example of possible values for R1. R1 can assume different values when associated to different entitlements.

From the example, it is evident that the most flexible pattern is **MV with Lookup**.

Near the field **Value**, click ... .

In the pop-up window, select in left list the available values to set.

Click right blue arrow, thus click **Ok**.

If the right is defined as **Multi Value** multiple values are displayed in the field **Value**.

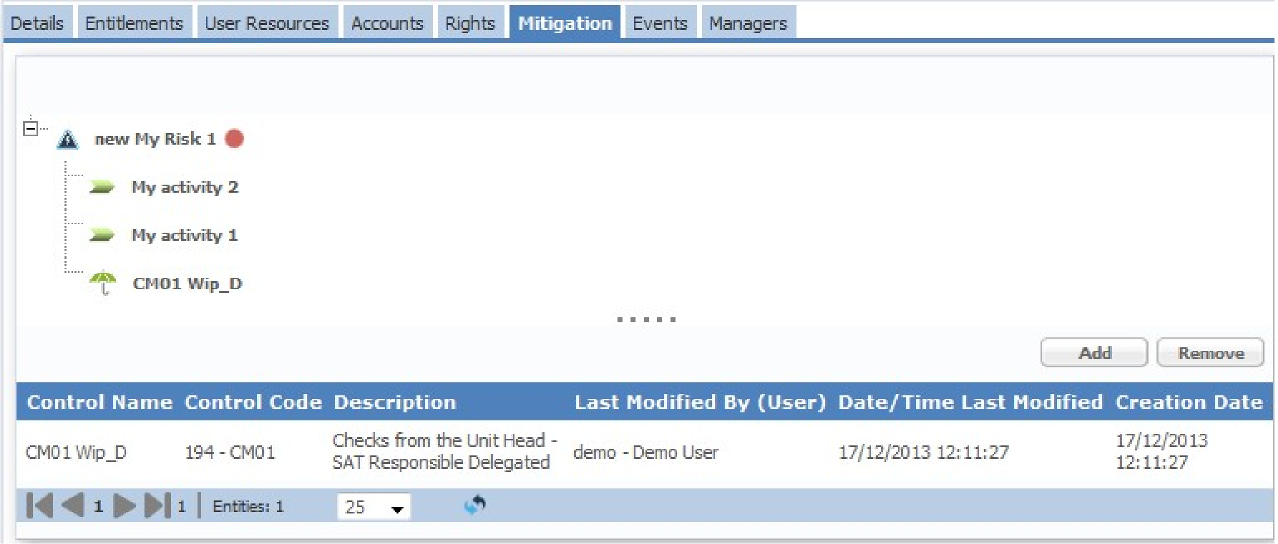
Mitigations

If a selected user is assigned a risk level, you can set a mitigation action for one or more of the at risk activities.

See Mitigation actions.

The risk information tree is displayed in the right frame. The first level displays a set of risks. The second level displays the user's at risk activities and any aggregated mitigation actions.

In the following example, an SoD risk results from a pair of activities.



Control Name	Control Code	Description	Last Modified By (User)	Date/Time Last Modified	Creation Date
CM01 Wip_D	194 - CM01	Checks from the Unit Head - SAT Responsible Delegated	demo - Demo User	17/12/2013 12:11:27	17/12/2013 12:11:27

Figure 47. Mitigation: general view

In the lower half of the right frame, the mitigations that are already assigned to the user are listed. In this example, **CM01 Wip_D**is listed.

You can add another mitigation, if any are available, by selecting the risk and clicking **Add**.

In the Appropriate Mitigations window, you can choose the mitigation and click **Ok**.

You can have a user with *N* aggregated mitigations. The number *N* is the sum of K1+K2+... K*n* mitigations that are related to different sets of at risk activities. You can remove the mitigation by selecting it and clicking **Remove**.

Events

IBM Security Identity Governance uses an integration interface to align and synchronize the data that is contained in the AG Core database with the data that is contained in the target systems.

A central role in the management of the synchronization is assigned to events.

An event is a brief yet complete description of what occurred an element in any part of the architecture. Usually the events can be generated by the AG Core itself or indirectly, by the target systems. Every time a system acts on the data, the changes are copied in appropriate packages, or events. These events are then sent to inform the other systems about that are listening.

Events are contained in appropriate tables of events, which are integral parts of the integration interface for the communication with the target systems. The AG Core communicates with the interface through events.

In the input flow, the target system that is connected to the input interface, communicates each change that is made to its data. The interface creates an event with information that is needed for the alignment, and then transmits it to the AG Core.

In the output flow, the AG Core changes the data and creates the corresponding events. It then transmits the events to the output interface, to which the related Target systems are connected. For each event, a state attribute is set to indicate the status of the event in the connection flow

An event can have one of the following states:

Unprocessed
The event was generated, but the alignment of the data is not yet performed.

Success
The alignment of the data was run successfully. An event in this state can automatically be eliminated or maintained as memory of the modification.

Error
The Event was correctly generated, but an error was detected in the alignment of the data.

You can view all the events that belong to a selected user.

The input events are shown in the IN Events accordion pane and the output events are shown in the OUT Events accordion pane.

In the IN Events accordion pane, click Filter/Hide Filter to view the set of filters that are shown in the following table:

Table 35. IN events filters

Filter	Description
Status	Event status can assume one of the following three values: • Unprocessed • Success • Error
Operation	Indicates the type of operation that is run on the external table. The following values are allowed: • Create user (directly or scheduled) • Modify user (directly or scheduled) • Delete user (directly or scheduled) • Move employee. Moves a user from one OU to another (directly or scheduled) • Custom
Account ID	Univocal identifier of the account.
Trace	Brief description of the error cause.

Table 35. IN events filters (continued)

Filter	Description
Event Start/End Date	Filters defining the time period for the search.

The set of events that are filtered is shown in a list where every event is characterized by a set of attributes. The attributes are listed in the following table.

Table 36. IN Event structure

Field	Description
ID	Event identifier.
User ERC	User identifier in the USER ERC table.
Operation	The following values are allowed: • Create User (directly or scheduled) • Modify User (directly or scheduled) • Delete User (directly or scheduled) • Move Employee (moves a user from one OU to another (directly or scheduled)) • Custom
Status	Event state can assume only three values: • Unprocessed • Success • Error
Trace	Contains the description of an error that occurred during event processing (ordinarily appears as Status = Error).
Identification Number	Contains unique information that is related to the user. For example, in the US with this parameter might be mapped the social security number (SSN).
OU Code	Indicates the unique identifier of an OU.
Action Type	This parameter usually is not used in IBM Security Identity Governance, but might be useful to interface some HR systems. For example, a SAP-HR, that provides this information after some particular actions on users. This parameter can be used even by custom business rules to define or manage some specific behaviors of the system.
Action Reason	This parameter usually is not used in IBM Security Identity Governance, but might be useful to interface some HR systems (es. SAP-HR) that provides this information after some particular actions on Users. This parameter can be used even by custom business rules to define/manage some specific behaviors of the system.
Event Date	Indicates the date of generation of the event.
Process Date	Indicates the date by which the event must be processed by the RE. Typically this date coincides with the event date but can be later if the events processing is postponed.

Table 36. IN Event structure (continued)

Field	Description
Ownership	Indicates the user database that caused the event on the external table.

Note: The fields that are indicated from free attribute 1 to *N*, depend on the target system, typically an HR system. These fields can vary widely.

In the OUT Events accordion pane, the set of filters that are shown in the following table is available.

Table 37. OUT Events filters

Filter	Description
Status	Event state can assume only three values: • Unprocessed • Success • Error
Operation	Indicates the type of operation that is run on the external table. The following values are allowed: • Add or remove functions • Add or remove delegation • Disable or enable user • Create, remove, or modify account • Change password • Add or remove service • Add or remove resource
Operation Code	Label identifying the operation.
Marker	Identifier of the Target system (toward the event is transmitted).
Trace	Brief description of the cause of the error.
Priority	Indicates a priority level for the event: • Running: the event was created during the normal operating procedures and has a higher priority. • Batch: the event was created with a lower priority. Events with the same priority level are processed in the normal order.
Event Start/End Date	Filters defining the time period for the search.

The set of events that are filtered is shown in a list where every event is characterized by a set of attributes. The attributes are listed in the following table.

Table 38. OUT Event structure

Field	Description
ID	Event identifier.
User ERC	User identifier in USER ERC table.
Operation	The following values are allowed: • Add or remove functions • Add or remove delegation • Disable or enable user • Create, remove, or modify account • Change password • Add or remove service • Add or remove resource
Status	Event state can assume only three values: • Unprocessed • Success • Error
Priority	Indicates a priority level for the event: • Running: the event was created during the normal operating procedures and has a higher priority. • Batch: the event was created with a lower priority. Events with the same priority level are processed in the normal order.
Trace	Contains the description of an error that occurred during event processing (ordinarily appears as Status = Error).
Target	Identifier of the target system to which the event is transmitted.
Free Attribute 1	Value 1.
Free Attribute 2	Value 2.
Free Attribute 3	Value 3.
...	
Free Attribute N	Value N.
Application	Application that is the object of the action relative to the event.
Operation Code	Label identifying the operation.
Event Date	Indicates the date that the event was generated.
Process Date	Indicates the date by which the event must be processed by the RE. Typically this date coincides with the event date but can be later if the events processing is postponed.

Note: The fields that are indicated from Free Attribute 1 to N, depend on the event.

You can perform two functions from the **Actions** menu on a selected event in the IN or an OUT accordion pane.

Re-Execute
Reprocess the event.

Remove
Deletes the event.

Error handling

Several types of errors can occur during the generation and processing of events.

The following list contains the main causes of errors that are associated with IN or OUT events.

- Temporary interruption of system operation.
- Errors in the structure of a rule.
- Errors that are caused by a lack of necessary data for the correct application of a rule.
- Errors due to data format incompatibilities in the data from the target system.
- Errors in the reprocessing order of events that are already in error.

A brief description of the reason for an error is contained in the **Trace** field.

General policy is to remediate an error on IN or OUT events.

Remedying an event in error means to determine the reason for the error, correct it, and finally reprocess the event through the rule engine (RE). If the cause of an error is not removed, reprocessing the event fails or new error events are generated.

The following list provides a set qualitative strategy to eliminate the causes of errors, for more commons situations:

- If the error is due to a temporary interruption in the system operation, reprocess the events in the correct order.
- If the error is due to a badly written rule, either default or custom, the rule must be corrected before you reprocess the event.
- If the error is due to the incompatibility of data to be entered with data already into AG Core, locate the error. Determine whether the error is in the AG Core data or the data from the target system. You might need to contact the target system and AG Core administrators for assistance.
- If the error is linked to sensitive data that is to be modified, also correct it in the USER ERC table. This operation is not mandatory, but keeps the data in alignment between II and AG Core.
- If the error is caused by AG Core data, it is possible to correct it directly from the AG Core Administration module. The event can be reprocessed only after the cause of the error is corrected.
- If the error is due to other error events, the previous events in error must be identified and corrected.
- If the reprocessing of an event generates of new error events, these events must be corrected before the original event is reprocessed.

Follow this general procedure to manage errors on IN or OUT events.

1. Given an error event, define the filters to identify all events relative to the same user.
2. Select the oldest event in error list.
3. Reconstruct the cause of the error based on available data, according to the indications provided in the preceding sections.
4. Remedy the event based on step 3.
5. Restart the rule engine (RE) to reprocess the event that you corrected
6. If the event is still in error, return to point 3.
7. If the reprocessing is successful, individually select all chronologically consecutive events and restart the RE to reprocess them one at a time.
8. If the generic event produces an error again, go back to point 1.
9. If all errors produced after point 1 are remedied and reprocessed successfully, the problem is resolved.

This procedure is valid for most error situations that can occur. In simpler cases, steps 1, 2 and 3 can be skipped.

Operation Code

This code specifies the operation that originated the event.

An operation can cause more than one event. For example, the operation for deleting a user implies events for the removal of entitlements from the user before the user is deleted. All of these events are specified by the same operation code.

The Operation Code is a string of characters that are generated based on standard mechanisms.

The standard structure of the Operation Code is

```
<prefix>_<code>
```

The `<prefix>`can be one of the following types, depending on the architectural module that is generating the event:

MR_SYNC
The event is generated by the Synchronization flow.

MR_IN
The event is generated by the read from or input flow.

MR_OUT
The event is generated by the write to or output flow.

PM The event is generated by the AG Core module, or is transferred to the AG Core without any code and AG Core transmits the event as though it generated it.

Note:
The string **PM** is used for AG Core because of legacy reasons.

The `<code>` can be one of the following forms:

Generated by the rule engine

```
<event Id>_<User Id on the Person>
```

Generated by the AG Core
A random number.

Structures differing from the standard structure can also be found.

Applications that are integrated with the AG Core communicate without using the standard Integration Interface. They can send and receive request to and from the AG Core. They can transmit their own operation code for the events that result from the requested operation. The operation code changes depending on the integrated application.

Note: If an event is delivered to AG Core by any module without the operation code, it is automatically considered as if the event originated by AG Core. The operation code uses the format:

```
PM_<random number>
```

Activities

You can view the activities associated to a selected user. This information provides a pattern of the operative scope of the user.

In Identity Governance and Intelligence, you can associate a user with one or more entitlements.

Entitlements can be associated to a set of business activities (see Access Risk Controls).

The **Activities** tab lists all activities associated with the user that was selected in the **Users** tab.

Groups

You can use functions to manage a hierarchy. The main hierarchy is the ORGANIZATIONAL_UNITS hierarchy.

For more information about organizational units, see Organization Units.

Groups is above the **View** and **Search** tabs.

View Use this tab to browse the hierarchy and select a group.

Search
Use this tab to search for a group by name or ID Code. Click **Filter**.

If a group of a hierarchy is affected by a certain level of risk, near the group is present a colored icon according to the usual risk level convention:

High 🔴

Medium 🟠

Low 🔵

Clicking a risk level icon that is associated to a group, the Conflict Info pop-up window opens, showing all the related information.

The **Actions** menu in the left frame lists the following actions:

ToggleMngr
Shows or hides the group manager. This action is shown only when you select **View**.

Move Moves a group to another position in the tree.

Add Adds a group.

Remove
Deletes a group.

Tree View
Switches from the **Search** to **View** after you select a group and provides the position of the selected group in the hierarchy.

This action is shown only when you select the **Search** tab.

Use the **Add** action to create a new Group.

For more information about the procedure, see "Adding an organizational unit" on page 105.

You can then specify the following options to the new group:

Inherit Parent Entitlements
All the entitlements that are assigned to the parent group are automatically assigned to the new group.

Inherit Parent Resources
All the resources that are assigned to the parent group are automatically assigned to the new group.

Use **Remove** to delete:

A single group
A single node.

A group and its entire subtree
A single node and all its children.

Note: When you run **Remove** on the root of a group subtree, the children of the group are automatically moved to the same level of the root group subtree. In other words, all the groups that are originally at the L level for the selected subtree, are redistributed to the L-1 level.

Use **Move** to choose a new position for a selected group.

Note: The `Inherit Parent Entitlements` and `Inherit Parent Resources` options are not supported in a Move action. The group that was moved maintains the entitlements and resources it had in its previous position.

Use **ToggleMgr** to show or hide the managers of the OUs. Double-click the root node of the organization to refresh the data.

The right frame displays different panes based on the tab you select in the upper side of the frame. **Details** is selected by default. It includes the following accordion panes:

- **Details**
- **Group Properties**

For editing information in these panes, make the edits, and click **Save**.

Details is automatically displayed when you select a group in the left frame. The following table describes the group details:

Table 39. Group details

Detail	**Description**
`Parent Group`	The name of the parent Group (automatically set after the group selection in the left frame).
`Type`	The type of Group.
`Name`	The name that is used in the Organization to identify the group.
`ID Code`	The univocal identifier of the Group.
`Exclude from SoD Validation`	Indicates whether the Segregation of Duties (SoD) control is enforced or bypassed.
`Owner`	The user who has responsibility over the selected group. Click ⋯ `User` and ⊗ `Clear` to enter a user or to clear the field.
`Description`	A short description of the group.

The **Group Properties** pane displays properties that provide additional information on a selected Group. They are custom properties and are defined by the Administrator. For example, the value of a property can be an external link to the set of implementation and compliance rules that must be followed by the Group. You can also add the values of these properties in the structure of a Rule.

Properties are made up by the `<Name,Value>` attributes.

Use the **Actions** menu in this pane to add or delete properties for a selected Group.

Add Adds a property.

Remove
Deletes a property.

Save Saves a property.

Note: You can define multi-value properties. In the **Group Properties** pane, click **Add** and specify a property `PROP_1` with a `VALUE_1` value. Click **Add** again and enter the same `PROP_1` property name with a different value `VALUE_2`.

The other group-related operational tabs available in the right pane are:

- Entitlements
- Group Resources
- Users
- Analysis
- Activities

Related tasks:

"Adding an organizational unit" on page 105
Complete this task to register a new organizational unit.

Entitlements

You can view all the entitlements that are already associated to a group of a selected hierarchy.

The **Entitlements** tab lists all the entitlements that are already aggregated to a group.

Entitlements can be assigned to a user only if they are already assigned to the group to which the user belongs. The following table lists the available filters.

Table 40. Entitlement filters and details

Filter	Description
Type	The type of entitlement: • Permission • IT role • Business role • External role
Application	The name of the application that includes the entitlement.
Name or Code	Name or operational code that is used within the organization to identify the entitlement.
Enabled	This attribute is a binary attribute: **Yes** The entitlement can be assigned to users. **No** The entitlement exists in the system but cannot be assigned to other users.
Administrative	If this check box is selected, only administrative entitlements are listed in the resulting list.

An entitlement can be characterized by a set of main attributes

Role Alignment Violation
An entitlement is in Role Alignment Violation (**VV** column) when it is not associated to the OU but you assign it to a specific user of that OU.

Default
An entitlement is automatically assigned to each user in a group. It is useful for modeling a basic entitlement with common functions that are assignable to all users that belong to a group.

Enabled
An entitlement is available for the users in the group.

Note:

1. Setting an entitlement as a default, automatically assigns it to every new user of the group. It is not automatically assigned to the users already present in the group.

2. For a Role Alignment Violation, you can change the initial `Yes` value to the final `No` value. However, you cannot do the opposite because the Role Alignment Violation can detect only when an entitlement is assigned for the first time to a specific group.

The **Actions** menu of this tab, lists the available functions.

Conflicts
Provides information about risks that are related to the selected entitlement.

Hierarchy
Shows the entitlement hierarchy.

Details
Provides specific information about all the permissions that are joined to a selected entitlement.

Status Shows the status of the permissions. The status of the permissions can be TBD, Ignored, Missing Activity, or Linked.

Add Adds an entitlement.

Remove
Deletes an entitlement. Ticking the **Hierarchy** check-box, it is possible to remove the entitlement through the entire group hierarchy.

For information about the procedure, see for adding an entitlement to an organization unit.

The **Conflicts** operation shows information about risks that are related to the entitlements of the group. Use the [Ctrl] or [Shift] keys to make multiple selections.

If all entitlements must be tested, no selection is needed.

You can use the **Status** operation to set or managed some attributes of an entitlement that is already aggregated to the OU.

Use the Role Status Management window to manage or set the following options.

Table 41. Role Status options

Option	Description
Default	Four values are available: **(*empty*)** No actions. **No** The entitlement is not a default entitlement. **Yes** The entitlement is a default entitlement. **Yes and align Users** The entitlement is a default entitlement and is assigned to all users in the OU.

Table 41. Role Status options (continued)

Option	Description
Enabled	Three values are available: **(*empty*)** No actions. **Yes** The entitlement is ready to be assigned to users. **No** The entitlement exists in the system but cannot be assigned to other users.
Span hierarchy	If this check box is checked, the entitlement status is propagated down the hierarchy.

The **Add** operation adds an entitlement to the selected group and to determines all the parameters that are related to the status of the entitlement.

The **Remove Entitlement** operation deletes the selected entitlement. Use the [Ctrl] or [Shift] keys for a multiple selection.

Note: A default entitlement can be removed from a user just like any other entitlement.

Related tasks:

"Adding an entitlement to an organizational unit" on page 99
You must assign the entitlement to the organizational unit before you can assign the entitlement to a user that belongs to the same hierarchy of the organizational unit.

Group Resources

Resources can be assigned to a user only if they are already assigned to the Group to which the user belongs.

The following table lists the available filters.

Table 42. Organizational unit resource filters

Filter	Description
Name	The name of the resource family.
Resource Type	The resource type name.
Resource Family	The resource family name.
Inheritable	In this column is indicated if the resource is or not inheritable. An inheritable resource is characterized by a green icon.

The **Actions** menu lists the available functions.

Add Assign a resource to a selected Group.

Remove
Deletes a resource from the selected Group.

A Resource can be assigned with either of two options.

Hierarchy

When a resource is assigned to an Group, the same resource is also assigned to the entire sub-tree under the Group. If a resource is removed, it is removed from the entire sub-tree as well.

Inheritance

The resource is automatically assigned to all users added in the Group.

Note: A resource that is assigned to an Group by inheritance is assigned to every new user in the Group. The resource is not assigned to the users that exist in the Group when the inheritance option is set.

Users

In this tab are shown users aggregated to the Organization Unit selected in the left frame.

The table below list the available filters (click the **Filter/Hide Filter** button):

Table 43. User filters

Filter	Description
User Type	This information allows to define different categories of users. See also User>Details.
Surname/Name/Code	This field can host the Surname or the Name or the Master UID of the user.
OU	Automatically set on OU selected in the left frame.
Hierarchy	If this check-box is ticked, the search is extended to users of OUs belonging to the sub-tree whose root coincides with OU field.

Activities

You can view the activities that are associated with a selected group and the related map, for getting the business processes pattern associated to a specific organization area (group).

You can associate a group with one or more entitlements.

These entitlements can be associated to a set of business activities (see Access Risk Controls).

In the tab **Activities**, are listed all activities that are associated to the group selected in the tab **Groups**.

The table lists the available filters:

Table 44. Available filters to list activities.

Business activity filters	
Filter	**Description**
Name	Name of the business activity.
Code	The unique identifier of the business activity.
Description	Brief description of the business activity.

Under **Activities**, you find other two tabs, **Search** and **Map**.

In **Search** you can select an activity, from a flat list, and automatically, in the rightmost frame, are shown all the users that are associated to the activity selected.

You can filter users with:

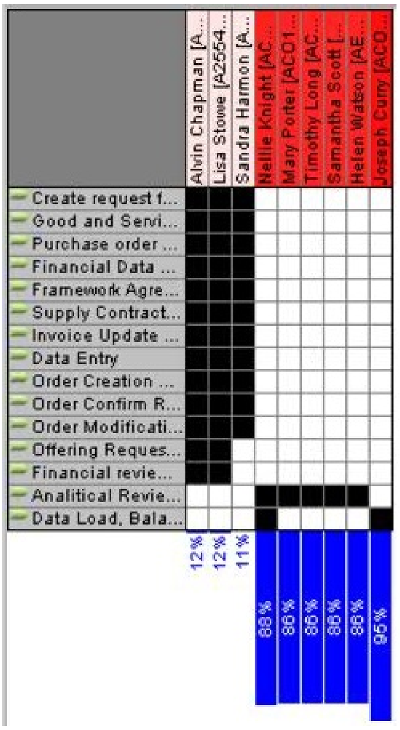
Table 45. Available filters to list users.

Filter	**Description**
User Type	Click the arrow and select one of the users types listed. The user type is defined in your security model.
Search Identity	Enter the name, the surname, or the master UID of the user.
Groups	Click ⋯ **Browse** to choose the Group of the user.
Hierarchy	If this check box is selected, the search starts from the root Organization Unit that is selected in the **Groups** field and is run on all the hierarchy.

In **Map**, you can view the map activities-users for all the activities that are associated to the group.

This map provides a visual indication of the operational profile of every user in the group.

A subset A of users could be associated to all or to a large part of activities, while a subset B of users could be associated to only one or few activities.



In the figure, users of subset A are indicated with the background white and subset B with the background red.

In the bottom part, is indicated for every user an index named *Divergence*.

Users reds (subset B) have high level of divergence that provides an alarm about the risk that is embedded into the associations activities-users.

Users of subset A have a low level of divergence.

In general, a low level of divergence provides a good pattern of associations activities-users.

A high level of divergence requires a more deep investigation.

For setting these types of investigations, the filter **Exclusion Treshold** can be used for setting different levels of exclusion, for isolating subsets of users for additive analysis.

It is possible to exclude also a single user, selecting it on the map and clicking **Exclude User**.

After this setting, you can define a dataset through **Actions** > **Review**.

This dataset can be used for a future campaign (see **Access Governance Core** > **Configure** > **Certification Datasets**.)

Roles

A role identifies the set of permissions that are assigned to a user. Use this set of panels to define and manage roles in your organization.

Roles can be published or unpublished.

A published role (the role name is shown in bold italic) can be assigned to

- One or more groups of an attribute hierarchy (in particular, to organizational units)
- One or more users

An unpublished role cannot be assigned.

In the hierarchical organization of a generic role, any component of the hierarchy can be published or unpublished, without any regard to the position of the specific component.

A role can be also object of:

- Consolidation (one shot), when, on demand, a group of entitlements can be organized into a role (Business Role or IT Role)
- Persistent Consolidation, when the role is periodically consolidated (by running a job with the Task Planner module)

A consolidated role is shown in bold orange.

A role under persistent consolidation is shown in bold italic blue.

You can use filters to search for specific roles. The following table lists the available search filters for roles:

Table 46. Role filters

Filter	Description
Type	Indicates one of the following entitlement types: • Permission • IT Role • Business Role • External Role
Application	Indicates the name of the application to which the entitlement is related. Use ... **Application** and ⊗ **Clear** to set an Application or clear the field.
Name or Code	Indicates the entitlement name, or the code that identifies it.
Published	The published attribute can have these values: **Yes** The role is published. **No** The role is unpublished. **All** Do not distinguish between published and unpublished roles.

The roles are listed by:

- Name
- Application
- Description

They are sorted by role type.

Important: Unfulfilled permissions and external roles are not displayed in the list.

Select a role and click **Actions** to display the following list of actions:

Role Version
Assigns a version to a role. The base version is 0.

Rollback
Returns the role to the previous version, from version *N* to version *N*-1.

Consolidate
Consolidating a role, the role replaces the set of entitlements that are assigned to a user that are consolidated into the role (for all the users who match this condition).

Dismiss
Reverses the consolidation operation.

Enable persistent consolidation
Enables the persistent consolidation of a Role.

Disable persistent consolidation
Disables the operation of persistent consolidation.

Publish
Publishes a role to assign it to an OU.

Unpublish
Reverses the operation of publishing a role.

Add Creates a role. No role needs to be selected to start this action.

Remove
Deletes a role.

For more information, see this procedure: “Adding an entitlement” on page 99.

Note: You can import a role also with Access Optimizer (for releasing a role after a role mining analysis), or through the Enterprise Connectors, or by using a dedicated bulk load.

Note: You could remove a Business Role (or an IT Role) that could host a required attribute permission. This last one is associated directly to the user.

For example, you can remove the association *User - IT Role* for an IT Role with three permissions, P1, P2, and P3, where P3 is a required attribute permission. In this case, while the association with P1 and P2 is removed, P3 is associated directly to the user.

You can publish an entitlement immediately after it is added. The **Details** tab shows data about a selected entitlement.

Table 47. Role details

Area	Detail	Description
Info	**Version**	Number from 0 to *N* that indicates the version of the role.
	Owner	User who is responsible for the selected role. Click ... **User** and ⊗ **Clear** to set a user or clear the field.
	Name	Name that is used in the organization to identify the role.
	Code	A code that is used in the organization to identify the role.
	Description	A brief description of the role.
	Type	Indicates one of the following entitlement types: • Business Role • External Role • IT Role • Permission
	Application	The name of the application that is related to the selected role. Click ... **Application** and ⊗ **Clear** to set an application or clear the field.
	Permission Type	This attribute tags and categorizes a set of permissions into a specific **Type**.
	Entitlement Families	The family of which the selected role is part.
	Expiration	The expiration date of the role. When an entitlement expires, some automatic controls might be run. Click 📅 **Calendar** and ⊗ **Clear** to set a date or clear the field.
	Last Review Date	Date of the last authorized modification on the entitlement.

Table 47. Role details (continued)

Area	Detail	Description
Business info	**Business Name**	Field for future use.
	Business Policy	Field for future use.

An entitlement can be associated to a set of properties that characterize it.

The **Entitlement Properties** accordion pane displays properties that are associated to an entitlement. Properties can add dynamic meanings to the entitlements. For example, a property can have a value that is used by a rule to manage a business process in the organization.

A property consists of a - *Key*,*Value* - pair of attributes.

Properties can be easily added into a new empty row with **Actions** > **Add**.

Table 48. Property attributes

Attribute	Description
Name	Name of the property.
Description	Description of the property.
Searchable	For future use.
Multivalue	Property can have a set of values rather than a single value.

Use this procedure to set a new property.

A property can be saved clicking the **Actions** > **Save**.

You can remove a property, selecting the check-box on the leftmost column and clicking **Actions** > **Remove**.

You can remove all properties with the same command, selecting the check-box on the blue attribute-bar.

The operational tabs for entitlements are:
- Management
- Users
- Org Units
- Permissions
- Rights
- Analysis
- History

Related tasks:

"Adding an entitlement" on page 99
Complete this task to register a new entitlement into the Identity Governance and Intelligence data model.

Management

Use the **Management** tab to build the hierarchy of a role.

You can use the following filters to search specific entitlements:

Table 49. Filters to search for the entitlements that make up a role.

Filter	Description
Type	The entitlement type can be one of the following: • Permission • IT Role • Business Role • External Role
Search Entitlement	The role name.
Application	The name of the application to which the entitlement is related. Use the … and ⊗ **Clear** buttons on the right side of the **Application** attribute box to set an Application or clear the field.

Select an entitlement and click **Actions** to display the following list:

Conflicts
Checks conflicts that are related to a set of entitlements.

Hierarchy
Shows the tree structure of the selected entitlement.

Add Adds an entitlement at the hierarchy level of the entitlement that is selected in the **Hier View** tab.

Remove
Deletes an entitlement.

Users

Use this tab to view the users who are assigned with the selected role.

You can use the following filters to search specific users:

Table 50. Filters to search for the users assigned with the entitlement.

Filter	Description
User Type	The category to which the user belongs as defined in the organization's structure.
UME	A digital identity for a user that can have more than one account on the same target system.
Search Identity	The first name, last name, or the master UID of the user.
Associated	If checked, the search result lists only users who are assigned to an OU. If cleared, the search result lists only users that are not associated with any OU; for example, new users who have not yet been assigned to any OU.
Groups	The name of the attributes group from which the user search starts.

Table 50. Filters to search for the users assigned with the entitlement. (continued)

Filter	Description
Hierarchy	If this box is checked, the search is extended to users of OUs that belong to the subtree whose root coincides with the **Groups** field.

Use the **Remove** function from the **Actions** menu to delete a user from the list. This operation is similar to removing the role from the set of roles available for the user.

Org Units

The **Org Units** tab shows the OUs that host the selected role.

You can use the following filters to search OUs:

Table 51. Filters to search for the OUs associated with the entitlement.

Filter	Description
Groups	The name of a specific attribute group. In this case it is the attribute group to which the organizational unit belongs.
Name	The name of a specific group of the hierarchy. In this case it is the name of the OU.
ID Code	The ID of a specific group of the hierarchy.

Click **Actions** and select one of the following:

Add Adds an OU to the list of OUs associated with the entitlement.

Remove
Deletes an OU.

Permissions

The **Permissions** tab shows the permissions that are included in the selected role.

You can use the following filters to search for specific permissions:

Table 52. Filters to search for the permissions that are in a role.

Filter	Description
Application	The application that is related to the permission. Use the … **Application** and ⊗ **Clear** buttons on the right side of the attribute box to set an application or clear the field.
Type	The type of permission, as defined within the organization.
Name	The name that is used within the organization to identify the permission.

Table 52. Filters to search for the permissions that are in a role. (continued)

Filter	Description
Status	The status of the permission: **Linked** The permission is joined to an activity. **Ignored** The permission is not joined to any activity. **Missing Activity** The operator does not know to which activities to join the permission. **To be Defined (TBD)** The permission is not joined to any activity but is not in the status **Ignored** or **Missing Activity**.

Managers

The **Managers** tab shows the managers that are aggregated to the selected role.

The following table lists the available manger filters.

Table 53. Manager filters

Filter	Description
Admin Role	The administrative role that is selected from a list of administrative roles.
First Name	The given name of the manager.
Last Name	The surname of the manager.
Master UID	The unique identifier of the manager.
Admin Role assignment	The assignment can have either of the following values: • **Direct** • **By Delegation**

After a user is selected from the list, click **Tree View** to display the position of the manager in the OU.

Rights

This tab shows the rights aggregated to the application access selected in the left frame.

The right frame displays two panels.

The left panel lists the existing application access - application association.

The **Name** (of the Right) is the available filter (click **Filter/Hide Filter**).

As you select an application access - application binomial, the right panel shows the properties of the associated Right:

Table 54. Right properties.

Property	Description
MVal/Lookup	The ✓ green icon indicates that the Right is multi-value or with lookup (it can be also both).
Name	The name of the right. If the right is required, near the name is present the 🔒 icon.
Status	Status of the Right • **None** 👤 indicates that no specific policy is defined for assigning a Right to a User. • **Restricted** ≣ indicates that when the Right is assigned to a User, it is possible to choose values only from a predefined set. • **Fixed** ABC indicates that it is not possible to choose a specific value (or a set of values) for the Right because its values are preset.
Actions	The following operations are available: **Edit**, **Show**, and **Clear**.

Click **Edit** to display the Lookup Management window, where you can select one or more values.

- Select the **Value** check box to select all the values that are listed.
- For a **Single Value** right, the Insert Value window opens, for setting the value.
- From the Lookup Management window, you can click **Fixed** and **Restricted** to change the status of the right.

Click **Show** to open the View Values window that shows the value of the right.

History

The **History** tab lists all the changes that are made on a selected entitlement or permission. You can search a specific change by clicking **Filter**/ and setting the **Revision** and **Date** filters.

The following history attributes shown:

Table 55. History attributes

Attribute	Description
Revision	The ID number of the revision of the selected entitlement or permission.

Table 55. History attributes (continued)

Attribute	Description
Operation	The operation that is involved with the update. The following types of operations are available: • Edit • Insert • Delete • Add Entitlement • Remove Entitlement • Permission Type • Owner • Entitlement Family • Workflow Authorization • Workflow Check
Field Label	The technical field (the column of a specific table of the AGC DB) involved with the operation in the **Operation** attribute.
Old Value	The value of the **Field Label** attribute before the update operation.
New Value	The value of the **Field Label** attribute after the update operation.
Date	The date of the update operation.

Click **Undo** to ignore the update in **in the last operation** and to restore the previous entitlement or permission data.

Applications

Documents the functions required for the management of Applications.

The Applications frame includes the **Name** and **Account** filters that are used to search Applications (click the **Filter/Hide Filter** button to specify them). It includes also command buttons that you can use to run basic operations on applications.

In this same frame, use the **Add/Remove** button to add or remove an application. Adding an application implies linking an Application to a specific Account.

For information about the procedure, see “Adding an application” on page 67.

Generally, several Applications can be linked to a specific Account configuration.

This association allows to consistently manage a set of Applications regarding the operating attributes that define how a User has access to the system. This mechanism increases the degree of security for accessing an Application and implies a series of password controls associated to the User’s account.

With the **Modify SoD** button, you can decide whether an Application must be excluded or not from SoD checks (the related checkbox in the **Details** tab and the SoD column in the Applications frame are automatically updated).

The Details pane shows details of the Application selected in the left frame:

Table 56. Application details

Details	Properties and descriptions
Info	**Owner** The user who is responsible for the selected Entitlement. Use the ⋯ **User** and ⊗ **Clear** buttons on the right side of the attribute's box to insert a User or clean the field. **Name** The name that is used by the Organization to identify the Application. **Description** A short description of the Entitlement.
Policy	**System Account** If this radio button is selected, the Account of the Application is the IDEAS System Account. **Custom Account** If this radio button is selected, the Application Account can be customized. **Disable out/target events generation** If this check box is selected, the generation of the out/target events is disabled. **Events Marker** Name of the Events. **Exclude from Risk validation** If selected, SoD control is enabled. The same data is also reported in the SoD column in the Applications frame (✗ icon).

An Application can be added to a set of properties that characterize it.

The Application Properties pane displays properties that can add specific information for the selected Application.

For example, a Property can have a value that is used by a Rule to manage a business process of the Organization.

A Property is identified by a pair of attributes, **Name** and **Value**, and can be easily added or removed with the **Add** or **Remove** buttons placed in the upper right side of the pane. The values of a property can be freely edited and saved with the **Save** button.

Table 57. Note about multi-value properties

ℹ	**Note:** MULTI-VALUE properties are possible. For example, you can specify a `PROP_1` property and associate it a `VALUE_1` value. You can then add a line in the Application Properties pane and specify the same property name (`PROP_1`) associated to a different value (`VALUE_2`).

The operating tabs for applications are:

- Application Access
- Users
- “Analysis” on page 216
- “Permission Type” on page 225

Related tasks:

“Adding an application” on page 67
Complete this task to register a new application. By default, a new application is joined to the default *System Account IDEAS* and the related *Events Marker IDEAS*.

Application Access

Documents how to manage application permissions.

The **Application Access** tab displays the permissions that are already associated with the application that is selected in the left frame. You can use the following filters to find permission definitions (selecting **Filter/Hide Filter**):

Table 58. Application Access filters

Filter	Description
Type	Type of permission • **Permission** • **External Role**
Permission Type	The permission type. This information can be useful to group permissions. Generally, permission types are loaded through a bulk load procedure.
Name or Code	Name or code of identification of the permission.

Table 58. Application Access filters (continued)

Filter	Description
Status	Status of the permission **Linked** The permission is joined to an activity. **Ignored** The permission is not joined to any activity. **Missing Activity** The operator does not know to which activities to join the permission. **To be Defined (TBD)** The permission is not joined to any activity but is not in the status **Ignored** or **Missing Activity**.

You can select the following **Actions**:

- **Set Auth** sets two types of authentication (not mutually exclusive). They are **Weak Authentication** *(UserID-Password)* and **Strong Authentication** *(Cert.X.509, smart card, Bio, ...)*.
- **Add** adds a permission.
- **Remove** removes a permission. A permission that originated from an external target system cannot be removed with this **Action** menu. Instead, the permission must be removed from the **Action** menu that is on the **Manage** > **Accounts** > **Attribute-to-Permission Mapping** page. This applies to group and nongroup permissions.
- **Fulfill** configures a permission as assignable to a user on a target system.
- **Unfulfill** configures a permission as not assignable to a user on a target system.
- **Publish** publishes a permission and makes it available for association with one or more groups and one or more users.
- **Unpublish** makes the permission no longer available for any association.

The tabs listed become available in the right frame after you select a permission:

Details

The **Details** tab on the right displays the permission data:

Table 59. Permission details

Detail	Description
Name	The name that is used in the organization to identify the permission.
Code	The code that is used in the organization to identify the permission.
External Ref	An external reference (external key) of the permission on the target system.
Description	Short description of the permission.
Permission Type	Type of permission (used to tag different subset of permissions of the same application).

Table 59. Permission details (continued)

Detail	Description
Owner	The user who is responsible for the selected permission. Click … **Users** and ⊗ **Clear Field** on the right side of the attribute's box to insert a user or clean the field.
Expiration	The expiration date of the permission. Some automatic controls can be made when a permission expires.
Last Review Date	The date of the last review that is made on the permission.

You can edit the values of the permission details and click **Save**.

Properties

The **Properties** tab displays properties that can add specific information to the selected permission.

A property consists of a - *Key*,*Value* - pair of attributes.

Properties can be easily added into a new empty row with **Actions** > **Add**.

Table 60. Property attributes

Attribute	Description
Name	Name of the property.
Description	Description of the property.
Searchable	For future use.
Multivalue	Property can have a set of values rather than a single value.

Use this procedure to set a new property.

A property can be saved clicking the **Actions** > **Save**.

You can remove a property, selecting the check-box on the leftmost column and clicking **Actions** > **Remove**.

You can remove all properties with the same command, selecting before the check-box on the blue attribute bar.

Parent hierarchy

In this tab, you can view the entitlement structure that hosts the selected permission.

Rights

The “Rights” on page 18 are extra attributes and are related to the permissions. A right determines the set of values that can characterize the generic transaction that is enabled by a permission.

The **Rights** tab displays rights that are already defined for a permission.

You can add or remove rights with **Actions** > **Add/Remove**.

A right is defined by the - *Name,Value* - attributes.

Each right can be **Single Value** or **Multi Value**, with more than one value set for the same *Name*.

In both cases, you can choose from a predefined set of values (**Lookup (Y/N)** attribute).

A right single-value with lookup is a single value *Vx* from a set of values (*V1,V2, ... VN*).

A right multi-value with lookup is a subset of several values (*Vx,Vy,Vz,...*) from a larger set of values (*V1,V2, ... VN*).

A right can be also **Required** or **Not Required**.

If the right is **Required**, at least one value must be always set.

If the right is **Required**, it is highlighted by a dedicated icon .

Table 61. Rights attributes

Attribute	Description
Name	The name of the Right.
Lookup (Y/N)	Tick this check-box for enabling a Lookup table.
List Name	The key of the Lookup table.
Multi-Value	Select this check-box to make the Right a multi-value one.
Required	Select this check-box for a Right that requires at least one value to be set.

You can add multiple rights to a permission. Use the related check box on the Rights row to add one or more properties to a selected permission.

To select all the Rights, select the check-box on the blue attribute bar.

Click **Save** to confirm any update.

History

The **History** tab lists all the changes that are made on a selected entitlement or permission. You can search a specific change by clicking **Filter**/ and setting the **Revision** and **Date** filters.

The following history attributes shown:

Table 62. History attributes

Attribute	Description
Revision	The ID number of the revision of the selected entitlement or permission.

Table 62. History attributes (continued)

Attribute	Description
Operation	The operation that is involved with the update. The following types of operations are available: • Edit • Insert • Delete • Add Entitlement • Remove Entitlement • Permission Type • Owner • Entitlement Family • Workflow Authorization • Workflow Check
Field Label	The technical field (the column of a specific table of the AGC DB) involved with the operation in the **Operation** attribute.
Old Value	The value of the **Field Label** attribute before the update operation.
New Value	The value of the **Field Label** attribute after the update operation.
Date	The date of the update operation.

Click **Undo** to ignore the update in **in the last operation** and to restore the previous entitlement or permission data.

Related concepts:

"Permissions based on user attributes" on page 16
An attribute permission is a specific type of permission that is used for mapping a user attribute that is imported from a target system. For harmonizing this feature with the role-based access control standard of the Identity Governance and Intelligence data model, you can use permissions and rights.

Related tasks:

"Verifying that an attribute-to-permission mapping is enabled" on page 83
Complete this task to verify that an attribute-to-permission mapping is enabled in the Access Governance Core module.

Users

Documents how to manage application users.

The **Users** tab displays the Users defined for the Application selected in the left frame. Users can be filtered by click the **Filter/Hide Filter** button and using the following filters:

Table 63. User filters

Filter	Description
Search Identity	This field can have the Name, the Surname or the User ID of a User.

Table 63. User filters (continued)

Filter	Description
Associated	If selected, the search result will include only Users defined to an OU. If not selected, the search result will include only Users that are not defined to any OU (for example, when a User has just been entered in the DB but has not yet been defined to any OU).
OU	Automatically set on a selected OU.
Hierarchy	If this checkbox is selected, the search is extended to Users of OUs belonging to the subtree whose root coincides with the OU field.

Note that a user might have an account associated with an application, but the user might not be assigned any entitlement that is related to that application.

Analysis

An *analysis* is the object that contains all the data required for a data analysis. The **Analysis** tab provides graphical dashboards and detailed information about the Entitlements (Permissions) and Users associated with the selected Application.

This tab displays information in the following categories:

- "Statistics"
- "Entitlement map" on page 217
- "Permissions" on page 217
- "Users" on page 221

Statistics:

This tab displays statistics information through charts and diagrams.

The following statistics are available:

Assignment Statistics
Assignment Statistics illustrates the statistics on assigned Entitlements, and Users with and without assignments.

Table 64. Dashboard set

Dashboard	Description
Entitlements	The entitlements (permissions) registered in the organization. The diagram illustrates the number of assigned and unassigned Entitlements - Permissions, and Roles.
Assignments	All user-entitlement assignments. The chart illustrates the number of assigned Permissions, and Roles to Users.
Users	The users who belong to the organization. The diagram illustrates the number of Users with directly assigned Permissions, with just Roles, and without assignments.

Table 64. Dashboard set (continued)

Dashboard	Description
Permissions	The entitlements (permissions) registered in the organization. The diagram illustrates the number of Permissions unassigned, directly assigned, and assigned through Roles.

Entitlement Statistics

Entitlement Statistics illustrates the number of Entitlements assigned to the following data elements.

- Users
- Permissions
- Organization Units
- Applications

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Entitlement map:

This tab displays the Entitlement and User association through a map diagram.

In the map, the vertical axis shows the entitlements whereas the horizontal axis shows the users. The black boxes show when an entitlement is assigned to a user.

You can select from the following actions:

- **Reshuffle**: by clicking **Reshuffle** the map will change. This operation is possible, after selecting the area.
- **Select area**: click **Select Area** to highlight an interested area. With the left mouse button click a block on the map to define the start position of the area. The area selected between the start/end positions will be covered with a yellow mask.
- **Single select**: allows you to return to single select mode. The single selection is possible only when the action is performed on the selected area, after the area involved is highlighted in yellow. The single block that is highlighted is the end position block of the **Select Area** action.
- **Zoom in/Zoom out**: the zoom action modifies the resolution of the map.

Permissions:

View this tab for an analysis of the Permissions assigned to the selected Application and its relations to other data elements such as Users and Organization Units.

This tab has the following sub categories.

- Permission
- Permission Details
- Users
- Organization Units

Permission

The **Permission** tab lists all Permissions assigned to the selected Application.

In this tab, you can:

- Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.
- Select a Permission to view the details of the Users and Organization Units assigned with it, in the right pane.

Table 65. Permission filter details

Filter	Description
Name	Name of the entitlement.
Application	Name of the application.
User Coverage	Type of user coverage. Directly assigned.

Permission Details

The **Permission Details** tab lists the Permission details, and the statistics of Users and Organization Units associated with the selected permission.

Table 66. Permission Details

Permission Details tab	Fields and descriptions
Permission	**Application** Name of the application. **Name** Name of the entitlement.
Users	**Users** Number of users assigned to the selected entitlement. **User Support (%)** Percentage of users to be assigned to the permission, from the entire set of users involved in the analysis. **Covered with just Roles** Number of users covered with the Role entitlement. **User Coverage (%)** Percentage of users that are assigned to the permission, from the entire set of users involved in the analysis.

Table 66. Permission Details (continued)

Permission Details tab	Fields and descriptions
Organization Units	**Org Units** Number of organization units involved in the selected entitlement. **Org Unit Support (%)** Percentage of organization units to be assigned to the permission, from the entire set of organization units involved in the analysis. **Covered with just Roles** Number of organization units covered with the Role entitlement. **Org Unit Coverage (%)** Percentage of organization units that are assigned with the entitlement, from the entire set of organization units that must be assigned with the entitlement.
	OU Spread OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread. **Minimum Farness** Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness. **Average Farness** Average distance of all OUs from the centroid of distribution. See Farness. **Average Coverage (%)** Average percentage of OUs assigned with the entitlement. **Maximum Coverage (%)** Maximum percentage of OUs assigned with the entitlement.

Users

The **Users** tab lists the Entitlement and User details.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Table 67. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 68. User details

User	Description
In/Out	The user status can be one of the following: • ✓ In Role (Role aggregated to the User) • ✗ Out of Role (Role not aggregated to the User)
Last Name	Surname of the user.
First Name	Name of the user.
Master UID	Unique ID assigned to the user.
Organization Unit	Name of the OU, in which the user is registered.

Select a User and click **Actions** > **View Tree** to view the Organization Unit structure.

Organization Units

The **Organization Units** tab lists the Entitlement and Organization Unit details.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Table 69. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.

Table 69. Entitlements (continued)

Entitlements	Description
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 70. Organization Unit

Organization Unit	Description
In/Out	The OU status can be one of the following: • ✓ In Role (Role aggregated to the OU) • ✗ Out of Role (Role not aggregated to the OU)
Code	Code assigned to the OU.
Name	Name of the OU, in which the user is registered.
Farness	Farness is a numeric index that provides an estimate of the virtual distance between OUs having the same entitlement/candidate role. It can measure the distance between OUs in which different registered users are assigned the same entitlement/candidate role.
Coverage (%)	Percentage of users in the OU who are assigned to the entitlement.
Users	Number of users assigned to the selected organization unit.

Select a User and click **Actions** > **View Tree** to view the Organization Unit structure.

Users:

View this tab for an analysis overview of the Users assigned with the selected Application.

This tab has the following sub categories.

- User
- User Details
- Permissions
- Applications

User

The **User** tab lists all Users assigned to the selected Application.

In this tab, you can:

- Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.
- Select a User and click **Actions** > **View Tree** to view the Organization Unit structure.
- Select a User to view the analysis report in the right pane.

Table 71. User filter details

Filter	Description
Master UID	Unique ID assigned to the user.
Last Name	Surname of the user.
First Name	Name of the user.
Organization Unit	Name of the OU, in which the user is registered. Select **Hier** to include all the Organization Unit starting from the root **OU**.
Permission Coverage	Type of coverage. Without assignments or with permissions directly assigned.

User Details

The **User Details** tab lists the User details, and the statistics of Entitlements associated with the selected User.

Table 72. User Details

User Details tab	Fields and descriptions
User	**Last Name** Surname of the user. **First Name** Name of the user. **Master UID** Unique ID assigned to the user. **Organization Unit** Name of the OU, in which the user is registered.
Permissions	**Permissions** Number of assigned permissions. **Permission Support (%)** Percentage of permissions to be assigned to the user, from the entire set of permissions involved in the analysis. **Covered through Roles** Number of permissions covered with the Role entitlement. **Permission Coverage (%)** Percentage of permissions that are assigned to the user, among the entire set of permissions involved in the analysis.

Table 72. User Details (continued)

User Details tab	Fields and descriptions
Applications	**Applications** Number of applications assigned with the entitlement. **Application Support (%)** Percentage of application to be assigned to the user, from the entire set of entitlements involved in the analysis. **Covered through Roles** Number of applications covered with the Role entitlement. **Application Coverage (%)** Percentage of applications that are assigned to the permission, among the entire set of applications involved in the analysis.

Permissions

The **Permissions** tab lists the Entitlements and Permissions assigned to the selected User.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Table 73. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 74. Permission

Permission	Description
In/Out	The permission status can be one of the following: • ✓ In Role (Role aggregated to the permission) • ✗ Out of Role (Role not aggregated to the permission)
Name	Name of the entitlement.
Application	Name of the application.

Applications

The **Applications** tab lists the Entitlements and Application assigned to the selected User.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

You can sort the displayed data in ascending or descending order, based on the data elements provided.

Table 75. Entitlements

Entitlements	Description
Name	Name of the entitlement.
Application	Name of the application.
Direct Users	Number of users assigned to the selected entitlement.
Permissions	Number of assigned permissions.
Assignments	Number of assignments.
OUs	Number of organization units involved in the selected entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Applications	Number of applications assigned with the entitlement.

Table 76. Application

Application	Description
In/Out	The application status can be one of the following: • ✓ In Role (Role aggregated to the application) • ✗ Out of Role (Role not aggregated to the application)
Name	Name of the application.

Permission Type

The **Permission Type** tab displays the permission types that are already defined for the selected Application. You can also add a new type, modify, or remove an existing permission type when necessary.

The following fields are available:

Field	Description
Name	The name of the permission.
Description	Short description of the permission.

Search

To search for specific permission types, use the **Filter** option. Otherwise, click **Hide Filter**.

1. Click **Filter**.
2. Specify information in the provided fields.
3. Click **Search**. Results matching the specified filter are displayed.

Add

To add a new permission type:

1. Click **Actions** > **Add**.
2. Specify information in the provided fields.
3. Click **Actions** > **Save**.

Modify

To modify a permission type:

1. Edit the information of the selected permission type.
2. Click **Actions** > **Save**.

Remove

To remove the permission type:

1. Select the check box of the permission type.
2. Click **Actions** > **Remove**.
3. In the Remove Permission Type window, click **Ok** to confirm the request.

Accounts

Describes how to customize an account configuration for an application.

The account configuration identifies a set of elements that determine the mode in which a user accesses an application.

The name of the default account that is provided for an application is IDEAS.

The left frame, which is titled Account Configuration, includes the **Name** and **Description** filters that are used to search Accounts (click the **Filter**/**Hide Filter** button to specify them).

In the same frame, you can use the **Actions** > **Add/Remove** button to add or remove an Account.

For more information, see this procedure: “Adding an account” on page 61.

Use the **Details** tab to display details of the selected Account in the left frame. The details are:

Table 77. Account Configuration details

Detail	Description
Name	Name of the selected Account.
Description	Short description of the selected Account.
Fulfillment	You can define the following fulfillment options: • **Automatic** • **Manual** • **Disabled**
Connectors	You can use the following radio-buttons to choose the typology of connectors joined to the selected accounts: • **IDEAS Connectors** • **Third Party**
Linked Applications	Click **New**/**Rename**/**Remove** buttons to specify or remove a set of Markers for the selected Account. You can then select **Manage** > **Applications** > **Details** to join an Application to a Marker specified in this panel.

Click **Save** to enable the selections that are made on the attributes you added or modified.

Further attributes that are enabled for configuration are grouped in the following tabs:

- Details (default tab)
- “Creation Policy”
- “Management” on page 228
- “Password Creation” on page 229
- “Users” on page 231
- “Applications” on page 233
- “Attribute-to-Permission Mapping” on page 233

Related tasks:

“Adding an account” on page 61
Complete this task to register a new account into the Identity Governance and Intelligence data model.

Creation Policy

Describes how to customize the Creation Policy tab of an Account Configuration for an Application.

Use this tab to customize the following attributes:

Table 78. Creation Policy settings

Attribute	Description	
Account	**Disable on creation** If selected, disables by default the new Users aggregated in the selected Account Configuration. **Expiration time (days)** The value can be: - `0`, to indicate that the Account has no expiration date. - `>0`, to indicate the number of days after which the Account expires.	
UserID	**Concatenate user attributes:** Use this text box to join User attributes concatenated by the plus (+) sign. Specify separators between "". For example: `Name + "." Surname + "@" + MailProvider + "." + "com"`	
Password	**Disable password first check** If selected, verifies that the passwords created or modified by an Administrator follow the rules set for: Password creation. **Allow empty password** If selected, allows a login without a password request. **Force Password Change (only for targets that allow it)** If selected, forces a new user, or a user whose password has been modified by the Administrator, to change the password at the next access.	

Click the **Save** button to enable the selections made on these attributes.

Management

Describes how to customize the **Management** tab of an Account Configuration.

Use this tab to customize the Management attributes. These attributes are organized in four sections.

The editing of contents in the **Management** tab, is enabled after the selection of one of the accounts listed in the **Account Configuration** tab.

Some of inners sections are enabled by ticking **Enable** check-box.

The Management attributes are:

Table 79. Account management settings

Attribute	Description
Account expiration policy	**Action to be taken after the account expires** Specifies which of the following actions is to be taken when the account expires: • **None**: no action is taken. • **Suspend**: the Account is suspended and a code numbered from 1 to 9 must be set. Any customer can freely join a proper meaning to these codes. • **Remove**: if the User Account has expired, the User is removed from the selected Account Configuration after a certain number of days, that you can set in **Remove after (days)**. **Expiration lock code** Code value (from 0 to 9) for the expiration blocking code.
Password policy	**Validity from the last login (days)** The time period, expressed in days, at the end of which the account is blocked if the User does not access the system. **Password validity (days)** The number of days between two consecutive password expirations. **Maximum number of passwords retries** The maximum number of consecutive failing attempts, after which the User account is blocked.
Password propagation	**Expiration class**: Allows to enable password transmission, coded with an appropriate algorithm.

Table 79. Account management settings (continued)

Attribute	Description
Password expiration notification	**Notification time (days)**: The number of days before a password expires, that the user is notified of the coming expiration. Use one of these radio-buttons to choose the policy followed when passwords expire: • **Lock account after password expiration** • **Force change password after password expiration**

Click **Save** to enable the selections made on the attributes.

Table 80. Cautionary note

⚠	**CAUTION:** **Any algorithm can be used to encrypt passwords. The chosen algorithm must be implemented in a class, whose path is to be specified in the Algorithm text-box.**

Password Creation

Describes how to customize the Password Creation tab of an Account Configuration defined for an Application.

This tab includes two accordion panes:

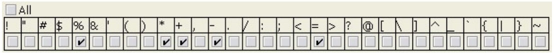
- **Password Creation**
- **Dictionary**

The following attributes are featured in the **Password Creation** accordion pane:

Table 81. Password creation attributes

Attribute	Description
Enable Password Construction	When selected, enables all the attributes that follow to build a password policy.
Minimum Length	Determines the minimum length of a password. Use **No Check** to neutralize this control.
Maximum Length	Determines the maximum length of a password. Use **No Check** to neutralize this control.
Allow Lowercase	Allows the use of lowercase characters.
Minimum Lowercase Characters	Specifies the minimum number of lowercase characters that must be included in a password. Use **No Check** to neutralize this control.
Allow Uppercase	Allows the use of uppercase characters.
Minimum Upper-case Characters	Specifies the minimum number of uppercase characters that must be included in a password. Use **No Check** to neutralize this control.

Table 81. Password creation attributes (continued)

Attribute	Description
Allow Special Characters	Allows the use of special characters (that is, characters that are not numbers or letters of the alphabet). If this checkbox is selected, the special characters to be allowed can be chosen in the lower bar:  □ All ! □ " □ # □ $ □ % ☑ & □ ' □ (□) □ * ☑ + ☑ , □ - ☑ . □ / □ : □ ; □ < □ = ☑ > □ ? □ @ □ [□ \ □] □ ^ □ _ □ ` □ { □ | □ } □ ~ □ Select the **All** checkbox to allow all available special characters.
Minimum Special Characters	Specifies the minimum number of special characters that must be included in a password. Use **No Check** to neutralize this control.
Allow Numerical Characters	Allows the use of numerical characters in passwords.
Minimum Numerical Characters	Specifies the minimum number of numerical characters that must be included in a password. Use **No Check** to neutralize this control.
Exclude ASCII Extended Characters	If this check box is selected, a password cannot contain extended ASCII characters (e.g. ö, ä, ñ, ...).
Verify with Personal Data	If this check box is selected, a password cannot contain the User's personal information (for example, User `Mario` cannot use a password such as `12Mario1971`).
Not equivalent to last Password	Verifies that the new password is not the same as the last password used. Currently, the latest eight passwords are saved, regardless of the enabling of the control; therefore, the user cannot use any of the last eight passwords saved. When comparing the most recent eight passwords, the passwords are not case sensitive.
Default Password	A default password is automatically added when a User Account is created. It can be modified by the Administrator who creates the Account.

Click **Save** to enable the selections made on these attributes.

Note: When building a password at least one of the four character types (lowercase, uppercase, special, numerical) must be allowed (the related checkbox must be selected).

A list of terms and the command keys necessary to manage them can be stored in the **Dictionary** accordion pane.

Select the **Enable Vocabulary** checkbox to check that new or modified passwords do not use invalid terms contained in the dictionary.

The **Actions** menu includes the following buttons:

- **Add**: allows to add a new term in the Dictionary.
- **Remove**: allows to remove a term from the Dictionary.
- **Save**: allows to save the latest selections.
- **Cancel**: allows to cancel the latest selections.

The control on invalid terms can be one of the following:

- **Prompt Search**: the system checks that a new or modified password is not exactly the same (**Exact** checkbox selected) as the word defined in the Dictionary.
- Search with **LIKE** filter: the system checks that a new or modified password does not contain a word defined in the Dictionary (**Exact** checkbox not selected).

Users

You can customize the characteristics of the account configuration of a specific user that is associated to an account.

The **Users** tab contains filters to search users (select the **Filter/Hide Filter**).

The available filters are:

Table 82. User filters

Filter	Description
First Name	Name of the user.
Last Name	Surname of the user.
Master UID	Identifies the user on the AG Core module.
User Account Filter	Click ... **Account Filter** to choose one or more filters that are related to the user account definition.
OU	Click ... **OU Search** to choose the OU of a User.
Hierarchy	If this check-box is selected, the search process is extended to all the hierarchy that start from the root OU specified in the **OU** field.

The **Actions** menu includes the following items:

- **Remove**: removes the selected User-Account.
- **Multiple Account**: changes the configuration of the account that is related to a set of users at the same time.

  For example, you can select N users who are related to the Active Directory (AD) account in the left pane.

  Thus, you can click **Actions** > **Multiple Account**and the Management window opens, where you can change some properties for all users selected (for example, if you must block the N selected user accounts).

The account details of a selected user are shown on the rightmost frame.

Table 83. Account details.

Detail	Description
Applications	Applications that are associated with the account configuration
Master UID	Identifies the user on the AG Core module
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see **Manage** > **Account**). These policies are applied for all the users that are associated to the account that expired.
Last Login	Date of the last login
Last Login Error	Date of the last login error
Number of Login Errors	Number of consecutive login errors. This value is reset to zero when a correct login is made.
Last Password Change	Date of the last password change
First Name	User name
Last Name	User surname
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user
Display Name	Personal data of the user as referred by **Master UID** .
Identity UID	Data incoming from a Target system and associated to the user who is referred by **Master UID** .
Account Attributes	A variable subset of account attributes. This subset is configured in **Manage** > **Accounts** > **Account Attributes**.

Note: In some views, only a subset of the data that is indicated could be shown.

The **Actions** menu in the rightmost frame lists the following actions:

Change Date
Changes the expiration date of the account.

Force Password
Forces the user to change the password at the next login of any of the applications that are associated to the account. A green icon is shown in the column **Force Change Password** of the frame **Users**.

Suspend/Restore
Suspend or restore the account. You can select different reason for suspending it (Technical, Security, Terminated, Expire, Authoritative, Maintenance) and for any reason type, you can set a value 0 - 9.

Change Password
Changes the password of the user that is selected in the **Users** frame.

Reset Login
Resets the last login date and the number of login errors of the user that is selected in the **Users** frame.

Related information:

“Accounts” on page 225
Describes how to customize an account configuration for an application.

Applications

Describes how to customize the Applications tab of an Account Configuration defined for an Application.

This tab shows the Applications aggregated in the Account selected in the left frame. **Name** and **Account** are the filters available for use (click the **Filter/Hide Filter** button to specify them).

Be aware that you might find the ✗ icon in the SoD column , which indicates that the related Application is out of SoD check (see the check-box **Exclude from SoD validation** in section **Manage** > **Applications** > **Details** > **Policy box**).

Attribute-to-Permission Mapping

Use the functions in this tab to map attributes from a target system to permissions in Identity Governance and Intelligence. You also map attribute values from the target system to rights values in Identity Governance and Intelligence. The mapping allows users to request and configure access in Identity Governance and Intelligence that is based on the attribute settings on the target systems.

The table on Attribute-to-Permission Mapping tab shows the attributes that are added to Identity Governance and Intelligence from a target system. If no attributes are added, then the table is empty.

You can add rows to the table by adding attributes individually or by discovering the attributes on a target system. You can also use this table to edit mappings that are imported from a bulk load operation. For more information, see the following topics:

- Chapter 7, “Attribute-to-permission mapping service,” on page 69
- “Adding an attribute-to-permission mapping manually” on page 72
- “Discovering attributes from a target system” on page 75
- “Importing an attribute-to-permission mapping with a bulk load operation” on page 70

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria and then click **Search**.

Table 84. Attribute-to-Permission Mapping table

Column Name	Description
Permission Name	The permission name. If not specified, the attribute name is used by default.
Attribute Name	The attribute name on the target system.
Type	The type of attribute. Possible types are `boolean` and `string`.
Multi-value	Indicates whether the attribute is multi-value or single value.
Required	Indicates whether the attribute is required. When an attribute is required, a default must be specified. When an attribute is not required, a default can be specified or not.

Table 84. Attribute-to-Permission Mapping table (continued)

Column Name	Description
Rights Value	Permission rights that are mapped to the attribute values.
Default	Indicates whether the attribute value is a default value. Only one attribute value may be selected as the default value.

Actions menu

The **Actions** menu includes these options:

Add
Select this option to add an attribute-to-permission mapping to the account.

Remove
Select this option to remove an attribute-to-permission mapping from the account.

Edit
Select this option to edit an attribute-to-permission mapping.

Discover account attributes from target
Select this option to discover account attributes from a target system, import the attribute names, and map them to permissions.

Enable
Select this option to enable an attribute-to-permission mapping that you added individually or that you imported from the target system.

Related concepts:

Chapter 7, “Attribute-to-permission mapping service,” on page 69
Administrators can map account attributes from a target system to permissions in Identity Governance and Intelligence. Administrators can also map allowed values for attributes to rights values, so that you can set a business-friendly name for the rights value.

Related information:

“Insert Attribute-to-Permission Mapping Track” on page 288
Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Account attributes

Access Governance Core supports different policies for managing the account attributes. You can choose a free subset of attributes of a specific account. This subset is associated to users information for all users that are linked to the account.

When you select an account in **Account Configuration**, the **Account Attributes** tab is automatically updated with the related account attributes configured and specified in the column **Name**.

You can manage account attributes of two types:

Standard account
These accounts, can be added through **Manage** > **Accounts** > **Account Configuration** > **Actions** > **Add**.

Accounts directly incoming from Target Administration module
These accounts are recognized by a marker with the prefix *ILC* (see the **Linked Application** box into **Manage** > **Accounts** > **Details**).

If you need to add another attribute to this column and you are considering a standard account, click **Account Configuration** > **Actions** > **Add**.

For information about the procedure, see “Managing attributes related to a standard account” on page 62.

If you need to add another attribute and you are considering an account that is marked as ILC, click **Account Configuration** > **Actions** > **Discover from target**.

For information about the procedure, see “Discovering attributes from an imported account” on page 62.

If you choose a label and click ⋯ `Attribute Localization`, an **Attribute Localization** window opens, where you can set the localization of the label.

Use the first check box on the left to select the corresponding row if you want to remove it, selecting **Actions** > **Remove**.

Select the **Visible** check box to specify that the data column must be displayed.

The **Position** yellow arrows define in which order the data columns are displayed in the system.

Clicking ⋯ `Attribute Localization`, the Attribute Localization window opens, where you can set the localization of the attribute in several languages.

In the **UI Rendering** column, for every datum, you must specify the type of UI element that renders it, as shown in the following list:

- **Textfield**
- **Textarea**
- **Checkbox (true,false)**
- **Checkbox (1,0)**
- **Passwordfield**
- **Date**
- **Date-hours**
- **Date-hours-seconds**

Note:

You can choose **Date**, **Date-hours**, **Date-hours-time** as rendering type for date.

If you set a default value in the **Default Value** position, the format of the default value must comply with the formats that are shared between all the modules.

These product formats are available:

Date `dd/MM/yyyy`

Date-hours
`dd/MM/yyyy HH:mm`

Date-hours-time
`dd/MM/yyyy HH:mm:ss`

To modify the product formats, read the indications that are provided for the Time and Date customization process.

Select **Actions** > **Save** to enable your changes.

Related tasks:

"Managing attributes related to a standard account" on page 62
Complete this task to manage attributes that are related to standard account (not imported through Target Administration Console) and associate these attributes to all the users associated to the account in the Access Governance Core module.

"Discovering attributes from an imported account" on page 62
Complete this task to discover attributes incoming from an account that is imported through Target Administration Console and associate these attributes to all the users associated to the account in the Access Governance Core module.

Resources

Describes how to manage resources.

Resources are entities used by the Organization to run administrative and production procedures. They are organized into Families and Types. A given Family of Resources corresponds to one or more Types, which in turn correspond to one or more Resources. Thus, a Resource cannot be introduced unless at least one Resource Type (paragraph 6.7.2) is already inventoried; introducing a Resource Type is subordinate to pre-selecting a Family of Resources (paragraph 6.7.3) to which the Resource Type is linked.

The name chosen for the Resource must be univocal within the Type it is associated to.

Each Resource is defined within a specific Family and Type.

Filters available for a Resource are listed in the table below:

Table 85. Resource filters

Attribute	Description
Family	Family of the Resource
Type	Resource type
Name	Name used within the Organization to identify the Resource Type
Description	Brief description of the Resource Type

Proceed as follows:

1. In the tab bar select **Settings** > **Resources**.
2. Click the Resource accordion pane.
3. In the left frame, click the **Filter/Hide Filter** button.
4. Set the data filters needed to search among all types.
5. Click the **Search** button.
6. To add a Resource:
   a. In the left frame, click the **Add** button.
      In the right frame, the **Edit** tab becomes active.
   b. Set the attributes for the new resource type.

    c. Click the **Save** button.
    d. Click **Ok** in the window that displays the outcome of the operation.
7. To edit a Resource:
    a. In the left frame, select the resource to be edited.
    b. In the right frame click the **Edit** tab.
    c. Modify the attributes of the resource.
    d. Click the **Save** button.
    e. Click **Ok** in the window that displays the outcome of the operation.
8. To delete a Resource:
    a. In the left frame, select the resource to be deleted.
    b. In the same frame, click the **Delete** button.
    c. Click **Ok** to confirm the operation.
    d. Click **Ok** in the window that displays the outcome of the operation.

Resource Family

A Resource Family is the highest level of abstraction into which Resources can be grouped.

The only available filters are Name and Description. Proceed as follows:

1. In the tab bar select **Settings** > **Resources**.
2. Click the Resources accordion pane.
3. In the left frame, click the **Filter/Hide Filter** button.
4. Set the data filters (Name, Description) needed to search among all families.
5. Click the **Search** button.
6. To add a new Resource Family:
    a. In the left frame, click the **Add** button.
       In the right frame, the **Edit** tab becomes active.
    b. Set the Name and Description attributes for the new family.
    c. Click **Save**.
    d. Click **Ok** in the window that displays the outcome of the operation.
7. To edit a Resource Family:
    a. In the left frame, select the Resource Family to be edited.
    b. In the right frame click the **Edit** tab.
    c. Modify the Name and/or Description attributes.
    d. Click **Save**.
    e. Click **Ok** in the window that displays the outcome of the operation.
8. To delete a Resource Family:
    a. In the left frame, select the Resource Family to be deleted.
    b. In the same frame, click the **Delete** button.
    c. Click **Ok** to confirm the operation.
    d. Click **Ok** in the window that displays the outcome of the operation.

Table 86. Resource note

Note icon	Note content
ℹ	**Note:** The Realms Resource Family is in the Realm Administration created during the installation procedure. This Family of Resources cannot be deleted, since it is required for the operation of the product. If the user attempts to delete it, the system prevents it and displays a warning message.

Resource Types

Resource Types are a more specific classification of a set of Resources and is defined within a specific Family. The filters available for a Resource Type are listed in the table below.

Table 87. Resource Type filters

Attribute	Description
Family	Family of Resource Type.
Name	Name used within the Organization to identify the Resource Type.
Description	Brief description of the Resource Type.

Proceed as follows:

1. In the tab bar select **Settings** > **Resources**.
2. Click the Resource Types accordion pane.
3. In the left frame, click the **Filter/Hide Filter** button.
4. Set the data filters needed to search among all types.
5. Click **Search**.
6. To add a Resource Type:
   - In the left frame, click **Add**.
   - In the right frame, the **Edit** tab becomes active.
   - Set the attributes for the new resource type.
   - Click **Save**.
   - Click **Ok** in the window that displays the outcome of the operation.
7. To edit a Resource Type:
   - In the left frame, select the resource type to be edited.
   - In the right frame click the **Edit** tab.
   - Modify the attributes.
   - Click **Save**.
   - Click **Ok** in the window that displays the outcome of the operation.
8. To delete a Resource Type:
   - In the left frame, select the resource type to be deleted.
   - In the same frame, click the **Delete** button.

- Click **Ok** to confirm the operation.
- Click **Ok** in the window that displays the outcome of the operation.

Table 88. Note about the Administration Resource Type

Note icon	Note content
ℹ	**Note:** The Administration Resource Type is in the Realm Administration created during the installation procedure. This Type of Resources cannot be deleted, since it is required for the operation of the product. If the user attempts to delete it, the system prevents it and displays a warning message.

Resources into Administration Realm

When you are logged in the Administration Realm, the available operations are the same as the other operations shown in this section. The Administration Realm includes special Resources that cannot be removed, since they are required for the platform operations. If the user attempts to delete them by mistake, the system prevents it and displays a warning message.

Related tasks:

"Assigning an administrator role to a user" on page 165
Complete this task to assign an administrator role to a User.

Configure

Configuration topics are grouped into sections.

- Certification Campaigns
- "Certification data sets" on page 246
- Rules
- Flow Processes
- Email
- Hierarchy

Certification campaigns

Certification campaigns can be run on different entities of the data model and on different data sets.

The following features are available for managing a certification campaign.

In the **Certification Search** frame, search certifications for the certification campaign you want. Click **Filter** for **Name**.

The status of a campaign is indicated by the following icons.

- ✓ **active**: Campaign is running and can be managed by reviewers
- ⊘ **stopped**: Campaign is complete
- ⊘ **stopping**: Campaign is waiting to complete

- **new**: New campaign that has never run
- **paused** : Campaign is paused and standing by
- **preview**: Campaign is available for preview before activation. When it is in preview, only the supervisor can examine the attributes of the campaign. The attributes are set to read-only.
- **waiting**: Campaign is waiting to start according to the configured schedule
- **error**: Campaign is in error
- **launched**: Campaign is queued to be run

You manage a campaign by using the **Actions** menu in the left frame. The following items are available.

- **Add** a new campaign
- **Remove** a selected campaign.
- **Launch** a selected campaign.
- **Active**: the campaign is activated and can be run.
- **Pause** a selected campaign.
- **Close** a selected campaign.
- **Preview** a selected campaign. Use this option to inspect the configuration of a campaign. All configurations are shown read-only. You must be a supervisor to preview a campaign.
- **Clone** a selected campaign. The name of cloned campaign is set to `SourceCampaignName_automaticID`, where *SourceCampaignName* is the name of the selected campaign and *automaticID* is a suffix of 13 digits.

If a campaign is in **Preview** state, the supervisor can inspect the attributes of the Campaign. If the configuration is satisfactory, the supervisor would ask to the AGC Administrator to **Launch** the campaign. If not, the supervisor can ask to **Close** it.

The **Close** action sends a request to a system task, which is scheduled through the Task Planner module.

The **Details** tab shows data relative to the selected Campaign.

The following table describes the details of a Campaign:

Campaign Detail	Description
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.

Campaign Detail	Description
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • *Entity* User Signed Off / Total *Entity H/M* Users • Working Progress J/TOT-M – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Click **Save** to save your changes.

The following tabs are shown in the right frame. See the topic for each tab for a description of the functions available.

- **Supervisors**
- **Reviewers**
- **Fulfillment**
- **Scheduling**
- **Notification**
- **View Configuration**

Supervisors

The **Supervisors** tab displays the supervisors in the campaign that is selected in the left frame.

Supervisors have attributes that are shown in the following table:

Attribute	Description
First Name	Given name of the supervisor
Last Name	Surname of the supervisor
Master UID	Master UID of the supervisor user
Org. Unit	Organizational Unit of the Supervisor

For an active campaign, the supervisors are fixed and the **Actions** menu is not active.

For a new campaign, the **Actions** menu shows the following actions.

- **Add** adds a supervisor.
- **Remove** removes a supervisor.

Click **Save** to enable your selections.

Note:

- You must configure at least one supervisor.
- If **Escalation Supervisor** is checked in the **Supervisors** tab, the supervisor can receive escalations from reviewers.

Reviewers

This tab shows all of the reviewers for the selected campaign.

The following table shows reviewer attributes.

Table 89. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	**User Hierarchy** If enabled, shows the available user hierarchy scope. It is always available for organizational units. **Entity** If enabled, shows the entity scope.
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use**Add** and **Remove** to define the reviewer list.

Click **Save** to enable your settings.

Fulfillment

This tab shows the fulfillment activities for the selected campaign.

Some of these options are available only for some campaigns.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set `Grace period=0`. Campaigns on Account have the following options: • `Delete the Account` • `Lock the Account`

Fulfillment Detail	Description
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of *name Process - name Activity*.
Custom Behaviour	The management of the fulfillment involves a set of rules.

Click **Save** to enable your settings.

Scheduling

This tab shows the scheduling for the selected campaign.

The following table shows schedule attributes.

Table 90. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	**Start date** If checked, enables the workflow processes to define the frequency and length of the campaign. **Duration** The following values are available: - 1, 2, or 3 weeks - 1, 2, 4, 6, or 9 months - 1 year - Continuous (never closed)
Execution Frequency	The following values are available: - 1, 2, or 3 weeks - 1, 2, 4, 6, or 9 months - 1 year - One time The set of values is bounded according to the **`Duration`** parameter. If `Duration=Continuous`, you cannot set values for this parameter.
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.

Click **Save** to enable your settings.

Notification

This tab shows the notifications for the selected campaign.

Notifications are sent to **Reviewers** and **Supervisors** in the selected campaign.

The following table shows notification attributes.

Notification Type	Description
Campaign Started for Reviewer	If **Enable** is set, the reviewer receives an email when the campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information about the campaign.
Activity Reminder for Reviewer	If **Enable** is set, the reviewer receives an email at the following times. • *K* days before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. • When the percentage of activity that is already managed is greater than X%. Determined by **Activity percentage** The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Reviewer	If **Enable** is set, the reviewer receives an email *K days* before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Supervisor	If **Enable** is set, the supervisor receives an email *K days* before the end of the campaign. Determined by **Days before end date**, *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Continuous Review for Reviewer	If **Enable** is set, the reviewer receives an email when a continuous campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Redirect	If **Enable** is set, the reviewer or supervisor receives an email in response to any action of redirection. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

Click **Save** to enable your settings.

View Configuration

This tab shows the view configuration of the selected campaign.

This tab appears if **User Certification Campaign** is selected in the left frame.

In this tab, you configure the columns that are shown in the **User View** and **Entitlement View** for the reviewers and supervisors of the Access Certifier module. Chapter 35, “Introduction to Access Certifier,” on page 679

You enable the user and entitlement views by setting the following check boxes:

- **User View**: columns available are fixed.
- **Entitlement View**: columns available are determined by the entitlements that are configured.

The columns available are shown in the following table.

Table 91. Columns for Entitlement View

Column	Description
Attestation buttons	Makes actions visible. • **Approve** • **Revoke** • **Sign Off** • **Notes** • **Redirect** • **Redirect to Supervisors**
Master UID	UID of the user.
User First Name	Given name of the user.
User Last Name	Surname of the user.
User info buttons	Makes user information visible. • **Details** • **Entitlements** • **External Data** • **Accounts** • **Activities** • **Rights**
OU Name - Code	Name and code of the organizational unit (OU).
OU Owner	Owner of the organizational unit, according to the setting in AGC.
OU Description	Short description of the organizational unit.
Application Name	Name of the application, with the information available about the application.
Application Owner	Owner of the application, according to the setting in AGC.
Application Description	Short description about the application.
Entitlement Name	Name of the entitlement. If the **Entitlement Localization** option is active, the entitlement is shown as a localized name.
Entitlement ID Code	ID code of the entitlement.
Entitlement Description	Short description of the entitlement.
Entitlement info button	Makes entitlement information visible. • **Details** • **Structure** • **Activities** • **Rights**

Table 91. Columns for Entitlement View (continued)

Column	Description
VV	Role Alignment Violation property, which is related to an entitlement assigned to a user but not joined to the organizational unit of the user.
User Type Name	Type of user, according to AGC settings.
Group Name [Code]	The IGI Administrator can configure several types of hierarchies that are based on user attributes. Every hierarchy can be made by several groups. A group is an element (a node) of the hierarchy, identifies by a name and a specific code. Every group can be associate to a set of entitlements.
Hierarchy Name	Identifier of the hierarchy. The base hierarchy is ORGANIZATIONAL_UNIT hierarchy.

The position of columns can be changed through the **Up** ⇧ and **Down** ⇩ arrows.

The first column in this list appears as the leftmost column in the view. The last column appears as the rightmost column in the view.

Click **Save** enable your selections.

Certification data sets

A campaign of certification is based on a data set, which is built with elements that are analyzed during the campaign.

The following base entity sets can be used to define a data set.

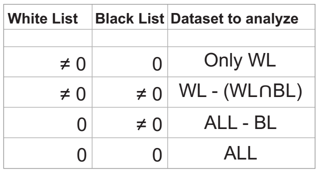
- **Groups**
- **Users**
- **Applications**
- **Entitlements**
- **Risks**
- **Account**
- **Advanced Settings**

For every entity set with exception of **Advanced Settings**, you can set a **White List** and a **Black List** of elements.

White List
Consists of elements to be analyzed.

Black List
Consists of elements that are excluded from analysis.

If an element in the white list is also put in the black list, it is not used for the analysis. The final entity set is determined according to the following table.



White List	Black List	Dataset to analyze
≠ 0	0	Only WL
≠ 0	≠ 0	WL - (WL∩BL)
0	≠ 0	ALL - BL
0	0	ALL

Only for the **Users** entity set, is possible to define a rule for loading a set of users into the **White List**.

The following filters are available for the **White List** and **Black List**.

Table 92. Entity filters

Filter		**Description**
Group	**Name**	Name of the group that you want to include into the data set.
	ID Code	ID code of the group.
	Activity	Click ⋯ **Browse** to choose the activity that is associated with the users through the permission that is associated with the users.
	Hierarchya	If checked, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.

Table 92. Entity filters (continued)

Filter		**Description**
Users	**Rule Flow**	If checked, the combo-box on the right is enabled and you can choose a flow of Rules for filling the User White List.
	First Name	Given name of the user.
	Last Name	Surname of the user.
	Master UID	Univocal identifier of the User
	User Type	Click the arrow and select from the list user types. The user type is defined in your security model.
	UME	Select this check box if the users you are searching have more than one account on the same target system.
	Search Identity	Enter the first name, the last name, or the master UID of the user.
	Associated	If selected, the search result shows only users that are associated with a group. If not checked, the search result shows only users that are not associated with any group. For example, a user might be entered in the database but is not yet associated with any Group.
	Groups	Click ⋯ **Browse** to choose the group of the user.
	Hierarchy	If checked, the search starts from the root that is selected in the **Groups** field and is run on all the hierarchy.
	Activity	Click⋯ **Browse** to choose the activity that is associated with the users through the permission that is associated with the users.
	Hierarchy	If checked, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.
Applications	**Name**	Name of the application.
	Marker	Name of a target system.

Table 92. Entity filters (continued)

Filter		Description
Entitlements	**Type**	Specifies one of the following entitlement types: • Permission • IT Role • Business Role • External Role
	Application	Name of the application that is related to the entitlement
	Name	Name of the entitlement
Risks	**Name**	Name of the risk
	Description	Brief description of the risk
	Type	Type of the risk
Account	**Name**	Name of the account
	Description	Brief description of the account

Related tasks:

"Deploying a new dataset" on page 87

Admin roles

Admin roles are used to manage IBM Security Identity Governance and Intelligence applications.

Admin roles are made up of entitlements. You can view both roles and entitlements in **Admin Roles**.

- Choose a view in the left frame. You can choose **Flat View** or **Hierarchy view**. **Flat View** is shown by default.
- Use filters to control the list of roles. Click **Filter**.
- Use the **Actions** menu to manage roles.

  Add Add a new administrative role

  Remove
  Deletes a selected role

  Publish
  Publishes a role so you can assign it to an OU

  Unpublish
  Unpublishes the role and makes it unavailable to users and OUs.

A role is in one of the following states:

- Published and available to be assigned
- Unpublished and not available to be assigned

A published role can be assigned to the following objects:

- One or more OUs
- One or more users

The following rules govern roles and entitlements.

- Any role or entitlement in the hierarchy can be published and unpublished.
- A newly added entitlement can be published.
- An unpublished role or entitlement is not available for assignment to OUs or users.

The **Details** tab shows data for the selected Admin role. The following table describes it.

Table 93. Admin Role details

Area	Detail	Description
Info	**Version**	A number from 0 to *N* that indicates the version of the role.
	Owner	The user who is responsible for the selected role. Use ⋯ **User** and ⊗ **Clear** to set a user or clear the field.
	Name	The name that is used in the organization to identify the role.
	Code	A code that is used in the organization to identify the role.
	Description	A brief description of the role.
	Type	Indicates one of the following entitlement types: • Business Role • External Role • IT Role • Permission
	Application	The name of the application that is associated with the selected role. Use ⋯ **Application** and ⊗ **Clear** to set an application or clear the field.
	Permission Type	This attribute tags and categorizes a set of permissions into a specific **Type**.
	Entitlement Families	The family of which the selected role is part.
	Expiration	The expiration date of the role. When an entitlement expires, some automatic controls might be run. Use 📅 **Calendar** and ⊗ **Clear** to set a date or clear the field.
	Last Review Date	The date of the last authorized modification on the entitlement.
	Auth Alias	An alias for the role. It can be any string of your liking. The alias is mandatory to assign the role to the activities of a process in Process Designer.
Business info	**Business Name**	This field is for future use.
	Business Policy	This field is for future use.

Every administrative role can be associated to specific properties.

A property consists of a - *Key,Value* - pair of attributes.

Properties can be easily added into a new empty row with **Actions** > **Add**.

Table 94. Property attributes

Attribute	Description
Name	Name of the property.
Description	Description of the property.
Searchable	For future use.
Multivalue	Property can have a set of values rather than a single value.

Use this procedure to set a new property.

Other tabs provide more information on Admin roles:

- "Scope"
- "Management"
- "Org Units" on page 252
- "Users" on page 252

Related tasks:

"Configuring user access to Service Center applications" on page 164
Complete this task to enable Users to access the Application in Service Center. These Applications must be properly configured. Users must have the right Roles to access one or more Application.

Scope

Use the **Scope** tab to choose a scope to join to a role.

When the role is assigned to a user, you are prompted to choose the elements to populate the scope.

Choose from the following scope entities.

- **Org Units**
- **Entitlement**
- **Application**
- **Risk**
- **Attribute Hierarchy**

Management

Use the **Management** tab to build the hierarchy of Admin Roles.

Click **Filter** to narrow the search. The filters available for the entitlements search are shown in the following table.

Table 95. Entitlements filters

Filter	Description
Type	Type of entitlements: • Permission • IT Role • Business Role
Name	Name of the entitlement.

Table 95. Entitlements filters (continued)

Filter	Description
Application	Application that is related to the entitlement. Use … **Application** to insert an application. Use ⊗ **Clear** to clear the field.

The following items are available in the **Actions** menu.

- **Conflicts**: Shows conflict information and the risk tree for the selected roles. You can define mitigation actions in the **Mitigation** tab.
- **Parents**: Shows the entitlement hierarchy of the selected entitlement
- **Add**: Adds a selected entitlement
- **Remove**: Removes a selected entitlement

Org Units

Use the **Org Units** tab to assign organizational units to Admin Roles.

Click **Filter** to narrow the search.

The following filters are available:

Table 96. OU filters

Filter	Description
Group	The name of a specific attribute group. In this case it is the attribute group of organizational units.
Name	The name of a specific group of the hierarchy. In this case it is the name of the OU.
ID Code	The ID of a specific group of the hierarchy.

You can select the following in the **Actions** menu:

- **Add** an OU
- **Remove** a selected OU

Users

Use the **Users** tab to assign users to Admin Roles.

Click **Filter** to narrow the search.

Use **Search Identity** to filter by **Name**, **Surname**, or **Master UID** of the user.

The tab shows all users that have the Admin Role that is selected in the left frame.

In the **Actions** menu, the following actions are available.

- **Edit**: Modify the scope of the user. Change the set of OUs managed by the User according to the selected Admin Role.
- **Add**: Add a user to an Admin Role with the **Add User** window.
- **Remove**: Remove a selected user from an Admin Role.

Rules

Rules are used to manage different types of events or for the automation of particular policies.

For a base introduction on rules, see Chapter 16, “Rules introduction,” on page 129.

The Rule Classes available in Access Governance Core are seven:

Live events
Rules that are triggered by Event Queues (see Events in Integration Interface). These types of events are processed in real time. Their purpose is to control the input/output data flow.

Deferred events
Rules that are triggered by the Event Queue IN. These types of events are processed by scheduling (see Task Planner). Their purpose is to aggregate events.

Authorization Digest
Rules that are triggered by changes in the User data set. These types of events are processed in real time. Their purpose is to validate enforcements.

Account
Rules for the creation of a user account.

Advanced
Rules that can be scheduled through Task Planner.

Attestation
Rules that are automatically applied in campaigns of attestation.

Hierarchy
Rules for the automatic building of hierarchies based on user attributes.

You can select the class of Rules in the filter section (click **Filter** button).

The filtering approach requires the selection of a **Rule Class** and according to the class, you can select from **Queues** or **Rule Sequnece (Flow)** combo boxes.

The **Actions** menu of the tab **Rules** in the left frame lists the following actions:

Import
For importing the XML representation of a Rule or of a Rule Sequence (Rule Flow).

Export For exporting a Rule or a Rule Sequence (Rule Flow).

Add Adds a Group of Rules (function that is maintained for legacy reason).

Remove
Removes a Rule or a Group of rules (for Groups, function that is maintained for legacy reason).

Enable/Disable
Enable or disable a Rule execution into a sequence.

Move Up/Down
Move the Rule up/down in the Rule sequence.

In the right frame you can find two main accordion panes:

Rules Package
In this accordion pane is available all functions for managing a Rule that is selected in the left frame.

Package Imports
In this accordion pane is present all functions for managing packages of rules.

Rules Package

This pane includes functions that manage rules with the Rules editor.

Based on your selections in the left tab **Rules**, a set of rule are listed in this pane.

The **Actions** menu lists the following actions:

Verify Checks the formal structure of the code that defines a rule (needs the selection of one of the rule listed).

Modify
Opens the Rules editor to modify a rule.

Delete Deletes a selected rule.

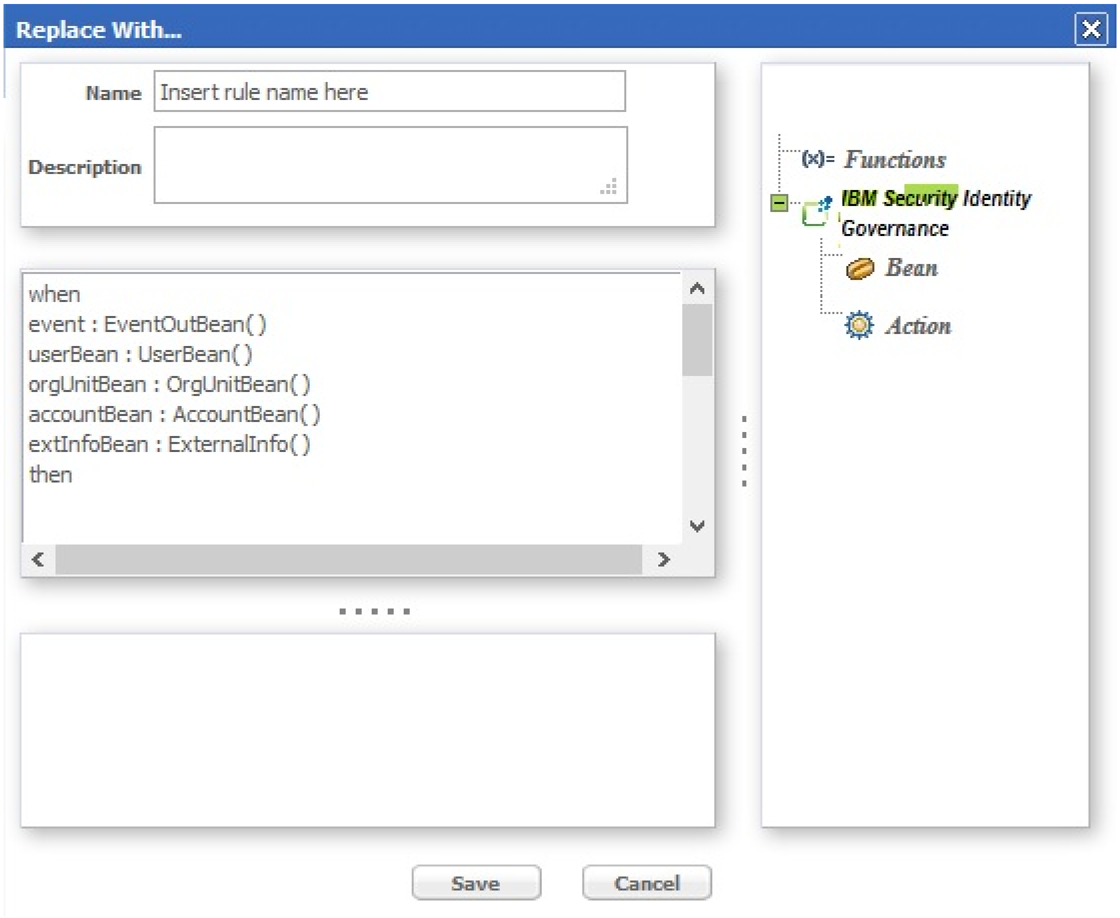
Create Creates a rule.

Add
Adds a rule that is selected in the list to a **Group** (legacy versions) or **Rule Sequence** that is selected in the **Rules** tab, on the left.

Rules Editor

The Rules Editor speeds up the writing of code contained in a Rule.

The next figure shows the Rules Editor panel:



```
when
event : EventOutBean()
userBean : UserBean()
orgUnitBean : OrgUnitBean()
accountBean : AccountBean()
extInfoBean : ExternalInfo()
then
```

Figure 48. The Rules Editor panel.

The next table shows what buttons and icons are present in the Rules editor:

Table 97. Symbols of the Rules editor.

Icon	Description
C	Import a Java class
C	Java class
▤	New variable
(x)=	New function
⬬	Bean
⚙	Action
▨	Associated rule: rule that is associated to a rules group
◇	Split: used to construct flow processes in situations that require a branch point.
◇	Constraints
📁	Rules group

Table 97. Symbols of the Rules editor. (continued)

Icon	Description
	Flow process

All the Rules must have the following structure:

- **Condition Area** (between “when” and “then”)
- **Action Area** (immediately after “then”).

The word **when** identifies the beginning of the conditions area.

Any number of conditions can be inserted and the actions will be executed only if all the conditions are verified (logic AND between each condition)

The word **then** identifies the beginning of the actions area.

Actions are written in normal Java code; all classes making up the libraries delivered with the product are available for writing actions.

A complete list and descriptions are available in the **Replace with...**.

The conditions are written according to Drools syntax.

Every condition verifies, within the Working Memory, whether or not there are one or more objects identified by the Beans. If such objects are actually found, the actions described above will be executed on them.

The **Replace with...** window contains the code obtained from the Editor.

From the frame on the right side of the window, predefined code blocks can be selected and placed directly into the **Replace with...**.

The objects are grouped in a hierarchy and managed through a tree structure.

The **Object** frame contains the nodes corresponding to the higher level object categories. The two initial main categories are:

- Functions
- Ideas

Based on the selection, the objects can be **Functions**, **Bean** or **Action** and their methods are visible below the selected object (fourth level of the tree):

Now, select a leaf object (a method) and insert it into the **Replace With...** frame (left) using the **Actions**>**Add** button.

This operation can be performed to modify or create a Rule.

Note: The name of a Bean can be written without its system path ONLY if it has been imported into the Package that contains the Rule.

Functions

The Functions category contains functions for fundamental Rule-writing constructs; the same frame lists the following four elements:

- if
- ifelse
- ifelseif
- for

Select one of the functions and click **Add** to insert the related parametric code into the **Replace with...** frame, at the end of the already-listed code. The parameters to edit are easily recognized because they are between two '$' symbols.

For example, in the IF ELSE construct, you have to edit the parameters CONDITION1, ACTION1 and ACTION2.

Proceed in one of two ways to edit the parameters:
- Directly write the code instead of the corresponding symbolic string (e.g., CONDTION1 included between two '$' characters);
- Use the editor again.

In this last case, click **Field** > **Bean** > **AccountBean** and select one of the objects listed, then click **Add**:

Selecting $ACTION2$ places the selected code block in the position that was covered by $ACTION2$. If none of the parameters in the window are selected, click **Ok** to place the code block at the end of the already-present code. To eliminate a potentially wrong insertion, cancel the corresponding code directly in the **Replace With...** frame.

Bean and Action Elements

The IBM Security Identity Governance folder contains the following two folders:
- Bean
- Action

These folders contain ALL the Beans and Actions imported into the Rules Package; in particular, the Bean folder contains the Beans imported into the Package that are part of the libraries delivered with the product. Client users of the AG Core can create additional personalized Beans.

This paragraph analyzes how to use a Bean in the Bean folder. By selecting Bean, the content of the Bean folder is presented in the form of a tree, where every Bean is a node and its child nodes represent its methods.

After selecting the Bean, click Add to insert it into the **Replace With...** frame.

Be sure to insert a semicolon (;) at the end of each line and put the code in order.

Be sure to assign the String parameter a string that makes sense.

The Action folders contain ALL Actions imported into the Package of the selected Rule; in particular, the Action folder contains all Actions imported into the Package that are part of the libraries delivered with the product.

The procedure for inserting Actions (even custom Actions) is exactly the same as that for inserting Beans.

Package Import

This pane includes functions that import and configure rule packages.

From the tabs bar, select **Configure** > **Rules** then click on the **Package Import** accordion pane on the right.

Configuring a Package consists of declaring certain objects available to all Rules in the Package.

Such a declaration consists of specifying an appropriate Java code in the allotted text box.

To make configuration of the Packages easier, insert blocks of predefined code (on the right side of the frame there is a small vertical toolbar with buttons).

The following actions are available for each Package:

- Import specific classes
- Insert variables
- Insert functions

The Rules programmer can write the Rule's code to directly call the objects that are set up for the Package containing the Rule.

Importing a class into a Package adds a class to a Rule without having to specify the entire path.

For example, after importing the class UserBean() into the Package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

Package Editor

An administrator familiar with programming languages can insert any object in the Package by writing the code directly in the text box.

A Package Editor is also available to assist administrators to accomplish this task.

The Editor uses the following buttons, located on the right-hand side of the text box:

- New Import
- New Variable
- New Function

Variables usually support objects that are already instanced with global visibility to all the Rules of the Package; if, for example, there is an object that contains all the parameters required to connect to the DB, the object can be assigned to an "sql" variable (always visible to the Package's Rules) and can be used in the Rule code, as shown in figure above.

Lastly, it is possible to create Functions that always have global visibility to all the rules of a package. For example, if several rules request an operation for the arithmetic average of two numbers, this can be created directly in the Package instead of in each single rule.

Import a Class

To import a class, click on **New Import** button in the vertical toolbar on the right-hand side of the Package Imports pane.

The Classes window opens (figure below) with a list of available classes

Choose a class, then click **Ok**.

The Java code corresponding to the selected class is written in the text area on the right-hand side of the Replace With... window.

Enter a New Variable

To insert a new variable, click on **New Variable** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Insert the object (specify entire system path) in the space <your class here>.

Insert a variable name in the space <variable name>; this name can then be used in every Rule of the Package.

Enter a New Function

To insert a new function click on (x)= **New Function** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Edit the parameters as follows:
- Replace <return Type> with the type of objects that result from processing the function (e.g. an integer, a string, a class, etc.).
- Replace <args here> with the list of parameters given to the function at input.
- {} needs to contain the body of the function, i.e., all the code that implements the function.

How to schedule a rule sequence

You can link a sequence of rules to a scheduled job.

The Task Planner module is dedicated to scheduling several types of jobs that optimize different tasks in the Identity Governance and Intelligence platform.

After you create a rule flow in Access Governance Core or in other modules, open the upper toolbar and click .

In Task Planner, select **Manage** > **Jobs** to access the Job Classes GUI.

From the list of **Job Classes**, choose AdvancedRuleFlow or DeferredEventsRuleFlow (depending on what your requirement is) and choose a relevant job from the resulting list.

In the lower frame of the **Details** tab, you find the parameters of the Job Class that you can set with the suitable values.

Concept of Rules Sequence

A sequence of rules is a structure that is used for grouping set of rules.

A Rules Sequence manages different Rule Groups.

Each sequence MUST have only one start point and one end point.

It's a best practice to use a sequence for managing a large quantity of rules and objects.

Starting from the Rule Classes Authorization Digest and Advanced, it is possible to create a custom Rules Sequence.

The left frame lists the registered custom Rules Sequences.

The following search filters are available (click **Filter/Hide Filter**):

Flow Process filters	
Filter	**Description**
Rules Class	In this field, the type of Rules Class associated with the Flow Process: • **Authorization Digest** • **Advanced**
Name	Process Name

In the **Actions** menu, are hosted these functions:

- **Add** adds Flow Processes.
- **Remove** removes Flow Processes.

Click **Save** to save your changes.

After a Flow is added, it is listed in the **Rules Flow** combo-box in the frame **Configure** > **Rule** > **Rules Sequence**.

Configuring and managing notifications by email or SMS

Select the **Notifications** tabs to configure and manage email and SMS notifications sent from Identity Governance and Intelligence. Use this service to send service notifications from several Identity Governance and Intelligence modules.

Select the following tabs:

Notification Settings
To configure basic and advanced settings.

Notification Templates

To set up templates based on email or SMS types. You can then link the templates to work flows that are defined for Access Requests, Access Certifier, reporting, and more, and send the emails or SMS messages automatically as intermediate or post-action steps.

Notification Monitoring

To view and manage a list of the jobs that ran to send email and SMS notifications.

Configuring notification settings

Select **Notification Settings** to set up the email and SMS notification service.

Configure the following basic and advanced settings:

Table 98. Email settings.

Settings type	Attribute	Description
Basic email settings	Sender email	The email address of the author of a notification.
Advanced email settings	Debug mode	If selected, debug data is sent to the email address specified in the **Static Recipient** text area.
	Static Recipient	The email address to which debug data is sent if **Debug mode** is flagged.
	Aggregation	Choose one of the following options to optimize the email service: **None** No special policy is applied. **Same Message** With this policy, the body text of more emails can be merged into a single message. **Same Recipient** With this policy, if an email is duplicated, only one email is sent to the recipient.

Table 98. Email settings. (continued)

Settings type	Attribute	Description
SMS settings	SMS enabled	Flag this check box to enable notifications by SMS
	SMS username	The user ID that is required to access the SMS service
	SMS password	The password that is required to access the SMS service
	SMS url	The URL where the SMS service can be accessed
	SMS port	The port number of the internet host that provides the SMS service

Use the **Test email** tab to send emails that test your templates. Follow these steps:

1. Make sure that the `EmailService` task in Task Planner is active.
2. Click **Test email** to display the Test Email window.
3. Click the arrow in **Template** to scroll the list of defined templates and pick the one that you want to test.
4. Make sure the **From** field has a value. If not so, enter an address in the **Sender email** field in the Email settings window and click **Test email** again.
5. In the **Recipient** section, enter the email addresses of the recipient, and, when required, of the carbon copy and blind carbon copy recipients. If more recipients are in one line, separate their email addresses with semicolons.
6. The **Params** section shows a field for every placeholder you added in the template. Manually enter values to resolve the placeholders in the email. If you do not enter values, blanks are shown in their place in the email.
7. Click **Ok** to send the test email.
8. Go to the Notification Monitoring window to check that the job that sent the email completed successfully.

Use the **Test SMS** tab to send SMS messages that test your templates. Follow these steps:

1. Make sure that the `EmailService` task in Task Planner is active.
2. Click **Test SMS** to display the Test SMS window.
3. Click the arrow in **Template** to scroll the list of defined templates and pick the one that you want to test.
4. Type the telephone number of the recipient of the SMS message in **To**.
5. Click **Ok** to send the test SMS.
6. Go to the Notification Monitoring window to check that the job that sent the SMS completed successfully.

Click **Save** to save your changes or **Cancel** to revoke them.

Defining notification templates

Select the **Notification Templates** tab to define and manage email and SMS templates based on the type of message.

The left pane of the window displays the already defined templates listed by **Type**.

To search for specific templates, click **Filter** and use any combination of the **Type**, **Name**, and **Description** attributes.

Select a template to view or edit its definition in the right pane of the window.

Click the **Actions** menu to add a template definition or to remove a selected one.

You can define templates for email notifications, SMS notifications, and both email and SMS notifications.

Adding a template requires that you define the attributes displayed in the right pane and listed in the following table:

Table 99. Notification template attributes

Section	Attribute	Description
Template information	**Type**	The type of template. Types are defined in Identity Governance and Intelligence. Choose one of these types: **Static** Choose this template for emails or SMS messages that are not associated with particular work flows and do not require the use of placeholders. **Access Request** Choose this template for emails or SMS messages associated with work flows for Access Requests. **Access Certifier** Choose this template for emails or SMS messages associated with work flows for Access Certifier. **CrossReport** Choose this template for emails or SMS messages associated with reporting tasks. **Reminder** Choose this template for emails or SMS messages that are sent as reminders before or after the expiration of an authorization request. They are associated with processes of type WorkFlow.
	Name	A name that identifies the template
	Description	A brief description of the template
	Enable SMS	Select to associate the template definition with an SMS message. Flag this check box also to define a template for both email and SMS notifications. **Remember:** The **SMS enabled** check box in Notification Settings must also be flagged.
Language tabs	A tab for each supported language in addition to the default language of the browser in use. A template can have multiple language versions, but a definition in the Default language is always required. Select a language tab and proceed to write your message. As you write, the corresponding language tab is marked by an asterisk until you save the template.	

Table 99. Notification template attributes (continued)

Section	Attribute	Description
Notification content	**Email Subject**	The subject of the email expressed in the available languages, selectable using the specific tab. To display a list of placeholder keys available for the chosen type of template, select ℹ . Select the placeholders and click **Ok** to add them in the text. The placeholders are resolved at `send` time.
	Email Body	The body of the email expressed in the available languages, selectable using the specific tab. To display a list of placeholder keys available for the chosen type of template, select ℹ. Select the placeholders and click **Ok** to add them in the text. The placeholders are resolved at `send` time. The scrollable text Box is editor-like with options for inserting lists, images, hyperlinks, and formatted text. You can write the body in plain text or in HTML. The body is saved in HTML format. Select the options at the foot of the text boxes to validate the placeholders or to work with the HTML versions of the email body.
	SMS Body	The text of the SMS message expressed in the available languages, selectable using the specific tab. This field becomes available only if you select **Enable SMS**. To display a list of placeholder keys available for the chosen type of template, select ℹ . Select the placeholders and click **Ok** to add them in the text. The placeholders are resolved at `send` time. Click **Validate** to validate the placeholders.
Notification options	**Validate**	Checks that the placeholders added in the notification are in line with the specified type of template.
	View Html	Shows a window with the HTML version of the email body. Does not apply to the SMS body.
	Import Html	Opens a window where you can paste content in HTML copied from another template or source. When you click **Ok**, the content is imported into the current template. Applies only to the email body.

When you click **Save** on the template definition, the asterisks displayed next to the unsaved language tabs are removed.

Placeholder keys available for notification templates:

You can add placeholder keys in the templates that you use for your service notifications. They are linked to configuration parameters of the related work flows. They are resolved with the values that the manager or operator who carries out the work flow enters at execution time.

The placeholder keys are particular to the type of template. When you select them in the Placeholders window, the program writes them in your template in the following syntax.

```
${placeholder}
```

The following table lists the keys by the type of template.

Table 100. Placeholders for notification templates

Type of email template	Placeholder
Static	No placeholders
Access Request	*beneficiary.userid*
	beneficiary.name
	beneficiary.surname
	applicant.userid
	applicant.name
	applicant.surname
	delegator.userid
	delegator.name
	delegator.surname
	subrequest.id
	request.id
	request.type
	request.status
	account.name
	account.password
	roles.name
	main.role.name
	role.fields
Access Certifier	*attestation.campaign.sender.name*
	attestation.campaign.sender.surname
	attestation.campaign.recipient.name
	attestation.campaign.recipient.surname
	attestation.campaign.name
	attestation.campaign.completion.percentage
	attestation.campaign.redirect
	attestation.campaign.escalation
	attestation.campaign.supervisor
	attestation.campaign.signoff
	attestation.campaign.start.date
	attestation.campaign.end.date
	attestation.campaign.type

Table 100. Placeholders for notification templates (continued)

Type of email template	Placeholder
CrossReport	*report.name*
	report.category
	report.format
	report.rowcount
	report.passphrase
Reminder	*beneficiary.userid*
	beneficiary.name
	beneficiary.surname
	applicant.userid
	applicant.name
	applicant.surname
	subrequest.id
	request.id
	request.type
	request.status

Tracking your notifications

Select the **Notification Monitoring** tab to view a list of the jobs that were run to send email and SMS notifications linked to the execution of work flows.

The jobs are run by the `EmailService` task of Task Planner, which must be in the active status.

The jobs are triggered at the end or during the execution of work flows that are configured to send a notification email or SMS at certain steps of their execution. A job is also triggered when you use the **Test email** or **Test SMS** tool in Notification Settings.

The list that you see in this window shows the jobs that were run up to the present. The list shows the following information about every job ID:

- The name of the template used for the notification
- The status of the job (`Pending`, `Completed`, `Error`)
- The application from where the notification was sent
- An identifier of the associated notification template
- Time-related information

Select a job to see further details about the sent notification in the lower part of the window. Here, you can read the following information:

- The sender and the recipient. If the notification was an SMS, the telephone number of the recipient is displayed. If the notification was sent by email, the email address of the recipient and of extra carbon copy recipients is shown.
- The language used
- The subject matter

To remove a line from the list, select a job and then select **Actions** > **Remove**.

Hierarchy (Polyarchies)

In the IBM Security Identity Governance model, polyarchies provide different organizational views in a hierarchical notation.

A generic hierarchy is based on a specific user attribute.

An additional hierarchy can be created at any moment by grouping users on attribute values.

If the attribute contains a hierarchy path, this is converted to a hierarchical notation.

Attributes can be classified as:

- **Single Value**
- **Multi Value**
- **Hierarchy**

In the following figure:

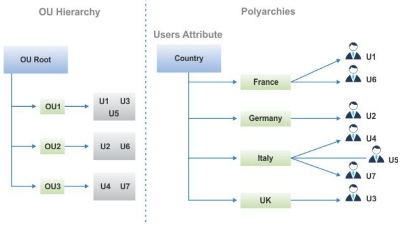


Figure 49. Example: classic OU hierarchy and flat Polyarchy single-value

The polyarchy above shows users grouped on the **Country** attribute.

In the typical organization units hierarchy, we can represent a set of users belonging to the same OU. But a set of users can stay in the same OU and can operate from different geographical locations.

In the example above U1, U3 and U5 are in the same OU1; but if they are grouped by attribute **_COUNTRY**, U1, U3 and U5 will be displayed on three different countries.

This example shows a flat polyarchy created by setting the single value option.

How is it possible to know in which cities of France the users U1 and U6 are working?

The users U1 and the U6, as described in the previous example, have the same attribute value “France”. In this case, to know the city of the users, we can set the option **Hierarchy Value** instead of the **Single Value**.

If the needed data are stored in the database (if the attribute contains a hierarchy path), the result will be as shown in the sample below:

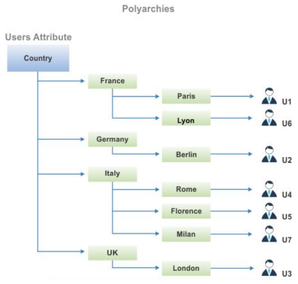


Figure 50. Example of polyarchy in which the attribute contains hierarchy path

This means that for user U1:

_COUNTRY=Country;France;Paris

while for user U5:

_COUNTRY=Country;Italy;Florence

In another example, if **_LOCALITY** is the attribute selected to represent a hierarchy and we have two locations in Frankfurt (Frankfurt 1 and Frankfurt 2), we can create a virtual location named Frankfurt as a father of the two, otherwise it will be represented as a flat hierarchy:

_LOCALITY=Frankfurt;Frankfurt2

In the **Configure** > **Hierarchy** tab, you can build any hierarchy by clicking **Actions>Add** (left frame) and configuring the attributes shown in the **Details** tab (right).

The hierarchy is built by a job that can be scheduled with the `AttributeHierarchyRefresh` task (**Task Planner** > **Manage** > **Tasks**), and activated by the **Actions>Build** button.

The elements needed to define a new Hierarchy are described in the following table:

Detail	Description
`Name`	Name used to identify the hierarchy.
`Description`	Brief description of the hierarchy.

Detail	Description
Conf Type	Manual: is built an empty hierarchy, only joined to the Name and listed in the combo-box Hierarchy available under **Manage** > **Groups**.
	Simple: allows the selection from the Field combo-box of the user attribute on which the hierarchy is built. The available set of attributes is the same set involved in the virtualization process defined in **Settings** > **Core Configurations** > **User Virtual Attributes tab**.
	Advanced: allows the building of the attribute group according to a rule selectable by the Rule combo-box, with three different options: • Auto: The selected rule is used to build the attribute group and to join the users to the nodes of the hierarchy. The hierarchy is automatically updated by AttributeHierarchyRefresh • Once: The selected rule is used to build the attribute group "one-shot", without the refreshing action managed by AttributeHierarchyRefresh task.
Value	The available values are: • Single Value • Multi Value • Hierarchy
Separator Char	This item must be indicated if the **Multi Value** (for example _PHONENUMBER) or the **Hierarchy** value is specified in the row above.
UserID Attribute (Authomatic Scope Assignment)	If this check box is ticked, the role selected into the **UserID Assigned Role** combo-box, is assigned automatically to the users involved in the attribute group selected in the left tab, with the scope policy defined by the check box **UserID Hierarchy**.
UserID Assigned Role	This combo-box hosts all the Administrative Roles available for the users involved in the attribute group.
UserID Hierarchy	If this check box is ticked, the generic user, to the level K of the hierarchy, will see all the users on levels K+1, K+2,... up to the last level of the hierarchy. Otherwise, he will see only the user of level K+1. **Note:** Root of the hierarchy is at level K=0

After the building of the hierarchy, in the **Configure** > **Hierarchy** > **User** tab, you can view:

- The nodes of the hierarchy according to different views (**View** or **Search** tabs)
- The users joined to the node of the hierarchy selected in the **View** or **Search** tabs

"Creating an attribute hierarchy" on page 106
Complete this task every time you need to a build a hierarchy.

"Configuring the attribute hierarchy" on page 106
Complete this task to create a hierarchy to structure the organizational unit.

Rights Lookup

You can define the lookup tables sets for managing rights with lookup.

In the left frame, you can filter by **Name** the list of tables (click **Filter**/**Hide Filter**).

In the **Actions** menu, you can create or delete tables.

For each table selected in the left frame, it is possible to add, in the right frame, a new value, adding a row through **Actions** > **Add** and setting the new value.

You must define a specific value that is associated to an optional short description, but also an optional *technical value*, that is a value with a specific meaning for the organization.

These values are used during the assignment of rights to a permission (see **Manage** > **Applications** > **Application Access** > **Rights**).

Monitor

You can monitor some elements.

The functions that are available for monitoring some elements are contained in the following list.

- "Report"
- "Role Compare"
- "Scheduled tasks" on page 272
- "TARGET inbound - Account events" on page 272
- "TARGET inbound - Access events" on page 275
- "OUT events" on page 277
- "IN - User events" on page 279
- "IN - Org. Unit events" on page 281
- "INTERNAL events" on page 282

Report

Scheduling and downloading are the main functions in Reports.

- Request schedules reports.
- Download downloads reports.

For unauthorized users, this menu is not available.

Role Compare

With this tab you can compare roles to verify if there are redundancies amongst roles and to optimize their definitions. For example, if you find that two or more role definitions specify similar things without a real requirement, you can reduce the definitions to just one single role.

To compare roles, you are first asked to specify the scope of the roles that you want to compare:

1. In the **Scope** field, select `OU` or `Application`.
2. In the field below, that can be **OU** or **Application** based on your previous choice, enter the name of the OU or application whose roles you want to compare. Alternatively, click the elipsis (...) button to get a list from which you can select your entity. A click of the elipsis opens another window that, based on the scope you selected helps you select an application or view and search an Organization Unit.

   If the scope is **OU**, you can flag the **Hierarchy** checkbox to have the roles of the Organization Unit listed in a hierarchical sequence.

After you specify the Organization Unit or the Application, all the defined roles associated within the entity are displayed in the list below. You can also use the filter fields to list specific roles and to sort roles in a particular order.

Roles are listed in tabular form displaying the following details:

Table 101. Details of roles listed for comparison.

Attribute	Description
Name	The name of the role (entitlement) preceded by the symbol that indicates the type: Permission, IT Role, Business Role, External Role. If the role name is shown in red, the role cannot be used for comparison because it is not assigned.
Application	The name of the application (set of roles and permissions) to which the role belongs. This column is blank when the scope is `OU`, and shows the name of the selected application when the scope is `Application`.
Direct Users	The number of users to whom the role is assigned directly (that is, not as a child of another assigned role).
Similarity Between Users	When you run a comparison between a selected role and all the other roles in the list, this column becomes populated with the percentage similarity in direct users of the entitlement in the row with the comparison role. For example, a 100% value, means that the two entitlements (including all their permissions) are assigned to the same user.
Permissions	The number of permissions included in the entitlement.
Similarity Between Permissions	When you run a comparison between a selected role and all the other roles in the list, this column becomes populated with the percentage similarity in permissions of the entitlement in the row with the comparison role. For example, a 100% value, means that the two entitlements include exactly the same permissions.

Table 101. Details of roles listed for comparison. (continued)

Attribute	Description
Assignments	The total number of direct and hierarchical (that is, as child role) assignments of the entitlement.
OUs	The number of Organization Units to which the entitlements are assigned through their user members.
OU Spread	A numeric index that provides an estimate of the homogeneous diffusion of a role in the hierarchical structure of an organization. If the spread value is very high, the role is not homogeneously scattered over a large number of OUs.
Applications	The number of applications that comprise this entitlement in their set of permissions and roles, if the scope is `OU`. If the scope is `Application`, the number is just 1.

To run the comparison, select the entitlement against which you want to compare the other entitlements in the list and click **Compare**. Then:

- The row of the entitlement is moved to the top and turns red
- The following columns of all entitlements become populated with percentages in similarity of direct users or permissions, respectively:
  - **Similarity Between Users**
  - **Similarity Between Permissions**
- The right panel becomes populated with a number of tabs that provide further details on the selected entitlement:

  Entitlement Details

  Map of Permissions

  Permissions

  Applications

  Users

  Organization Units

Scheduled tasks

In this section are displayed all the scheduled tasks which are running or just started.

In the **Actions** menu, the **Remove** button allows you to remove the scheduled tasks from the list.

These tasks are scheduled using the Task Planner module.

TARGET inbound - Account events

In this section you can monitor events, related to accounts, incoming from the target systems.

Events related to accounts on the targets can be filtered as described in the following table:

Table 102. Filters you can specify to list Target inbound - account events.

Filter	Description
Status	Event status can be one of the following values: • Unprocessed • Success • Error
Operation	Indicates the type of available operation: • Add permissions • Remove permissions • Disable user • Enable user • Create user • Remove user • Add right • Remove right • Entitlement add child • Entitlement remove child • Custom
Operation Code	Indicates the customized code of a specific event. It is selectable only if the **Operation** filter is set on **Custom**.
Account ID	Identifier of the account involved in the event.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Trace	Brief description of the error cause.
Process ID	An identifier assigned by the target system to one or more events.
Event Start-End Date	Filters defining the time period for searching events.

The target inbound - account events are listed in a table showing the following details:

Table 103. Target inbound - account event details.

Field	Description
ID	The event identifier, a sequential number.
Process ID	An identifier assigned by the target system to one or more events. This information can be used when writing rules to identify events or sets of events.
Account ID	The identifier of the account involved in the event.

Table 103. Target inbound - account event details. (continued)

Field	Description
Operation	The operation made on the account: • Add permissions • Remove permissions • Disable user • Enable user • Create user • Remove user • Add right • Remove right • Entitlement add child • Entitlement remove child • Custom
Status	The event status can be one of these values: • Unprocessed • Success • Error
Trace	A short description of the error.
Detail	Optionally provided by the target system.
Marker	The marker of the event. It may coincide with the identifier of the target system.
Permission	The permission that was added or removed.
Permission Type	The type of the permission that was added or removed.
Name	Personal data of the user subjected to a `create`, `remove`, `enable`, or `disable user` operation.
Surname	Personal data of the user subjected to a `create`, `remove`, `enable`, or `disable user` operation.
Email	Personal data of the user subjected to a `create`, `remove`, `enable`, or `disable user` operation.
DN	Personal data of the user subjected to a `create`, `remove`, `enable`, or `disable user` operation.
Display Name	Personal data of the user subjected to a `create`, `remove`, `enable`, or `disable user` operation.
Identity UID	Personal data of the user subjected to a `create`, `remove`, `enable`, or `disable user` operation.
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The user who caused the event on the external table.

The following options become available when you click **Actions**:

Details
Displays additional details of a selected event in the TargetEvent window.

Re-Execute
Runs again the operation of a selected event.

Delete all filtered
Removes all the events resulting from a specific filtered search.

Remove
Removes the selected event.

TARGET inbound - Access events

In this section you can monitor events, related to operations of role creation or deletion, as well as of addition or removal of child roles, incoming from target systems.

Events related to the creation or deletion of roles incoming from (external) targets can be filtered as described in the following table:

Table 104. Filters you can specify to list Target inbound - Access events.

Filter	Description
Status	Event status can be one of the following values: • Unprocessed • Success • Error
Operation	Indicates the type of operation associated with the event: • Create External Role • Delete External Role • Add External Role Child • Remove External Role Child
Operation Code	Not used.
Process ID	An identifier assigned by the target system to one or more events.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Trace	Brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The target inbound - access events are listed in a table showing the following details:

Table 105. Target inbound - access event details.

Field	Description
ID	The event identifier, a sequential number.
Process ID	An identifier assigned by the target system to one or more events. This information can be used when writing rules to identify events or sets of events.

Table 105. Target inbound - access event details. (continued)

Field	Description
Operation	The operation associated with the event. Can be one of the following: • Create External Role • Delete External Role • Add External Role Child • Remove External Role Child
Status	The event status can be one of these values: • Unprocessed • Success • Error
Trace	A short description of the error.
Marker	The marker of the event. It may coincide with the identifier of the target system.
Master Application	The name of the application that includes the external role implicated in the event.
Master name	The name of the created or deleted external role for which the event was started.
Master type	The type of external role. It can be a permission or an external role.
Master entitlement type	The entitlement type identifier of the permission or external role.
Master Description	A short description of the permission or external role.
Child Marker	For events involving the addition or removal of an external role child, it is the marker of the event. It may coincide with the identifier of the target system.
Child Application	The name of the application that includes the external role child implicated in the event.
Child name	The name of the added or removed external role child for which the event was started.
Child type	The type of the external role child. It can be a permission or an external role.
Child entitlement type	The entitlement type identifier of the external role child.
Child Description	A short description of the external role child.
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The user who caused the event on the external table.

The following options become available when you click **Actions**:

Details
Displays additional details of a selected event in the TargetEvent window.

Re-Execute
Runs again the operation of a selected event.

Delete all filtered
Removes all the events resulting from a specific filtered search.

Remove
Removes the selected event.

OUT events

In this section you can monitor all events related to definitions of Users in output to external targets.

Output events can be filtered as described in the following table:

Table 106. OUT queue filters

Filter	Description
Status	Event status can be one of the following values: • Unprocessed • Success • Error
Operation	Indicates the type of available operation: • Add permissions • Remove permissions • Disable user • Enable user • Create user • Remove user • Add right • Remove right • Entitlement add child • Entitlement remove child • Custom
Operation Code	Indicates the customized code of a specific event. It is selectable only if the **Operation** filter is set on **Custom**.
Account ID	Identifier of the account involved in the event.
Trace	Brief description of the error cause.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Event Start-End Date	Filters defining the time period for searching events.

Every event is characterized by a the following attributes.

Table 107. Attributes of OUT events.

Field	Description
ID	Event identifier.
Account ID	Account identifier, related to the target system involved by the out event.
Master UID	Univocal identifier of the user.

Table 107. Attributes of OUT events. (continued)

Field	Description
Operation	Indicates the type of available operation: • Add permissions • Remove permissions • Add delegation • Remove delegation • Disable user • Enable user • Create account • Remove account • Modify account • Change password • Add service • Remove service • Add resource • Remove resource • Add role to user • Remove role to user
Status	Event status can assume only three values: • Unprocessed • Success • Error
ERC Status	The status of the User_ERC table. It can be: • Unprocessed • Success • Error
Trace	Brief description of the error cause.
Marker	Marker of the event. It might coincide with the identifier of the target system.
Free Attribute 1	Sensitive data 1.
Free Attribute 2	Sensitive data 2.
...	...
Free Attribute N	Sensitive data N.
Application	The name of the application impacted by the operation/event.
Code Operation	A code optionally assigned to the operation.
Event Date	Indicates the event generation date.
Process Date	Indicates the date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	Indicates the user which caused the event on the external table.

The **Actions** menu includes the following buttons to manage OUT events:

Re-Execute
Reprocesses the operation associated with the selected event.

Remove
Deletes the selected event.

IN - User events

In this section you can monitor all events related to users in input from external target systems.

Input events can be filtered as described in the following table:

Table 108. Filters you can specify to list user events in input from external target systems.

Filter	Description
Status	Event status can assume one of the following three values: • Unprocessed • Success • Error
Operation	Indicates the type of operation associated with the event: • Create User • Modify User • Remove User • Move User • Create User (Deferred) • Modify User (Deferred) • Remove User (Deferred) • Move User (Deferred) • Custom
Operation Code	Not used.
Trace	Brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The events related to users in input from external target systems are listed with the following attributes:

Table 109. Details of User events in input from external target systems.

Field	Description
ID	The event identifier, a sequential number.
User ERC	The code of the User_ERC table with the attributes of the user processed in the operation/event. The USER_ERC table contains a copy of user data from the external system and matches the PERSON table in the AG Core database.

Table 109. Details of User events in input from external target systems. (continued)

Field	Description
Operation	The operation associated with the event. Can be one of the following: • Create User • Modify User • Remove User • Move User • Create User (Deferred) • Modify User (Deferred) • Remove User (Deferred) • Move User (Deferred) • Custom
Status	The event status can be one of these values: • Unprocessed • Success • Error
Trace	A short description of the error.
Detail	Further information on the error that is optionally provided by the external system.
Identification Number	The ID of the user processed in the event.
OU Code	The Organization Unit associated with the user processed in the event.
Action Type	Fields optionally used by the external system to add information about the operation.
Action Reason	Fields optionally used by the external system to add information about the operation.
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The process that owns the event. It is usually is the name of the connector used with the target system.

The following options become available when you click **Actions**:

Details
Displays the details of the selected event in the IN Events window.

User Data
Displays system and personal data of the user processed in the selected event in the Details window.

Re-Execute
Runs again the operation of the selected event.

Delete all filtered
Removes all the events resulting from a specific filtered search.

Remove
Removes the selected event.

IN - Org. Unit events

In this section you can monitor all events related to Organization Units in input from external target systems.

Input events can be filtered as described in the following table:

Table 110. Filters you can specify to list Organization Unit events in input from external systems.

Filter	Description
Status	Event status can assume one of the following three values: • Unprocessed • Success • Error
Operation	Indicates the type of operation associated with the event: • Create OU • Modify OU • Remove OU
Trace	Brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The events related to Organization Units in input from external systems are listed with the following attributes:

Table 111. Details of User events in input.

Field	Description
ID	The event identifier, a sequential number.
OU ERC	The code of the OU_ERC table with the attributes of the Organization Unit processed in the operation/event. The OU_ERC table contains a copy of Organization Unit data from the external system and matches the Organization Unit table in the AG Core database.
Operation	The operation associated with the event. Can be one of the following: • Create OU • Modify OU • Remove OU
Status	The event status can be one of these values: • Unprocessed • Success • Error
Trace	A short description of the error.
Identification Number	The ID of the Organization Unit processed in the event.
OU Code	The name of the Organization Unit processed in the event.
Action Type	Fields optionally used by the external system to add information about the operation.

Table 111. Details of User events in input. (continued)

Field	Description
Action Reason	Fields optionally used by the external system to add information about the operation.
Event Date	The event generation date.
Process Date	The date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).
Ownership	The process that is owner of the event. It is usually is the name of the connector used with the target system.

The following options become available when you click **Actions**:

Details
Displays the details of the selected event in the IN Events window.

Re-Execute
Runs again the operation of the selected event.

Delete all filtered
Removes all the events resulting from a specific filtered search.

Remove
Removes the selected event.

INTERNAL events

In this section you can monitor events triggered by operations run locally on the entities of your security model and impacting the AG Core database.

Internal events can be filtered as described in the following table:

Table 112. Filters you can specify to list internal events.

Filter	Description
Status	Event status can assume one of the following three values: • Unprocessed • Success • Error

Table 112. Filters you can specify to list internal events. (continued)

Filter	Description
Operation	Indicates the type of operation associated with the event. It can be one of the following: • Create Application • Remove Application • Modify Application • Create Entitlement • Remove Entitlement • Modify Entitlement • Create User • Remove User • Modify User • Create OU • Remove OU • Modify OU • Change SOD Status • Add User Entitlement • Remove User Entitlement
Entity Type	The type of entity impacted by the event. It can be one of the following: • Application • Entitlement • OU • User
Trace	A brief description of the error cause.
Event Start-End Date	Filters defining the time period for searching events.

The events related to operations run locally on the entities of your security model are listed with the following attributes:

Table 113. Details of internal events.

Field	Description
ID	The event identifier, a sequential number.

Table 113. Details of internal events. (continued)

Field	Description
Operation	The operation associated with the event. Can be one of the following: • Create Application • Remove Application • Modify Application • Create Entitlement • Remove Entitlement • Modify Entitlement • Create User • Remove User • Modify User • Create OU • Remove OU • Modify OU • Change SoD Status • Add User Entitlement • Remove User Entitlement
Status	The event status can be one of these values: • Unprocessed • Success • Error
Trace	A short description of the error.
Entity type	The type of entity impacted by the event. It can be one of the following: • Application • Entitlement • OU • User
Name	The name of the entity impacted by the event.
Description	A description of the entity impacted by the event.
Code	The identification of the entity impacted by the event.
Event Date	The event generation date.
Process Date	The processing date of the event (generally coincides with the event date but can be later if processing of the event was postponed).

The following options become available when you click **Actions**:

Re-Execute
Runs again the operation of the selected event.

Delete all filtered
Removes all the events resulting from a specific filtered search.

Remove
Removes the selected event.

Tools

Several functions speed up and facilitate the tasks of the following modules:

- Bulk Data Load

Bulk Data Load

You can load bulk data in the AG Core database.

You can run several types of bulk data-loading in the AG Core database.

The **Actions** tab (left) shows the supported operations.

After you select an operation in **File Batch**, select one of the following options:

- **Download** to get a template (XLS file), related to the currently selected operation.
- **Browse** to search in the file system for an XLS file for the selected loading operation.

When the operation is completed, an information record is appended in the lower-right pane to the list of the previously completed operations.

In the same pane, you can select:

- **Input File** to get the file used in the operation.
- **Log File** to get the operation report.

A generic record track distinguishes between **Mandatory** and **Optional** fields.

If a mandatory field is empty or populated with unexpected values, the row is skipped unless otherwise specified in the documentation.

According to the data load behavior, populating an **Optional** field with unexpected or incorrect values might cause a row to be skipped.

For information about the procedure, see “Creating a bulk load operation” on page 89.

The following procedures are available:

- Add Internal Resources to User-Entitlement
- Add Resources To User-Entitlement
- Add Resource To Org Unit
- Insert Account Attributes
- Insert Application Access
- Insert Applications
- Insert Attribute-to-Permission Mappings
- Insert Entitlements
- Insert Organization Units
- Insert Property
- Insert Resources
- Insert Rights Look-up
- Insert User Account Attributes

- Insert Users
- Remove Account Attributes
- Remove Application Access
- Remove Applications
- Remove Entitlements
- Remove Entitlements from OU
- Remove Internal Resources From User-Entitlement
- Remove Organization Units
- Remove Resources
- Remove Resources From Org Unit
- Remove Resources From User-Entitlement
- Remove User Account Attributes
- Remove User-OU-Entitlement Assignments
- Remove Users
- User-OU-Entitlement Assignments

Insert Account Attributes Record Track

Use this batch procedure to insert and update attributes of account configurations.

Table 114. Insert Account Attributes record track.

Information	Description	Validation
ACCOUNT_CONFIGURATION_NAME	The name of the account configuration. It cannot be `Ideas`.	Mandatory This name must already exist in Identity Governance and Intelligence.
ACCOUNT_ATTRIBUTE_NAME	The name of the account attribute.	Mandatory
VISIBLE	If the value is `True`, the attribute is displayed. If the value is `False`, the attribute is not displayed. The default is `False`.	Optional
UI_RENDERING	The type of UI element that renders the attribute. It can be one of the following: • Checkbox • Checkbox01 • Date • Datetime • Datetimeseconds • Passwordfield • Textarea • Textfield The default is `Textfield`.	Optional

Table 114. Insert Account Attributes record track. (continued)

Information	Description	Validation
ENGLISH	The translation of the attribute name in the respective languages.	Optional
ITALIAN		
GERMAN		
FRENCH		
SPANISH		
PORTUGUESE		
CHINESE		
JAPANESE		
CHINESE_TAIWAN		

The batch procedure verifies that the required fields are populated.

Insert Applications Record Track

This batch procedure can be used to insert Applications.

Table 115. Insert Applications Track

Information	Description	Validation
APPLICATION	Application identifier name.	Mandatory
DESCRIPTION	A free text field for describing the Application.	Optional
CONFIGURATION	Configuration identifier.	Optional
DISABLE_SYNC	Can assume the values `TRUE` or `FALSE`.	Optional
TARGET	Target identifier.	Optional

This batch procedure can be used to insert Applications. It verifies that the required fields are populated.

In the `APPLICATION` field, enter the Application name. If there is no existing Application with this name, the Application is added. If the Application already exists, the record is skipped.

If the `CONFIGURATION` field is empty, a default configuration is assigned to the Application. If the configuration does not exist, it is created.

If the value of `DISABLE_SINC` is `TRUE`, the synchronization is disabled. If the value is `FALSE`, empty, or if a wrong value is given, the synchronization is enabled.

The `TARGET` field must be populated with the name of the Target System.

If both the `TARGET` and `CONFIGURATION` fields are empty, a fictitious target named `IDEAS` is assigned.

If `TARGET` is empty and `CONFIGURATION` is populated, a target with the application name is created.

If TARGET is filled with a target identifier that does not exist, the target identifier is created.

Insert Attribute-to-Permission Mapping Track

Use this batch procedure to insert an attribute-to-permission mapping. It verifies that the required fields are populated.

Table 116. Insert Attribute-to-Permission Mapping Track

Information	**Description**	**If TYPE is boolean**	**If TYPE is string**	**Validation**
ATTRIBUTE_NAME	Attribute name.			Mandatory
TYPE	Possible values are string and boolean.			Mandatory
REQUIRED	Possible values are TRUE or FALSE.	REQUIRED is not applicable.	The default value is FALSE.	Optional
MULTI_VALUE	Possible values are TRUE or FALSE. By default, the value is FALSE. In other words, the default is a single value.	MULTI_VALUE is not applicable.	When MULTI_VALUE is either TRUE or FALSE, only one attribute value can be specified as the default value.	Optional
ATTRIBUTE_VALUE	Attribute value. If an attribute has multiple values, each value has one row.	ATTRIBUTE_VALUE has two rows for boolean type. Each row has two parts that are separated by a forward slash. The first row is TRUE/*<value>*, and the second row is FALSE/*<value>*, where *<value>* is the real attribute value at the target end point. For example, the first row is TRUE/Yes, and the second row is FALSE/No. TRUE indicates that the permission is assigned to the user. FALSE indicates that the permission is not assigned to the user.		Optional
INACTIVE	Possible values are TRUE or FALSE.	INACTIVE is not applicable.	The default value is FALSE.	Optional

Table 116. Insert Attribute-to-Permission Mapping Track (continued)

Information	Description	If TYPE is boolean	If TYPE is string	Validation
DEFAULT	Indicates whether this attribute value is a default value. Possible values are TRUE or FALSE.	DEFAULT is not applicable.	The default value is FALSE. Only one attribute value can have a DEFAULT value of TRUE. The **Default** option in the Add Attribute page uses a radio button. If INACTIVE is TRUE, this attribute value cannot be set as the default value.	Optional
TARGET	Target identifier.			Mandatory
APPLICATION_NAME	Application name. **Note:** If more than one application is available for an attribute, this value is mandatory.			Optional
PERMISSION_NAME	Permission name. If not specified, it defaults to the attribute name.			Optional
RIGHTS_VALUE	Permission rights that are mapped to the attribute values.	RIGHTS_VALUE is not applicable.	If RIGHTS_VALUE is empty, then ATTRIBUTE_VALUE is used as the default. **Note:** If ATTRIBUTE_VALUE is empty in the template, regardless of whether a RIGHTS_VALUE is present, then RIGHTS_VALUE is empty in the database.	Optional

Related concepts:

"Permissions based on user attributes" on page 16
An attribute permission is a specific type of permission that is used for mapping a user attribute that is imported from a target system. For harmonizing this feature with the role-based access control standard of the Identity Governance and Intelligence data model, you can use permissions and rights.

Related tasks:

"Importing an attribute-to-permission mapping with a bulk load operation" on page 70
Complete this task to import an attribute-to-permission mapping by using a bulk load operation.

Insert Entitlements Record Track

Use this batch procedure to import entitlements into your security model.

This batch procedure can be used to enter/update Entitlements and organize them into a hierarchy. It verifies that Mandatory fields are populated.

For ALL Optional fields, if the NULL string is specified, the related item will be:

- set to the default value;
- cleaned, if a default value is not expected.

Table 117. Insert Entitlements record track

Information	**Description**	**Validation**
NAME	The name of the entitlement	Mandatory
CODE	The univocal identifier of the entitlement	Optional
DESCRIPTION	A description of the entitlement	Optional
TYPE	The type of entitlement. It can be one of the following: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
PERMISSION_TYPE	Permission Type identifier.	Mandatory for entitlement type 1
APPLICATION	The name of the application to which the entitlement belongs. The application must be already defined.	Mandatory for all entitlement types but 3
ADMINISTRATIVE		Optional
LANGUAGE	The localization language	Mandatory if localized version
PARENT_NAME	The name of the parent entitlement. If defined, the parent entitlement must be listed before as a role without parent.	Optional
PARENT_CODE	The code of the parent entitlement. If it exists, the parent entitlement must be listed before as a role without parent.	Optional

Table 117. Insert Entitlements record track (continued)

Information	Description	Validation
PARENT_TYPE	Parent Entitlement Type identifier. Allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role An external role can be parent only to other external roles and permissions.	Mandatory if PARENT_NAME or PARENT_CODE were entered.
PARENT_APPLICATION	The name of the application to which the parent entitlement belongs. The application must be already defined.	Mandatory if PARENT_NAME or PARENT_CODE were entered.
OWNER_CODE	The identifier code of the person who owns the entitlement. The code must be already defined.	Optional
SCOPE_TYPE	The scope type that defines the operational limitations of the entitlement.	Optional
ENTITLEMENT_FAMILY	The name of the entitlement family where the entitlement is classified.	Optional
BUSINESS_NAME	The name of the business activity with which the entitlement is associated.	Optional
BUSINESS_POLICY	The name of the business policy with which the entitlement is associated.	Optional

Table 118. Note about entitlements

Information icon	Content of note about entitlements
ℹ	[1]**NOTE**: for Entitlements of TYPE=3, the APPLICATION field must be left blank. This field must be populated for the other types of entitlement. [2] **NOTE**: for Entitlements of TYPE=1, the PERMISSION_TYPE field must be populated. [3]**NOTE**: PARENT_TYPE is Mandatory ONLY if PARENT_NAME or PARENT_CODE has been specified. The same policy applies to PARENT_APPLICATION.

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

*Table 119. [4]**Entitlement Localization** options*

Concept	Description	
Localization Active	**YES**	**NO**
LANGUAGE	This field can be empty or host the language specification.	This field must be empty. If it is not empty, the entire row is skipped.
[4]**CODE**	This field is the unique identifier of the entitlement. If CODE is not specified, the system provides an automatically generated CODE. In this sense, it might be considered an optional item of the record track.	This field must be empty. If it is not empty, the entire row is skipped.
NAME	If **LANGUAGE** is empty or if the `IL` string is specified, the technical name of the entitlement is in **NAME**. If **NAME** is specified, the name of the entitlement, joined with the language that is specified in **LANGUAGE**, is in **NAME**.	
Entitlement specification	• `NAME/CODE` • `TYPE` • `APPLICATION` • `PERMISSION_TYPE`	• `NAME/CODE` • `TYPE` • `APPLICATION` • `PERMISSION_TYPE`

The **TYPE** field contains the Entitlement Type.

The **APPLICATION** field contains the Entitlement Application name and is mandatory for Permissions, IT roles, and External roles.

Entitlement existence is verified using the given NAME/CODE and TYPE (for TYPE = 1 and 2, APPLICATION is also verified; for TYPE = 1 only, PERMISSION_TYPE is also verified).

If there is already an Entitlement with the given NAME/CODE and TYPE-APPLICATION-PERMISSION_TYPE, it is updated with any information present in the optional **DESCRIPTION** field. Otherwise the Entitlement is entered.

The **PARENT_NAME**, **PARENT_TYPE**, and **PARENT_APPLICATION** fields are verified to ensure that the proposed hierarchy fulfills the Entitlement hierarchy definition. PARENT_TYPE must thus be different than Permission and there must be a parent Entitlement with the given PARENT_NAME/PARENT_CODE and PARENT_TYPE (TYPE = 2 also includes verification of PARENT_APPLICATION).

Parent Entitlement verification applies either to preexisting Entitlements or to the entire XLS file. Therefore, Entitlements need not be entered into the XLS file in any particular order.

Insert Organization Units Record Track

Table 120. Insert Organization Units Track

Information	Description	Validation
NAME	OU identifier name.	Mandatory
CODE	OU identifier code.	Mandatory
DESCRIPTION	A free text field for describing the OU.	Optional
PARENT_CODE	Parent OU identifier code.	Mandatory

This batch procedure can be used to insert/update Organization Units and organize them into a hierarchy. It verifies that Mandatory fields are populated.

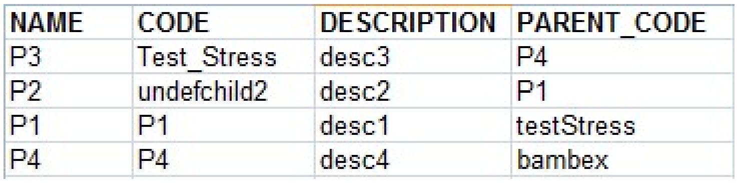
The **CODE** field contains the OU Code. If there is no existing OU with this name, the OU is inserted. If an OU with this Code already exists, the OU is updated with the given Name and Description. The **PARENT_CODE** field contains the code of the OU designated to be the Parent.

OUs are assigned to their respective Parent OUs. Presence of the Parent OU is verified with the given Parent Code.

PARENT_CODE verification applies either to a preexisting OU or to the entire XLS file. Therefore, OUs need not be inserted into the XLS file in any particular order. If the PARENT_CODE field is empty, the OU is assigned to the root OU.

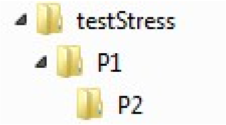
If a Parent OU with the given code does not exist, the OU is assigned to a technical OU (the code for a technical OU is "-undefined-"). The technical OU is created only at the first occurrence of this situation. The orphan OUs assigned to the technical OU will need to be properly repositioned within the OU hierarchy by the operator.

An example of the XLS file structure is shown below:

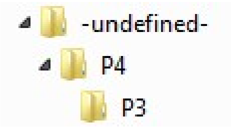


NAME	CODE	DESCRIPTION	PARENT_CODE
P3	Test_Stress	desc3	P4
P2	undefchild2	desc2	P1
P1	P1	desc1	testStress
P4	P4	desc4	bambex

Using the record track just shown, this first OU hierarchy will be built:



Another OU hierarchy will be built:



Since the bambex OU does not actually exist, this second one is required. P4 is thus assigned as a child of the “technical OU” named “-undefined-”.

Insert Resources Record Track

This batch procedure can be used to insert/update Resources.

Insert Resources Track		
Information	**Description**	**Validation**
RESOURCE_NAME	Resource name.	Mandatory
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory
ATTR1	Customizable field for client purposes.	Optional
ATTR2	Customizable field for client purposes.	Optional

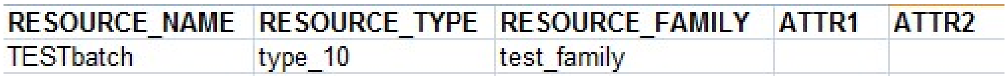
This batch procedure can be used to insert/update Resources.

It verifies that mandatory fields are populated as well as:

- The existence of the **RESOURCE_TYPE** and **RESOURCE_FAMILY** mandatory fields. If missing, they are inserted.
- The existence of a Resource with the given **RESOURCE_NAME**, **RESOURCE_TYPE**, and **RESOURCE_FAMILY**. If such resource does not exist, it is inserted. Otherwise, the information for the resource is updated.

ATTR1 and **ATTR2** are two customizable fields for client use and are useful for mapping resources to other optional fields (for example, **TEMPLATE** and **GENERIC_RES_REF** for the Access Provisioning (AP) Module).

An example of the XLS file structure is shown below:



RESOURCE_NAME	RESOURCE_TYPE	RESOURCE_FAMILY	ATTR1	ATTR2
TESTbatch	type_10	test_family		

Insert Users Record Track

Use this batch procedure to insert and update users.

Table 121. Insert Users record track.

Information	Description	Validation
CODE	The user's identifying code.	Mandatory
NAME	The user's first name.	Mandatory
SURNAME	The user's last name.	Mandatory
SEX	The user's gender: • 0: Male • 1: Female	Optional
OU	The code of the organization unit where the user is assigned.	Optional

Table 121. Insert Users record track. (continued)

Information	Description	Validation
USER_TYPE	Describes the position of the user in the organization. For example, it can indicate the title of the user (User Manager, Security Officer, or more), or, if the user is external, the type of relationship with the organization (Business Partner, Customer, Supplier).	Optional
EMAIL	The user's email address.	Optional
PHONE_NUMBER	The user's telephone number.	Optional
DN	The distinguished name of the user.	Optional
FISCAL_CODE	Any code or number issued by a national government (Fiscal code, SSN) that is used for the purpose of persona identification.	Optional
DATE_OF_BIRTH	Follows the format specified on the operating system.	Optional
PLACE_OF_BIRTH	User's place of birth and address information.	Optional
ADDRESS		Optional
CITY		Optional
STATE		Optional
COUNTRY		Optional
POSTAL_CODE		Optional
Additional columns may be added with user virtual attributes taken from external inventoried repositories.	Only User virtual attributes with names that do not start with an underscore (_) are allowed.	Optional

This batch procedure can be used to insert and update users. It verifies that the required fields are populated.

If the **OU** field contains a value, the procedure checks for the OU that matches the OU code entered. If the OU does not exist, the OU code value entered is ignored. A user with the matching **CODE** is then searched for.

If the user already exists, the user's information (**SURNAME**, **NAME**, **GENDER**) is updated. If no matching user is found, the user is created and added to the specified OU. If the OU does not exist, or if the OU field is empty, the user is not added to any OU.

If any of the loaded optional data is flawed, the user is still inserted and the error notified upon loading.

Insert User Account Attributes Record Track

Use this batch procedure to insert and update details and attributes of user accounts.

Table 122. Insert User Account Attributes record track.

Information	Description	Validation
ACCOUNT_CONFIGURATION_NAME	The name of the account configuration. It cannot be any of the following: • `Ideas` • The names of accounts that are accessed with Identity Brokerage Adapters .	Mandatory This name must already exist in Identity Governance and Intelligence.
USER_CODE	The user's Master UID.	Mandatory This name must already exist in Identity Governance and Intelligence.
IDENTITY_UID	The ID code of the account.	Mandatory
ACCOUNT_NAME	The given name with which the user registered to the account.	Optional
ACCOUNT_SURNAME	The surname with which the user registered to the account.	Optional

Table 122. Insert User Account Attributes record track. (continued)

Information	Description	Validation
ACCOUNT_PASSWORD	The password that the user provides to access the account.	Optional The field can be empty only if one of the following conditions is true: • **Allow empty password** is selected for the account configuration in **Access Governance Core** > **Manage** > **Accounts** > **Creation Policy**. • **Enable password check box for Administrator** is selected for the account configuration in **Access Governance Core** > **Manage** > **Accounts** > **Creation Policy**. Also, a password is present in **Default Password** in **Access Governance Core** > **Manage** > **Accounts** > **Password Creation** .
EMAIL	The user's email address.	Optional
ACCOUNT_EXPIRATION_DATE	The expiration date of the account for this user. The date is in the format that is specified on the operating system.	Optional
DISPLAY_NAME	The user's name as it is displayed on the target.	Optional
DN	The distinguished name of the user.	Optional
LAST_LOGIN	The date of the last login of this user on this account. The date is in the format that is specified on the operating system.	Optional

Table 122. Insert User Account Attributes record track. (continued)

Information	Description	Validation
LAST_WRONG_LOGIN	The date of the last failed login of this user on this account. The date is in the format that is specified on the operating system.	Optional
NUMBER_LOGIN_ERROR	The number of consecutive login errors. This value is reset to zero when the user logs in correctly.	Optional
LAST_CHANGE_PASSWORD	The date of the last password change for this user on this account. The date is in the format that is specified on the operating system.	Optional
Extra columns can be added for account attributes. Each must be titled with the ACCOUNT_ATTRIBUTE_NAME of the attribute.	The account attributes must be already present. Add them either manually in the user interface or with the Insert Account Attributes batch procedure.	Optional

The batch procedure verifies that the required fields are populated.

For accounts that do not have a matching user (USER_CODE), the procedure can only insert - not update - the ID code (IDENTITY_UID).

If any of the loaded optional data is flawed, the user account data and attributes are still inserted. The error is notified upon loading.

Remove Account Attributes Record Track

Use this batch procedure to remove account attributes from account configurations.

Table 123. Remove Account Attributes record track.

Information	Description	Validation
ACCOUNT_CONFIGURATION_NAME	The name of the account configuration. It cannot be `Ideas`.	Mandatory
ACCOUNT_ATTRIBUTE_NAME	The name of the account attribute.	Mandatory

The batch procedure verifies that the required fields are populated.

Remove Applications Record Track

This batch procedure can be used to remove Applications.

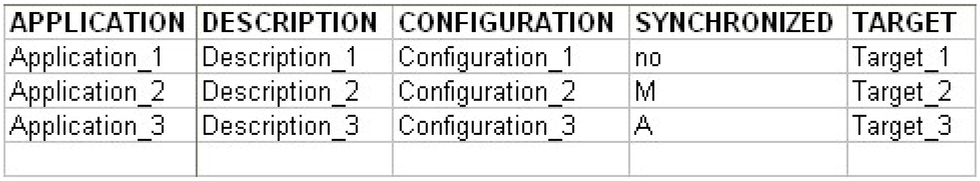
Remove Applications Track		
Information	**Description**	**Validation**
APPLICATION	Application identifier name.	Mandatory
DESCRIPTION	A free text field used to describe the Application.	Unused

Remove Applications Track		
Information	**Description**	**Validation**
CONFIGURATION	Configuration identifier.	Unused
SYNCHRONIZED	Can be one of these values: • **NO**: not synchronized • **M**: manually • **A**: automatically	Unused
TARGET	Target identifier.	Unused

This batch procedure can be used to remove Applications. It verifies that the required fields are populated.

Enter the Application name in the **APPLICATION** field. If no Application is found with this name, the record is skipped. If the Application exists, the Application is removed.

An example of the XLS file structure is shown below:



APPLICATION	DESCRIPTION	CONFIGURATION	SYNCHRONIZED	TARGET
Application_1	Description_1	Configuration_1	no	Target_1
Application_2	Description_2	Configuration_2	M	Target_2
Application_3	Description_3	Configuration_3	A	Target_3

Remove Entitlement from OU Record Track

This batch procedure can be used to remove an Entitlement from an Organization Unit.

Table 124. Remove Entitlements from OU Track

Information	Description	Validation
OU_CODE	OU identifier code.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name.	Mandatory
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
ENTITLEMENT_TYPE	Entitlement Type identifier. Allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
ENTITLEMENT_APPLICATION	Entitlement Application identifier name.	Mandatory[1]
PERMISSION_TYPE	Permission Type identifier name.	Mandatory[2]

This batch procedure can be used to remove an Entitlement from an Organization Unit.

It verifies that the required fields are populated.

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	**Description**	
Localization Active	**YES**	**NO**
Entitlement specification	**ENTITLEMENT_CODE** Or • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2]. If **ENTITLEMENT_CODE** is specified, it is the univocal identifier of the entitlement. The **ENTITLEMENT_NAME** is the technical name of the entitlement.	An entitlement must be specified by: • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2].

[1] **NOTE:** If **ENTITLEMENT_TYPE** = 3, the **ENTITLEMENT_APPLICATION** field must be blank. Otherwise, it must be populated.

[2] **NOTE:** If **ENTITLEMENT_TYPE** = 1, the **PERMISSION_TYPE** field must be populated.

The **OU_CODE** field must contain an existing OU code. If not, the row is skipped.

Entitlement existence is verified using the values of **ENTITLEMENT_NAME**, **ENTITLEMENT_TYPE**, **ENTITLEMENT_APPLICATION** (**ENTITLEMENT_APPLICATION** is mandatory when **ENTITLEMENT_TYPE**= 1, 2, or External_Role) and **PERMISSION_TYPE** (only when **ENTITLEMENT_TYPE**= 1).

If there is no such Entitlement, the record is skipped. If the Entitlement exists and is assigned to the specified OU, the assignment is removed.

Remove Entitlements Record Track

This batch procedure is used to remove Entitlements.

Table 125. Remove Entitlements Track

Information	Description	Validation
NAME	Entitlement identifier name.	Mandatory
ENTITLEMENT_CODE	This field hold the univocal identifier of the Entitlement.	Optional
DESCRIPTION	A free text field for describing the Entitlement.	Unused
TYPE	Entitlement Type Identifier. Allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
PERMISSION_TYPE	Permission Type identifier.	Mandatory[2]
APPLICATION	Application identifier name.	Mandatory[1]
PARENT_NAME	Parent Entitlement identifier name.	Unused
PARENT_TYPE	Parent Entitlement Type identifier. Allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Unused
PARENT_APPLICATION	Parent Application identifier name.	Unused

This batch procedure is used to remove Entitlements. It verifies that the required fields are populated.

Table 126. Note about terms

ℹ	For legacy reasons, the following terms can be assumed as equivalent: **NAME** is equivalent to **ENTITLEMENT_NAME** **TYPE** is equivalent to **ENTITLEMENT_TYPE** **APPLICATION** is equivalent to **ENTITLEMENT_APPLICATION** Note however that the Record Track **MUST BE** specified only by the keywords indicated in the Information column of the preceding table.

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	**Description**	
Localization Active	**YES**	**NO**
Entitlement specification	**ENTITLEMENT_CODE** Or • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2]. If **ENTITLEMENT_CODE** is specified, it is the univocal identifier of the entitlement. The **ENTITLEMENT_NAME** is the technical name of the entitlement.	An entitlement must be specified by: • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2].

[1] **NOTE:** If **ENTITLEMENT_TYPE** = 3, the **ENTITLEMENT_APPLICATION** field must be blank. Otherwise, it must be populated.

[2] **NOTE:** If **ENTITLEMENT_TYPE** = 1, the **PERMISSION_TYPE** field must be populated.

The **APPLICATION** field contains the Entitlement Application name and is mandatory only for Permissions, IT roles, and External roles.

The **PERMISSION_TYPE** field contains the Entitlement Permission Type name and is mandatory only for Permissions.

The existence of an Entitlement is verified using the given **NAME** and **TYPE** (for **TYPE**= 1, 2, or External_Role,**APPLICATION** is also verified; for **TYPE**= 1 only, **PERMISSION_TYPE** is also verified). If there is already an Entitlement with the given **NAME** and **TYPE**, the Entitlement is removed. Otherwise the record is skipped.

The removal of an Entitlement implies a change in the hierarchy of Entitlements that is not managed by this batch procedure.

Remove Organization Units Record Track

This batch procedure can be used to remove a set of Organization Units.

Remove Organization Units Track		
Information	**Description**	**Validation**
NAME	OU identifier name.	Unused

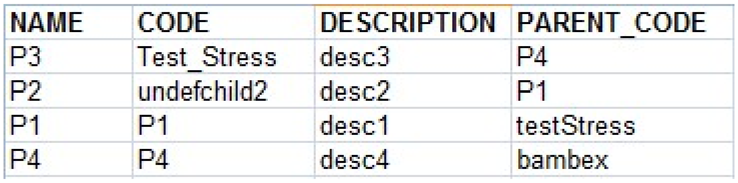
Remove Organization Units Track		
Information	**Description**	**Validation**
CODE	OU identifier code.	Mandatory
DESCRIPTION	A free text field for describing the OU.	Unused
PARENT_CODE	Parent OU identifier code.	Unused

This batch procedure can be used to remove a set of Organization Units. It verifies that the required fields are populated.

The **CODE** field contains the OU identifier code. If no OU exists with this **CODE**, the record is skipped. If an OU with this **CODE** does exist, its children are assigned to its parent OU and the OU is then removed.

The root OU cannot be removed.

An example of the XLS file structure is shown below:



NAME	CODE	DESCRIPTION	PARENT_CODE
P3	Test_Stress	desc3	P4
P2	undefchild2	desc2	P1
P1	P1	desc1	testStress
P4	P4	desc4	bambex

Remove Resources Record Track

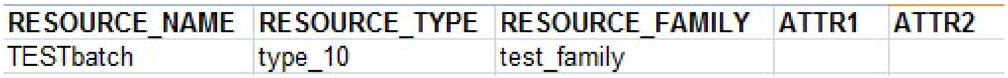
This batch procedure can be used to remove Resources.

Remove Resources Track		
Information	**Description**	**Validation**
RESOURCE_NAME	Resource name.	Mandatory
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory
ATTR1	Customizable field for client purposes.	Unused
ATTR2	Customizable field for client purposes.	Unused

This batch procedure can be used to remove Resources. It verifies that the required fields are populated.

It checks for a Resource with the given **RESOURCE_NAME**, **RESOURCE_TYPE**, and **RESOURCE_FAMILY**. If there is no such Resource, the record is skipped. If the Resource exists, it is removed.

An example of the XLS file structure is shown below:



RESOURCE_NAME	RESOURCE_TYPE	RESOURCE_FAMILY	ATTR1	ATTR2
TESTbatch	type_10	test_family		

Remove User-OU-Entitlement Assignments Record Track

This batch procedure can be used to manage Entitlement Assignment.

Table 127. Remove User-OU-Entitlement Assignments Track

Information	Description	Validation
USER_CODE	User identifier code.	Mandatory
USER_OU	User OU identifier code.	Optional
ENTITLEMENT_NAME	Entitlement identifier name.	Mandatory
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
ENTITLEMENT_TYPE	Entitlement Type identifier. The allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
ENTITLEMENT_APPLICATION	Entitlement Application identifier name.	Mandatory[1]
PERMISSION_TYPE	Permission Type identifier name.	Mandatory[2]

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	**Description**	
Localization Active	**YES**	**NO**
Entitlement specification	**ENTITLEMENT_CODE** Or • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2]. If **ENTITLEMENT_CODE** is specified, it is the univocal identifier of the entitlement. The **ENTITLEMENT_NAME** is the technical name of the entitlement.	An entitlement must be specified by: • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2].

	[1] **NOTE:** If **ENTITLEMENT_TYPE** = 3, the **ENTITLEMENT_APPLICATION** field must be blank. Otherwise, it must be populated. [2] **NOTE:** If **ENTITLEMENT_TYPE** = 1, the **PERMISSION_TYPE** field must be populated.

This batch procedure can be used to manage Entitlement Assignment. It verifies that the required fields are populated.

The procedure checks for a User with the given **USER_CODE**. If the User is already assigned to an OU, the User's OU must match the value entered in the **USER_OU** field. Otherwise, the row is skipped.

The **USER_OU** field must contain an existing OU code. If it does not, the row is skipped.

The existence of the entitlement is verified using the values of **ENTITLEMENT_NAME**, **ENTITLEMENT_TYPE**, **ENTITLEMENT_APPLICATION** (**ENTITLEMENT_APPLICATION** is mandatory when **ENTITLEMENT_TYPE**= 1, 2, or External_Role) and **PERMISSION_TYPE** (only when **ENTITLEMENT_TYPE**= 1).

If there is no such Entitlement, the record is skipped.

If the Entitlement exists and is assigned to the specified User, the assignment is removed.

Remove Users Record Track

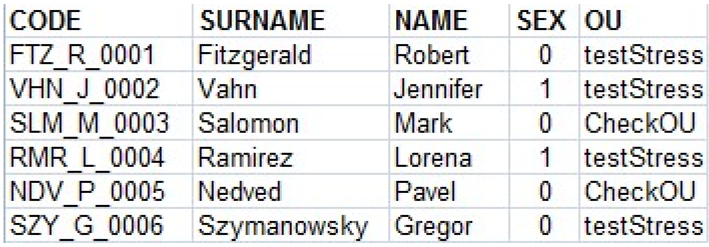
This batch procedure can be used to remove Users.

Remove Users Track		
Information	**Description**	**Validation**
CODE	User identifier code.	Mandatory
SURNAME	User Surname.	Mandatory
NAME	User Name.	Mandatory
SEX	User's gender. Allowed values are: • 0: Male • 1: Female	Unused
OU	OU code.	Unused

This batch procedure can be used to remove Users. It verifies that the required fields are populated.

It searches for a User with the given **CODE**, **NAME**, and **SURNAME**. If found, the User is removed. Otherwise, the record is skipped.

An example of the XLS file structure is shown below:



CODE	SURNAME	NAME	SEX	OU
FTZ_R_0001	Fitzgerald	Robert	0	testStress
VHN_J_0002	Vahn	Jennifer	1	testStress
SLM_M_0003	Salomon	Mark	0	CheckOU
RMR_L_0004	Ramirez	Lorena	1	testStress
NDV_P_0005	Nedved	Pavel	0	CheckOU
SZY_G_0006	Szymanowsky	Gregor	0	testStress

Remove User Account Attributes Record Track

Use this batch procedure to remove user accounts.

Table 128. Remove User Account Attributes record track.

Information	Description	Validation
ACCOUNT_CONFIGURATION_NAME	The name of the account configuration. It cannot be any of the following: • `Ideas` • The names of accounts that are accessed with Identity Brokerage Adapters .	Mandatory
IDENTITY_UID	The ID code of the account.	Mandatory

The batch procedure verifies that the required fields are populated.

User-OU-Entitlement Assignments Record Track

This batch procedure can be used to manage Entitlement Assignments.

Table 129. User-OU-Entitlement Assignments Track

Information	Description	Validation
USER_CODE	User identifier code.	Optional
OU_CODE	OU identifier code.	Mandatory[3]
IN_HIER	Values can be **TRUE** or **FALSE**.	Optional
ENTITLEMENT_NAME	Entitlement identifier name.	Mandatory
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
ENTITLEMENT_TYPE	Can be one of the following: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
ENTITLEMENT_APPLICATION	Entitlement Application Identifier Name	Mandatory[1]
PERMISSION_TYPE	Permission Type identifier name	Mandatory[2]

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	**Description**	
Localization Active	**YES**	**NO**
Entitlement specification	**ENTITLEMENT_CODE** Or • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2]. If **ENTITLEMENT_CODE** is specified, it is the univocal identifier of the entitlement. The **ENTITLEMENT_NAME** is the technical name of the entitlement.	An entitlement must be specified by: • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2].

ℹ	[1] **NOTE:** If **ENTITLEMENT_TYPE** = 3, the **ENTITLEMENT_APPLICATION** field must be blank. Otherwise, it must be populated. [2] **NOTE:** If **ENTITLEMENT_TYPE** = 1, the **PERMISSION_TYPE** field must be populated.

ℹ	[3]**NOTE**: If **USER_CODE** is not present, **OU_CODE** MUST BE specified.

This batch procedure can be used to manage Entitlement Assignments. It verifies that the required fields are populated.

The procedure checks for a User with the given **USER_CODE**. If the User is already assigned to an Organization Unit, the User's OU must match the given **OU_CODE** field value. Otherwise, the row is skipped. If **USER_CODE** is not populated, Entitlement is assigned only to **OU_CODE**.

If the **IN_HIER** field is TRUE, Entitlement is assigned in hierarchy.

If not already aggregated to an OU, the User is aggregated to the given User OU.

The **OU_CODE** field must contain an existing OU code. If it does not, the row is skipped.

The existence of the Entitlement is verified using the values of **ENTITLEMENT_NAME, ENTITLEMENT_TYPE, ENTITLEMENT_APPLICATION** (**ENTITLEMENT_APPLICATION** is mandatory when **ENTITLEMENT_TYPE**= 1, 2, or External_Role) and **PERMISSION_TYPE** (only when **ENTITLEMENT_TYPE**= 1).

If there is no such Entitlement, the record is skipped. The following three aggregations are created:

- **Entitlement - Entitlement**: Entitlement is published and assignable to Users
- **Entitlement - OU**: Entitlement is available in an Organization Unit
- **Entitlement - User**: Entitlement is assigned to the User

Add Resources to User/Entitlement Record Track

This batch procedure can be used to add Resources to an Entitlement already assigned to a User.

Add Resources to User/Entitlement Track		
Information	**Description**	**Validation**
USER_CODE	Code of the User.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name. If the **Entitlement Localization** option is active, this is the "technical name" of the Entitlement.	Mandatory
ENTITLEMENT_CODE	Univocal identifier of an Entitlement.	Mandatory
ENTITLEMENT_TYPE	Entitlement Type identifier. The allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
ENTITLEMENT_APPLICATION	Application identifier name.	Mandatory[1]
PERMISSION_TYPE	Permission Type identifier.	Mandatory[2]
RESOURCE_NAME	Resource name.	Mandatory
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory

This batch procedure can be used to add Resources to an Entitlement already assigned to a User.

It verifies that the required fields are populated; when a Mandatory field is missing, the row is skipped.

Note: The Resource to be assigned to the Entitlement/User, MUST BE a Resource already assigned to the OU to which the User (**USER_CODE**) belongs.

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	**Description**	
Localization Active	**YES**	**NO**
Entitlement specification	**ENTITLEMENT_CODE** Or • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2]. If **ENTITLEMENT_CODE** is specified, it is the univocal identifier of the entitlement. The **ENTITLEMENT_NAME** is the technical name of the entitlement.	An entitlement must be specified by: • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2].

[1]

NOTE: If **ENTITLEMENT_TYPE** = 3, the **ENTITLEMENT_APPLICATION** field must be blank. Otherwise, it must be populated.

[2]

NOTE: If **ENTITLEMENT_TYPE** = 1, the **PERMISSION_TYPE** field must be populated.

Add Internal Resources to User/Entitlement Record Track

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

Table 130. Add Internal Resources to User/Entitlement Track

Information	**Description**	**Validation**
USER_CODE	Code of the User.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name. If the **Entitlement Localization** option is active, this is the "technical name" of the Entitlement.	Mandatory
ENTITLEMENT_CODE	Univocal identifier of an Entitlement.	Mandatory

Table 130. Add Internal Resources to User/Entitlement Track (continued)

Information	Description	Validation
ENTITLEMENT_TYPE	Entitlement Type identifier. Allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
ENTITLEMENT_APPLICATION	Application identifier name.	Mandatory[1]
PERMISSION_TYPE	Permission Type identifier.	Mandatory[2]
INT_RESOURCE_NAME	Internal Resource name.	Optional.
INT_RESOURCE_TYPE	Internal Resource Type name. Allowed values are: • **OU**: the Resource is an Organization Unit • **E**: the Resource is an Entitlement • **A**: the Resource is an Application • **R**: the Resource is a Risk	Mandatory
INT_RESOURCE_CODE	Univocal identifier of the Resource type specified in the row above.	Mandatory
RESOURCE_SPEC_1	Used if **INT_RESOURCE_TYPE** = **E**	Optional
RESOURCE_SPEC_2	Used if **INT_RESOURCE_TYPE** = **R** or **E**	Optional
RESOURCE_SPEC_3	Used if **INT_RESOURCE_TYPE** = **E**	Optional

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

It verifies that the required fields are populated; if a Mandatory field is missing, the row is skipped.

Table 131. Note about resources

ℹ	**Note:** The Resource to be assigned to the Entitlement/User must be a Resource already assigned to the OU to which the User (**USER_CODE**) belongs.

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	**Description**	
Localization Active	**YES**	**NO**
Entitlement specification	**ENTITLEMENT_CODE** Or • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2]. If **ENTITLEMENT_CODE** is specified, it is the univocal identifier of the entitlement. The **ENTITLEMENT_NAME** is the technical name of the entitlement.	An entitlement must be specified by: • **ENTITLEMENT_NAME** • **ENTITLEMENT_TYPE** • **ENTITLEMENT_APPLICATION** • **PERMISSION_TYPE** See Note[1] and Note[2].

[1]

NOTE: If **ENTITLEMENT_TYPE** = 3, the **ENTITLEMENT_APPLICATION** field must be blank. Otherwise, it must be populated.

[2]

NOTE: If **ENTITLEMENT_TYPE** = 1, the **PERMISSION_TYPE** field must be populated.

Depending on the specified **INT_RESOURCE_TYPE**, different combinations of parameters are allowed as shown in the table below:

Table 132. Combinations of parameters available for adding Internal Resources

	INT_RESORCE_TYPE			
Field	**OU**	**E**	**A**	**R**
INT_RESOURCE_CODE	OU_CODE	ENTITLEMENT_CODE	N.A.	N.A.
INT_RESOURCE_NAME	N.A.	Entitlement name.	Application name.	Risk name.
RESOURCE_SPEC_1	N.A.	ENTITLEMENT_ TYPE	N.A.	N.A.
RESOURCE_SPEC_2	N.A.	If **RESOURCE_SPEC_1**=1 (Permission) or**RESOURCE_SPEC_1**=2 (IT Role) the Application name joined with the IT Role or Permission must be specified.	N.A.	Environment name.
RESOURCE_SPEC_3	N.A.	If **RESOURCE_SPEC_1** = 1 (Permission), the related Permission Type must be specified.	N.A.	N.A.

Add Resources to OU Record Track

This batch procedure can be used to add Resources to an OU.

Add Resources to OU Track		
Information	**Description**	**Validation**
OU_CODE	Code of the OU target.	Mandatory
RESOURCE_NAME	Resource name.	Mandatory
RESOURCE_TYPE	Resource Type name.	Mandatory
RESOURCE_FAMILY	Resource Family name.	Mandatory
HIERARCHY	The allowed values are: • **TRUE**: Resource is added in hierarchy • **FALSE**: Resource is added only to the OU indicated by **OU_CODE** (default value)	Optional
INHERITANCE	The allowed values are: • **TRUE**: The Resource is automatically available to any User assigned to the OU (**OU_CODE**) • **FALSE**: The Resource is not automatically available to Users of the OU (default value).	Optional

This batch procedure can be used to add Resources to an OU.

It verifies that the required fields are populated; if a Mandatory field is missing, the row is skipped.

For **HIERARCHY** and **INHERITANCE** fields, an empty field is equivalent to **FALSE** value (default value).

Remove Int Resources from User/Entitlement Record Track

Remove Profile from Activity Record Track ARC

This batch procedure can be used to remove Internal Resources from an entitlement already assigned to a user. The structure of the record track is the same as the one described in Add Internal Resources to User_ Entitlement Record Track or in “Add Resources to OU Record Track.”

Remove Resources from User/Entitlement Record Track

Remove Profile from Activity Record Track ARC

This batch procedure can be used to remove resources from an entitlement already assigned to a user. The structure of the record track is the same as the one described in “Add Resources to User/Entitlement Record Track” on page 308 and “Add Resources to OU Record Track.”

Remove Resource from OU Record Track

Remove Profile from Activity Record Track ARC

This batch procedure can be used to remove Resource from an OU.

The structure of the record track is the same as the one described in “Add Resources to OU Record Track” on page 312 or in Add Permission to Activity Record Track.

Insert Organization Units Record Track

Table 133. Insert Organization Units Track

Information	Description	Validation
NAME	OU identifier name.	Mandatory
CODE	OU identifier code.	Mandatory
DESCRIPTION	A free text field for describing the OU.	Optional
PARENT_CODE	Parent OU identifier code.	Mandatory

This batch procedure can be used to insert/update Organization Units and organize them into a hierarchy. It verifies that Mandatory fields are populated.

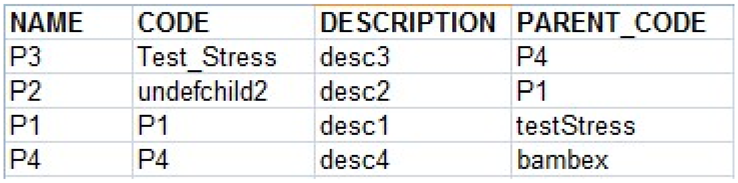
The **CODE** field contains the OU Code. If there is no existing OU with this name, the OU is inserted. If an OU with this Code already exists, the OU is updated with the given Name and Description. The **PARENT_CODE** field contains the code of the OU designated to be the Parent.

OUs are assigned to their respective Parent OUs. Presence of the Parent OU is verified with the given Parent Code.

PARENT_CODE verification applies either to a preexisting OU or to the entire XLS file. Therefore, OUs need not be inserted into the XLS file in any particular order. If the PARENT_CODE field is empty, the OU is assigned to the root OU.

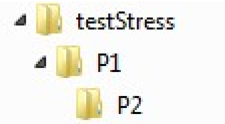
If a Parent OU with the given code does not exist, the OU is assigned to a technical OU (the code for a technical OU is "-undefined-"). The technical OU is created only at the first occurrence of this situation. The orphan OUs assigned to the technical OU will need to be properly repositioned within the OU hierarchy by the operator.

An example of the XLS file structure is shown below:

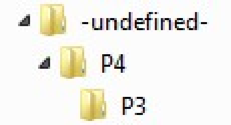


NAME	CODE	DESCRIPTION	PARENT_CODE
P3	Test_Stress	desc3	P4
P2	undefchild2	desc2	P1
P1	P1	desc1	testStress
P4	P4	desc4	bambex

Using the record track just shown, this first OU hierarchy will be built:



Another OU hierarchy will be built:



Since the bambex OU does not actually exist, this second one is required. P4 is thus assigned as a child of the “technical OU” named “-undefined-”.

Insert Property Record Track

Table 134. Insert Property Record Track.

Information	Description	Validation
ENTITY_TYPE	Indicates the type of Entity to be associated with a set of properties. The possible values are: • **E**: Entitlement • **A**: Application	Mandatory
K1	Entity logic key.	Mandatory
K2	Entity logic key.	Mandatory
K3	Entity logic key.	Mandatory
NAME	Indicates the name of the property.	Mandatory
VALUE	Indicates the value of the NAME property .	Mandatory
MULTIVALUE	The possible values are: • **TRUE**: Property is multi-value • **FALSE**: Property is single-value (default value)	Optional
INHERITABLE	The possible values are: • **TRUE**: Property is inheritable. • **FALSE**: Property is not inheritable (default value)	Optional
ACTION	The DELETE tag indicates a property that is to be deleted.	Mandatory
ENTITLEMENT_CODE	This field holds the univocal identifier of the Entitlement.	Optional
EXTERNAL_ROLE	Specifies if the entitlement is an external role. Can be TRUE or FALSE (default).	Optional

This batch procedure can be used to insert/update Properties.

It verifies that mandatory fields are populated; if a mandatory field is missing, the row is skipped.

Properties support multivalue, so the same NAME can be repeated multiple times with different values.

The combinations of Logic Keys K1, K2 and K3 are shown in the table below:

Table 135. Entity Logic Keys combinations.

Entities\Keys	K1	K2	K3
Business Role	Name of the BRole	*empty*	*empty*
IT Role	Name of IT Role	Name of the Application	*empty*
Permission	Name of Permission	Name of the Application	Permission Type
Application	Name of the Application	*empty*	*empty*

The Entitlement associated with the Property can be specified by the (K1,K2,K3) combination or by the ENTITLEMENT_CODE.

Add Internal Resources to User/Entitlement Record Track

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

Table 136. Add Internal Resources to User/Entitlement Track

Information	Description	Validation
USER_CODE	Code of the User.	Mandatory
ENTITLEMENT_NAME	Entitlement identifier name. If the **Entitlement Localization** option is active, this is the "technical name" of the Entitlement.	Mandatory
ENTITLEMENT_CODE	Univocal identifier of an Entitlement.	Mandatory
ENTITLEMENT_TYPE	Entitlement Type identifier. Allowed values are: • 1 (for Permission) • 2 (for IT role) • 3 (for Business role) • External_Role	Mandatory
ENTITLEMENT_APPLICATION	Application identifier name.	Mandatory[1]
PERMISSION_TYPE	Permission Type identifier.	Mandatory[2]
INT_RESOURCE_NAME	Internal Resource name.	Optional.

Table 136. Add Internal Resources to User/Entitlement Track (continued)

Information	Description	Validation
INT_RESOURCE_TYPE	Internal Resource Type name. Allowed values are: • **OU**: the Resource is an Organization Unit • **E**: the Resource is an Entitlement • **A**: the Resource is an Application • **R**: the Resource is a Risk	Mandatory
INT_RESOURCE_CODE	Univocal identifier of the Resource type specified in the row above.	Mandatory
RESOURCE_SPEC_1	Used if **INT_RESOURCE_TYPE** = **E**	Optional
RESOURCE_SPEC_2	Used if **INT_RESOURCE_TYPE** = **R** or **E**	Optional
RESOURCE_SPEC_3	Used if **INT_RESOURCE_TYPE** = **E**	Optional

This batch procedure can be used to add Internal Resources to an Entitlement already assigned to a User.

It verifies that the required fields are populated; if a Mandatory field is missing, the row is skipped.

Table 137. Note about resources

ℹ	**Note:** The Resource to be assigned to the Entitlement/User must be a Resource already assigned to the OU to which the User (**USER_CODE**) belongs.

Depending on whether the **Entitlement Localization** is active or not active, you can specify the entitlements in different ways. See the IBM Security Governance installation procedure for details. The following table describes the options.

Entitlement Localization options		
Concept	**Description**	
Localization Active	**YES**	**NO**

Entitlement Localization options		
Concept	**Description**	
Entitlement specification	**`ENTITLEMENT_CODE`** Or • **`ENTITLEMENT_NAME`** • **`ENTITLEMENT_TYPE`** • **`ENTITLEMENT_APPLICATION`** • **`PERMISSION_TYPE`** See Note[1] and Note[2]. If **`ENTITLEMENT_CODE`** is specified, it is the univocal identifier of the entitlement. The **`ENTITLEMENT_NAME`** is the technical name of the entitlement.	An entitlement must be specified by: • **`ENTITLEMENT_NAME`** • **`ENTITLEMENT_TYPE`** • **`ENTITLEMENT_APPLICATION`** • **`PERMISSION_TYPE`** See Note[1] and Note[2].

[1]

NOTE: If **`ENTITLEMENT_TYPE`** = 3, the **`ENTITLEMENT_APPLICATION`** field must be blank. Otherwise, it must be populated.

[2]

NOTE: If **`ENTITLEMENT_TYPE`** = 1, the **`PERMISSION_TYPE`** field must be populated.

Depending on the specified **INT_RESOURCE_TYPE**, different combinations of parameters are allowed as shown in the table below:

Table 138. Combinations of parameters available for adding Internal Resources

	INT_RESORCE_TYPE			
Field	**OU**	**E**	**A**	**R**
INT_RESOURCE_CODE	OU_CODE	ENTITLEMENT_CODE	N.A.	N.A.
INT_RESOURCE_NAME	N.A.	Entitlement name.	Application name.	Risk name.
RESOURCE_SPEC_1	N.A.	ENTITLEMENT_ TYPE	N.A.	N.A.
RESOURCE_SPEC_2	N.A.	If **RESOURCE_SPEC_1**=1 (Permission) or**RESOURCE_SPEC_1**=2 (IT Role) the Application name joined with the IT Role or Permission must be specified.	N.A.	Environment name.
RESOURCE_SPEC_3	N.A.	If **RESOURCE_SPEC_1** = 1 (Permission), the related Permission Type must be specified.	N.A.	N.A.

Insert Rights Lookup Record Track

Insert Rights Lookup Track		
Information	**Description**	**Validation**
NAME	Indicates the name of the Right.	Mandatory
VALUE	Indicates the value of the Right NAME.	Mandatory

This batch procedure can be used to insert/update a set of values for every Right.

It verifies that Mandatory fields are populated; if some Mandatory field is missing, the row is skipped.

Tipically, we have a set of rows (or more than one set) with:

- the same Name for every row of the set
- a distinct Value for every row of the set

Insert Application Access record track

Use this batch procedure to import application accesses from an external target. An application access might be an external role or a permission.

Table 139. Insert Application Access record track

Information	Description	Validation
NAME	The name of the application access.	Mandatory
CODE	The unique identifier of the application access.	Optional
DESCRIPTION	A description of the application access.	Optional
TYPE	The type of application access. It can be: • Permission • External_Role	Mandatory
PERMISSION_TYPE	Permission Type identifier for both external roles and permissions.	Mandatory
APPLICATION	The name of the application to which the application access belongs. The application must be already defined.	Mandatory
EXTERNAL_REF	An external reference (external key) for the application access on the target system.	Optional
FULFILLMENT	TRUE (the application access is fulfilled) or FALSE (the application access is not fulfilled).	Optional. Empty field is acknowledged as FALSE.
PUBLISH	TRUE (the application access is published) or FALSE (the application access is not published). Also, FULFILLMENT must be TRUE for the application access to be published.	Optional. Empty field is acknowledged as FALSE.
PARENT_NAME	The name of the parent external role.	Optional
PARENT_CODE	The code of the parent external role.	Optional

Table 139. Insert Application Access record track (continued)

Information	Description	Validation
PARENT_TYPE	Parent Entitlement Type identifier: `External_Role`	Mandatory if PARENT_NAME or PARENT_CODE entered.
PARENT_PERMISSION_TYPE	The Permission Type identifier of the parent external role, if one was entered.	Mandatory if PARENT_NAME or PARENT_CODE entered.
PARENT_APPLICATION	The name of the application to which the parent external role belongs. The application must be already defined.	Mandatory if PARENT_NAME or PARENT_CODE entered.
OWNER_CODE	The identifier code of the person who owns the application access. The code must be already defined.	Optional
RIGHT_NAME	The identifier of the right.	Mandatory, when a right is associated to a permission
RIGHT_CONTENT	The key of the lookup table.	Optional. If empty, means that the right that is indicated in RIGHT_NAME is without lookup.
RIGHT_MV	TRUE (the right is multi-value) or FALSE (the right is single value).	If any valid value is specified, the value set is FALSE
RIGHT_REQUIRED	TRUE (the right is required) or FALSE (the right is not required).	If any valid value is specified, the value set is FALSE.
RIGHT_DEFAULT_VALUE	The default value that can be assigned to a right.	Mandatory only if RIGHT_REQUIRED is TRUE.

The bulk load can be used for loading application accesses of different applications, but the common policy is to use a single bulk load that is related to a single application.

The data in the bulk load replaces completely the data previously present into the Access Governance Core central repository, for the application set.

A common case is if you to have N application accesses of APP1 and you need to add another *App_Acc*.

For addressing this case, you must prepare a bulk load with all the previous N application accesses, with the extra data that is related to *App_Acc*.

For a specific application, the final content of the central repository is perfectly described by the content of the last .XLS file loaded.

Conversely, if you have into the central repository of Access Governance Core an application access that is not present into the bulk load file, the application access is deleted by the repository.

It is not allowed the update of an application access previously present into to the central repository of Access Governance Core: you must load the new version.

The primary key is made up by the set of four mandatory fields: APPLICATION, NAME, TYPE, PERMISSION_TYPE.

If you want to define an EXTERNAL_REF, also the set of attributes APPLICATION, TYPE, PERMISSION_TYPE, EXTERNAL_REF is a primary key.

External roles and permissions can be inserted in a hierarchy. However, external roles and permissions cannot be added as children of a permission.

If both PARENT_NAME and PARENT_CODE are left blank, the external role or permission is inserted and possibly published, but is not associated to a hierarchy.

If only one of these fields are left blank, the fields PARENT_TYPE, PARENT_PERMISSION_TYPE, and PARENT_APPLICATION are mandatory fields.

PUBLISH can be set to TRUE only if FULFILLMENT is TRUE or if the external role or permission is already fulfilled.

RIGHT_NAME, RIGHT_CONTENT, RIGHT_MV, RIGHT_REQUIRED are information that is related to permissions. RIGHT_NAME is mandatory only for a permission that hosts a right.

Remove Application Access record track

Use this batch procedure to remove external roles and permissions from your security model.

The line is skipped, when the external role or permission is not found.

Table 140. Remove Application Access record track

Information	Description	Validation
NAME	The name of the external role.	Mandatory if CODE is left blank
CODE	The univocal identifier of the external role.	Optional
TYPE	The type of external role. • Permission • External_Role	Mandatory if CODE is left blank
PERMISSION_TYPE	Permission Type identifier.	Optional, unless it is defined and CODE is blank
APPLICATION	The name of the application to which the external role belongs. The application must be already defined.	Mandatory if CODE is blank
EXTERNAL_REF	The name that is used for the external role or permission on the external system.	Optional

If the EXTERNAL_REF column is populated, the attribute is used in lieu of NAME.

Settings

Use this area to configure basic features of Identity Governance and Intelligence.

This area features the following tabs:

"Core configurations"
Where you can configure several aspects related to the basic behavior of Identity Governance and Intelligence.

"Configure password service" on page 330
Where you setup the Configure Password service for users who have lost their password to Identity Governance and Intelligence.

Core configurations

In the core configuration area, you can configure items that are related to the basic behavior of the Identity Governance and Intelligence platform.

The elements that can be configured are located in the following tabs.

- General
- User Virtual Attributes
- "Internal Events" on page 329

General

The general configuration attributes are described in the following table:

Table 141. General configuration attributes.

Attribute		Description
General	**Log Level**	Four different log levels can be set: • **Error**: Records errors only. • **Warning**: Records errors and indications of possible errors. • **Info**: Records errors, warnings, and information messages. • **Debug**: Records errors, warnings, information messages, and messages associated to the debugging phase.
	View Person's sensible data	If selected, all personal data is visible to Identity Governance and Intelligencemodules; otherwise, it is hidden.

Table 141. General configuration attributes. (continued)

Attribute		Description
SoD/External SoD	**Enable Role Policy**	If selected, all controls for role conflict (Access Risk Controls) are enabled, including controls for External SoD.
	Enable external SoD	If selected, the information about risks associated to users will be provided by external systems.
	Split Role into Permissions	If selected, the common hierarchical structure of a Role is split into a flat collection of component Permissions, before sending it to an external SoD engine.
	Rest	With this radio button you can specify the ReST service address.
	Class	With this radio button you can specify the Java Class used for managing external SoD.
Security	**Token Validity (minutes)**	Indicates the time frame validity of the SAML token, expressed in minutes. The SAML token contains sensitive information related to the user accessing the system, and is used for different steps of the authorization process.

Table 141. General configuration attributes. (continued)

Attribute		Description
Access Select what credentials are requested by the system to grant users access to the Service Center.	**Login UserID and Password**	The credentials requested in the login phase are User ID and password.
	Login UserID	Select this option if you are using a single sign-on authentication method that is based on Open IDConnect or on ISAM (external authentication). The identity of the user is paired with the name of an account that is owned by the user. These two items are used to grant access to a user. When you select this option, you are asked to select an account name in another window. • If you select `Ideas`, you are also asked to select the name of an attribute of this account. • If you select another account, no attribute is asked. The account name alone is used. If the system uses external authentication for single sign-on and this option is not selected, by default it authenticates with the `Ideas` account and the `code` attribute. See Single sign-on overview for reference.
	Login DN	The credentials requested in the login phase include the distinguished name extracted from a digital certificate (generally stored into a smartcard).
	Login SAML	The credential requested in the login phase is a token SAML.
	Internal authorization	Select this option if you are using a single sign-on authentication method that is based on LPTA keys (internal authentication). Note that this option nullifies the `Forget password` feature. See Single sign-on overview for reference.

Table 141. General configuration attributes. (continued)

Attribute		Description
Auditing	**Set Hour**	If selected, sets the Start (`hh:mm`) attribute and changes the measurement unit from minutes to hours of the Repeat every attribute.
	Start (hh:mm)	Defines the time to start the daily audit task.
	Repeat every	Defines the snooze time (in seconds).
	Number of Lines	Number of lines involved in the audit process.

Click **Save** to record your selections.

Important: If you have enabled the **Enable external SoD** with the radio-button **Rest**, you have to update two **IBM Security Identity Governance Task Planner** tasks:

- NightShift
- Housekeeping

Proceed according to the procedure shown below:

1. Access to**IBM Security Identity Governance Task Planner** module
2. Select **Manage** > **Tasks**
3. Select **Actions** > **Add**
4. In the **Details** tab, set a name of the new task **SystemRiskAnalisys**
5. In the **Scheduler** combo box, select the scheduler **Singleton**
6. Click on **Save**
7. Repeat the steps 3, 4, 5 and 6 for the new task **BatchProccessedActionsAGC**
8. In the tab **Task**, select the task **NightShift**
9. Stop the task with **Actions** > **Stop**
10. Repeat the steps 8 and 9 for the task **Housekeeping**
11. Select the stopped task **NightShift**
12. In the central frame, select the tab **Job**.
13. Select the job **SystemRiskAnalisys** and delete it with **Actions** > **Remove**
14. Select the stopped task **Housekeeping**
15. In the central frame, select the tab **Job**.
16. Select the job **BatchProccessedActionsAGC** and delete it with **Actions** > **Remove**
17. In the tab **Task**, select the task **SystemRiskAnalisys**.
18. In the central frame, select the tab **Job**.
19. Select **Actions** > **Add**
20. In the Specify a Job for This Task pop-up window, select the job **SystemRiskAnalisys**
21. Click on **Ok**
22. Repeat the steps 17,18 and 19 for the task **BatchProccessedActionsAGC**
23. In the Add a Job to a Task pop-up window, select the job **BatchProccessedActionsAGC**

24. Click on **Ok**
25. In the **Task** tab, select the task **NightShift**
26. Start the task with **Actions** > **Start**
27. Repeat the steps 25 and 26 for the tasks **Housekeeping**, **SystemRiskAnalisys**, **BatchProccessedActionsAGC**

Important: To update the risk patterns of the registered users after enabling or disabling **External SoD**, run the **Refresh Violation Detection** operation. To do this, select **IBM Security Identity Governance Access Risk Controls** > **Tools** > **Refresh Violation Detection**.

User virtual attributes

Access Governance Core supports a policy for linking user data from external sources. This policy is called virtualization.

The left pane displays a list of the inventoried repositories:

UserErc
The main integration interface table of Identity Governance and Intelligence.

S_User
The table of the users of the Access Requests module.

Swim_User
This table is disabled by default and is used by the Access Requests module.

Note: Do not remove these repositories. You can add other repositories, but the removal of these default repositories can compromise the virtual mapping function.

The enabled repositories are displayed in green; it is disabled in red.

The enabled repositories are used by Access Governance Core.

The right pane contains the **Details** and the **Attribute Mapping** tabs.

When you select a repository in the left pane, the **Details** pane is automatically updated with the repository data.

Repository details are described in the next table:

Table 142. User virtual attributes - repository details.

Detail	Description
Name	Repository name
Description	Short description of the repository
Enabled	When this attribute is selected, the repository is accessible. When it is not selected, the repository cannot be accessed even if the connection parameters are configured correctly.
Type	Repository type. Currently, only the `database` type is available.

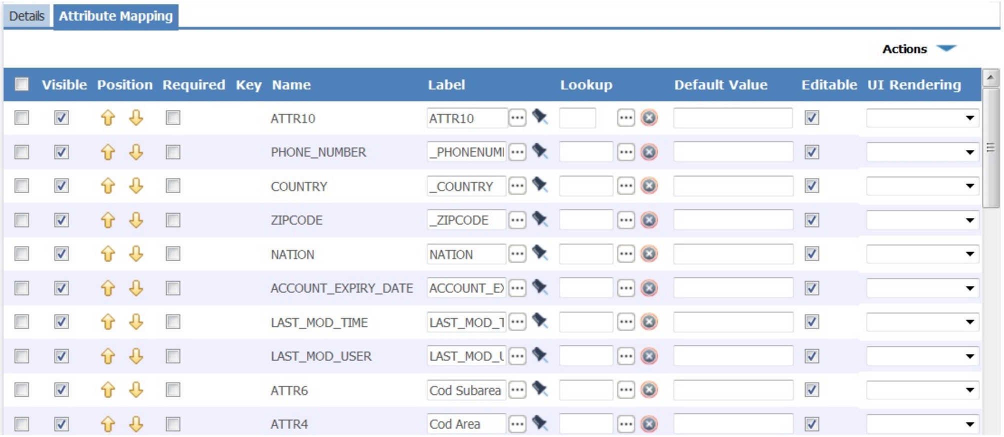
Table 142. User virtual attributes - repository details. (continued)

Detail	Description
Connection	A connection to the database can be: • Internal. PM (AG core module) • External.
Connection Type	This attribute is displayed only if an external connection was chosen. These connection types are available. • JNDI • Custom
JNDI Name	The JNDI name is used for the connection to the database according to the configuration used on the application server in use. It is shown only if the JNDI external connection selected.
Driver	The database driver. It is shown only if a custom external connection selected.
URL	The URL used for connecting to the database. It is shown only if a custom external connection was selected.
UserId	The database User ID. It is shown only if a custom external connection was selected.
Password	The database password. It is shown only if a custom external connection was selected.
Table Name	The name of the table that is to be linked to the PERSON table as part of the customization task.
Database User	The user who is granted access to the database, if the authentication password to the database matches with the User ID.
Key Column	The name of the column in the PERSON table that must match with the column that is selected in the remote table.
Query File	An XML file that contains one or more queries to the database that is hosting the remote table. These queries are used to collect data for building the customized table.

Note: For some repositories, only some of the attributes are active and appear depending on the selection.

Each type of connection requires different parameters. The connection type is chosen in the intermediate part of the **Details** tab, in the `Type` and `Connection` fields. All the parameters that are needed for the selected connection are displayed in the lower part of the same pane.

The virtualization process is based on the **Attribute Mapping** tab:



☐	Visible	Position	Required	Key	Name	Label	Lookup	Default Value	Editable	UI Rendering
☐	☑	⇧ ⇩	☐		ATTR10	ATTR10			☑	▾
☐	☑	⇧ ⇩	☐		PHONE_NUMBER	_PHONENUMI			☑	▾
☐	☑	⇧ ⇩	☐		COUNTRY	_COUNTRY			☑	▾
☐	☑	⇧ ⇩	☐		ZIPCODE	_ZIPCODE			☑	▾
☐	☑	⇧ ⇩	☐		NATION	NATION			☑	▾
☐	☑	⇧ ⇩	☐		ACCOUNT_EXPIRY_DATE	ACCOUNT_E>			☑	▾
☐	☑	⇧ ⇩	☐		LAST_MOD_TIME	LAST_MOD_1			☑	▾
☐	☑	⇧ ⇩	☐		LAST_MOD_USER	LAST_MOD_U			☑	▾
☐	☑	⇧ ⇩	☐		ATTR6	Cod Subarea			☑	▾
☐	☑	⇧ ⇩	☐		ATTR4	Cod Area			☑	▾

The main information of this window is in the **Name** and **Labels** columns.

In the **Name** column, you find the attributes that are related to the repository selected in the **Repository** tab.

If you need to add another attribute to this column, click **Actions** > **Add** and select the attribute from the **Select attribute to add** window.

For the UserErc repository only, if the **Select attribute to add** window does not include an attribute that you might need, you must first create the new attribute in the Identity Governance and Intelligence database. For information about the procedure, see "Adding columns to the UserErc table" on page 165.

In the **Labels** column, you find the attributes that are related to system fields.

If you choose a label and click `Select System Field`, a Select System Field window opens, where you can set the system field that you want to associate to the **Name** on the same row.

For example, you can consider the **`USER_ERC`** table as repository involved into the virtual mapping.

Each attribute can be set in two different modes:

Mode 1
The **`USER_ERC`** attribute (listed under the column **Name**), is mapped with an attribute of **`PERSON`**. Changing the value of an attribute in one table causes the same change in the other table. To customize an attribute with Mode 1, insert the name of the **`PERSON`** attribute to be associated, preceded by an underscore ("_"), into the **Label** column.

Mode 2
The attribute in **`USER_ERC`** is only displayed among the users' external data, on the User Management page of the AG Core Console. To customize an attribute by using Mode 2, insert the attribute and assign it a name in the **Label** text-box. In this case, the change in **`USER_ERC`** is also reflected in the external table.

If you choose a label and click ⋯ `Attribute Localization`, an **Attribute Localization** window opens, where you can set the localization of the label.

The label can be associated to a set of values, related to the **Lookup** control column.

When you click … `Lookup`, a **Lookup Options** window opens.

There you can find several options that are provided by default (`Internal`) or freely configurable (`Pop-up` or `Selectfield`). For more information, see **AGC** > **Configure** > **Rights Lookup**.

To delete a value you previously set for **Lookup** control, click ⊗ **Clear**.

A label can be also associated to a **Default Value** that can be set and shown to the user in Access Requests workflow activities.

You can also decide whether the label value is editable by selecting the related check box in the **Editable** column.

In the **UI Rendering** column, for every datum, you must specify the type of UI element that renders it, as shown in the following list:

- **Textfield**
- **Textarea**
- **Checkbox (true,false)**
- **Checkbox (1,0)**
- **Passwordfield**
- **Date**
- **Date-hours**
- **Date-hours-seconds**

Note:

You can choose **Date**, **Date-hours** or **Date-hours-time** as rendering type for date.

If you set a default value in the **Default Value** position, the format of the default value must comply with the formats that are shared between all the modules.

These product formats are available:

Date `dd/MM/yyyy`

Date-hours
`dd/MM/yyyy HH:mm`

Date-hours-time
`dd/MM/yyyy HH:mm:ss`

To modify the product formats, read the indications that are provided for the Time and Date customization process.

Use the first check box in the left to select the corresponding row if you want:

- Remove it, selecting **Actions** > **Remove**.
- Set as default, indicated with a green check mark, selecting **Actions** > **Set Key** (single selection).

Select the **Visible** check box to specify that the data column must be displayed.

The **Up/Down** yellow arrows define in which order the data columns are displayed in the system.

Select the **Required** check box to specify that the data must exist in the column.

After you click **Actions** > **Add**, the check box is flagged and disabled as not editable if you select attributes that are indicated with a green check mark. In other words, the check box is disabled if you select attributes that are required for the repository that is selected in the **Repository** tab.

If a **Required** check box is not flagged, you can select it to specify that the attribute is required for the remote table/system.

Select **Actions** > **Save** to enable your changes.

Related tasks:

"Adding columns to the UserErc table" on page 165
You can extend the UserErc table with extra columns to import additional user data from another system.

Internal Events

Use this tab to specify if events should be triggered and recorded for local operations that involve the entities of your security model and have an impact on the AG Core database.

The event generation mechanism is used by default for operations (such as the creation of a user, the removal of an entitlement, or the modification of an application) that are run on external targets and need to be communicated to Identity Governance and Intelligence. An event is created and associated to every operation, and stored in a table in Identity Governance and Intelligence. This table can be accessed by the Rules engine and the events stored within can be subjected to additional processing.

Operations run locally on Identity Governance and Intelligence are by default not associated to events. They are saved directly on the database. However, you may want the event mechanism to be applied also to the operations that are run locally on the Identity Governance and Intelligence user interface. In this way, they can be processed by the Rules engine and undergo the same type of processing that is applied to external events.

If you want that events be created also for operations run from the Identity Governance and Intelligence interface, flag any or all of the following check boxes:

Table 143. Options for the creation of internal events associated to local operations.

Attribute		Description
Application	**Enable Internal Events**	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: • Create Application • Remove Application • Modify Application

Table 143. Options for the creation of internal events associated to local operations. (continued)

Attribute		Description
Entitlement	**Enable Internal Events**	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: • Create Entitlement • Remove Entitlement • Modify Entitlement • Add User Entitlement • Remove User Entitlement
Organizational Unit	**Enable Internal Events**	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: • Create OU • Remove OU • Modify OU
User	**Enable Personal Data Internal Events**	Flag if you want an event to be created and stored in the Internal Events table every time one of the following actions is completed: • Create User • Remove User • Modify User
	Enable SoD Status Change Internal Events	Flag if you want an event to be created and stored in the Internal Events table every time the SoD status of a user is changed.

Click **Save** to enable your selections.

Configure password service

Use this tab to create and manage the security questions for users who have lost or forgotten their password to access Identity Governance and Intelligence.

When a user forgets the Identity Governance and Intelligence password and must reset it, the user must answer the security questions in order to log in.

The answers must match the answers entered when the user logged in for the first time. If the answers are correct, the user is given a new password or allowed to reset it.

Use **Configure password service** to create and manage the set of security questions and to set up the details of the response mechanism.

Use the following tabs:

"Configure Forgotten Password service"
Enable the password service and specify the number of security questions that the user must answer.

"Security questions" on page 332
Add, change, or remove security questions in English and other languages.

Configure Forgotten Password service

Use this tab to set up the number of security questions that a user, who is requesting to access Identity Governance and Intelligence after being unable to provide his/her password, must answer correctly.

When a user forgets the password and must reset it, the user must answer security questions to verify its identity. Use this tab to configure the set of security questions that the user must answer to regain access.

In the **Admin configuration** section, select **Enable password service** to enable the following services:

Forgot password
Enables users to reset their Service Center password if they forget it. Users are authenticated with security questions, and either they can enter a new password or they receive a one-time password at their registered email address. Depending on the configuration setup, users might have the option to change their email address.

Self Care
Service Center module where users can change their passwords

Password reset
An Account Change process of the Access Requests module where a manager or entitled person can reset the password for a user

In the **Security questions configuration** section, enter the following information:

Number of security questions asked at first login
Number of security questions to ask a new user. The answers are used for verification when the user is unable to provide the login password.

Number of security questions asked for reset
Number of questions to ask a user who has forgotten a password. This number must be smaller or equal to the number of questions asked at first login.

Number of failed attempts allowed
If the user is unable to correctly answer all the questions asked for reset in the number of attempts specified here, the password is not provided. The user must follow a different process to ask for help. For example, the user might call the Help-desk, an administrator, or a manager.

Note: This option applies to the `Forgot password` and `Self Care` features. It does not affect `Password reset`.

Minimum length of the answer
The minimum number of characters required for every answer.

In the **Mode Configuration** section, specify how to proceed after the user successfully answered all the security questions asked.

Allow user to change password immediately
User is prompted to enter a new password and can login immediately.

Send one-time password to known user address

A new password is emailed to the user. The password is valid for only one login during which the user is prompted to enter a new password.

Select **Allow user to change email address** to let the user edit the address to which the password is to be sent.

Security questions

Use the Security questions tab to work with security questions that a user must answer to receive or reset a password.

The window displays the available security questions. To view a particular question or groups of questions in the list, use the fields located above the **Search** button.

- To view questions in a particular language, click the arrow in **Active Language** to choose a language from a list. The default is the language setting for your Web browser.
- To view specific questions, search for words or strings that you know are in the questions. Enclose the search text between percent symbols (%).
- To find a particular question, you can also enter its **Localization Code**. A localization code is automatically created when the question is added.
- Use the **Active for user** pull-down list to choose Active, Inactive, or All questions. Active questions are questions in the current set.

The **Security Questions** section lists the questions. Unless you choose a different language in the `Active Language` filter, the questions are displayed in the default language of your Web browser. Questions not defined in the active language are shown in English and are followed by a warning that they are not available in the chosen language.

Click the ellipsis (...) next to a question to view it, edit it, or add a localized version.

Use the **Actions** menu to perform one of the following actions:

- **Add** a question.
- **Remove** a selected question. Use the check boxes to select questions.

Add new questions in English first. You can enter a localized version of a question only after the question is defined in English.

The **Active for user** check box makes a question available to users. When a new question is saved, the **Active for user** check box is clear. It is not available to users. To make a question available for use, select the check box. Before you edit a question, or add a locale, clear the check box. You do not need to clear the check box to remove a question.

When a question is removed or thoroughly modified, users who have that question in their `Forgot password` list are asked to answer a new question at their next login.

Chapter 22. Introduction to Access Risk Controls

Access Risk Controls (ARC) module enforces segregation of duties (SoD) checks, based on an innovative relation established between two different layers: the business activities layer and the role-based access control (RBAC) model.

One of the major difficulties that a real organization encounters when implementing an RBAC-based IAG system, is mapping the entities planned within its business model, such as processes, activities, and permissions, with the entities outlined by the RBAC model, such as roles, users, and segregation of duties (SoD) rules.

This problem is particularly evident when transitioning from an existing authorization model, in which authorization profiles have been layered over time with a business-driven vision, to a RBAC model, which requires uniform organizational planning and centralized management of the entire authorization flow.

The Access Risk Controls engine is the tool capable of connecting these two models -- Business and RBAC. More specifically, the ARC module extends features of the RBAC model by introducing the "at-risk activities" concept.

It is always desirable, if not necessary, to prevent a member of the organization from taking on operational privilege that might cause a conflict of interest, and possibly have a detrimental effect on the organization.

For example, consider an employee whose task is to analyze the market searching for new products to add to the company production process.

For obvious reasons, the organization strongly advises that this person should not be simultaneously entrusted with signing of product purchase orders.

The general principle is that an individual employee should not be authorized to perform tasks which might damage the organization.

This aspect is one of the main elements that lead to the implementation of an IAG system.

In the RBAC model, this problem is modeled and managed using the segregation of duties (SoD) concept.

SoD imposes constraints so that a user with a certain role cannot take on another role whose nature conflicts with the one already assigned.

ARC embeds the management of SoD aspects into the more general concept of risk.

The ARC module provides a set of functions that enable:

- Definition of the entire set of activities necessary to complete each specific business process.
- Tracking the risks aggregated to a generic set of activities.

- Aggregation of each activity with the necessary set of authorization entitlements to perform the activity.
- Tracking the entire set of conflicts among the different authorization entitlements.
- Tracking a set of at-risk roles registered in the system.
- Tracking a set of illegal users registered in the system.

Manage

The following functions for managing the main entities of this module are available:

- Business Activities
- Tech Transformation
- Mitigation Controls
- Risk Definitions
- Domains

Business activities

You can manage all functions that are related to the business activity and for modeling a business activity tree structure.

In the left pane **Business Activity**, two tabs are available.

In the **Tree View** tab, you can:

- Browse in the business activity tree for selecting the activity.
- Add or remove activities by using the **Actions** menu.

In the **Search** tab, you have the filters to search for an activity (by clicking **Filter/Hide Filter**) and the **Actions>View** menu item for toggling to the **Tree View** tab.

The table lists the available filters:

Business activity filters	
Filter	**Description**
Name	Name of the business activity.
Code	The unique identifier of the business activity.
Description	Brief description of the business activity.

The content of the right frame changes depending on the tab that is selected in the upper side of the pane. When you access the business activity web interface, the **Details** tab is active by default. Under this tab are available two different accordion panes, selectable by clicking the pane title bar.

- **Activity details**
- **Activity property**

After an activity is selected in the left pane, the **Activity details** pane shows the related data. The **Activity property** pane displays data, related to the selected activity, contained in the external repositories.

The table lists the activity details:

Activity details	
Detail	**Description**
Parent Activity	Name of the parent activity (automatically set after the activity selection in the left frame).
Name	Name that is used within the organization to identify the activity.
ID Code	The univocal identifier of the activity.
Description	Brief description of the activity.
Owner	User who is responsible for the activity. Click ⋯ **User** on the right side of the attribute box to insert a user.

An activity can be aggregated to a set of properties that characterize it.

The **Activity property** pane displays properties that can add specific information about the selected activity.

For example, a property can have, as its value, an external link to the set of implementation regulations and standards compliance that must be implemented by that activity. Another example consists of considering the values of properties into the structure of a rule.

A property is identified by a pair of attributes - *Name*,*Value* -

Properties can be easily added/removed/saved by using the **Add** or **Remove** or **Save** items of the **Actions** menu in the upper right side of the pane.

Note:

It is possible to have multi-values properties. Therefore, it is possible to specify a property **PROP_1** and associate it to a value *VALUE_1*.

Add a line, in the **Activity Property** pane, and specify the same property name (**PROP_1**) associated to a different value (*VALUE_2*).

The available operations that are related to the business activities are:
- Details
- “Linked Permissions”
- “Risk memberships” on page 336
- “Applicable domains” on page 337

Linked Permissions

You can link permissions to activities.

As you select an activity in the left frame, the **Linked Permission** tab is enabled and shows a tree view of the permissions and groups that are associated with the selected Activity.

Note: The *And/Or* condition can be applied to all properties of groups and to everything is contained in the groups; this condition is useful for the SoD analysis.

From the **Linked Permission** tab, it is possible to perform several operations, through the **Actions** buttons:

- **Add Group** adds a group that is identified by an icon and by **PROFILE_GROUP_*random_number***, where **PROFILE_GROUP_** is a fixed string, and ***random_number*** is a random label that is composed by 13 ciphers. **This name is not modifiable!** Any group can contain permissions *And/Or* groups.
- **Add Perm** (Permission) adds permissions directly to the selected activities or to a group.
- **Add Rights** is enabled only if the activity is associated to a permission with rights, and the permission is associated to a group.
- **Remove** removes rights, permissions, and groups (the removal of a group involves the instant removal of everything that is associated with the group).
- **And/Or** inverts the value of the boolean condition of the selected group node.

For **Add Group**, **Add Perm**, and **Add Rights**, a dedicated window opens and shows all the entities that are registered in the system and ready to be added.

For example, for adding a Permission, click **Actions** > **Add Perm**, the window Select Permission opens.

In this window, the following filters can be used for permissions search (click **Filter/Hide Filter**):

Permission filters	
Filter	**Description**
Application	Name of the Application for filtering Permissions. Click ... **Set Application** on the right side of the attribute's box to set an Application.
Type	Type of filtered Permission. Click ... **Set Permission Type** on the right side of the attribute's box to set a Permission Type.
Name	Permission name.
Status	This filter can have four values: • **TBD** when a permission is not joined to any activity but is not in the status Ignored or Missing Activities. • **Linked** if a permission is joined to an activity. • **Ignored** if a permission is not joined to any activity. • **Missing Activities** when the operator doesn't know to which Activities to associate the permission.

Risk memberships

This section allows you to display all risks aggregated to a selected activity.

The **Risk Membership** tab contains the list of risks associated with the activity selected in the left frame.

Selecting a risk from the list and clicking **Actions>Risk**, the Activities risk window opens displaying the list of all activities associated with the risk selected.

If the **Hier** column is flagged with the ✓ icon, the Risk selected is associated with all activities included in the selected activity.

After selecting an activity, by clicking **Actions>View**, the Tree View window opens and displays the exact position of the activity in the hierarchy.

Applicable domains

This section allows you to display all domains aggregated to a selected activity.

The **Applicable Domains** tab contains the list of domains that are already aggregated to the activity selected in the left frame. In the **Applicable Domains** tab, the filters that can be used to perform a domain search are **Name** and **Description**.

Business Activity Mapping

From this tab, you can associate the permissions to one or more activities.

The relationship between the activities and the permissions is "many to many".

An activity can be described using a set of aggregated permissions that are necessary for its implementation. In addition, a single permission can be aggregated to more than one activity.

In the **Permission** tab (left) you can search a specific permission according to the filters summarized in the table below (by clicking **Filter/Hide Filter**):

Table 144. Permission filters

Filter	Description
Application	Name of the application in which the illegal permissions are filtered. Use the ... **Set Application** button on the right side of the attribute box to insert an application.
Type	Type of filtered permission. Use the ... **Set Permission Type** button on the right side of the attribute box to insert a permission type.
Name	Permission name.

Table 144. Permission filters (continued)

Filter	Description
Status	This filter can have four values: • **TBD**: when a permission is not associated to any activity but is not in the status Ignored or Missing Activity. • **Linked**: when a permission is associated to an activity • **Ignored**: when a permission is not associated to any activity • **Missing Activities**: when the operator does not know to which activities the permission should be associated.

The results are displayed in the same pane according to the attributes summarized in the table below:

Table 145. Permission attributes

Attribute	Description
Status	Status of the permission.
Name	Name of the permission.
Type	Type of application.
Application	Name of the application.

From the **Permission** tab, clicking a permission, the **Details** tab (right) is enabled.

In the upper part of this pane is available the information about the selected permission and two check boxes that allow you to change the status of the selected permission from TBD to Ignore or Missing Activity.

Table 146. Permission details

Detail	Description
Name	Name of the permission.
Application	Name of the application.
Description	Brief description of the permission.

To add an activity, click **Add** and, from the Add window, choose the desired activity from the **Tree view** tab or by clicking the **Search** tab and entering the filters for the search operation (by clicking **Filter/Hide Filter**).

Table 147. Activity filters

Filter	Description
Name	Activity name.
Identifier	Unambiguous identifier of the activity.
Description	Brief description of the activity.

To remove an activity, in the **Details** tab, from the list of the associated activities, select the desired activity, then click **Remove**.

When the permission-activity association is removed, the status of the permission changes back to TBD.

After the desired operation was performed, click **Save** in the bottom right part of the pane.

The ℹ icon here indicates that when a permission is in **Linked** status, it is not possible to change it to any other status. To modify the status of the Linked permission, you must remove the associated activity.

Mitigation controls

Mitigations actions are used to define a set of suggested policies that can be activated to correct a conflicting situation, which is theoretically prevented by the risk violation detection.

Each action describes a procedure that the responsible administrator can activate when faced with an identified conflict that must be handled appropriately.

The control action can be performed automatically or manually by an authorized operator.

The ℹ icon here indicates that in the current version of the product, none of the mitigation actions are aggregated to specific automatic procedures.

The **Mitigation** tab contains the list of mitigation actions listed by the system. Select a mitigation control to view its details as displayed in the **Control Details** accordion pane (hosted in the **Mitigation details** tab). In the **Control Properties** accordion pane (at the bottom right of the same tab), are listed the **Mitigation properties**; the administrator can add the properties. This step is not mandatory.

The filters that can be used to perform a mitigation search are **Name** and **Description**. The **Controls** details are indicated in the table below:

Table 148. Controls details

Detail	Description
Name	Name of the mitigation action.
Proc. Code	Numeric code associated with the mitigation.
Description	Brief description of the mitigation.
Extended Description	Extended description.
Link	This attribute can be used to indicate an external link.

In the **Mitigation** tab, a mitigation control can be added or removed by clicking **Add** or **Remove**. In the list below are shown the main operations related to the mitigation controls:

- Mitigation details

- Applicable Risks
- Applicable Domains
- Assigned Users

Applicable risks

In this section are available the procedures used to aggregate risks to mitigations.

In the **Applicable Risks** tab are listed all the risks already aggregated to the mitigation control just selected in the **Mitigation** tab, on the left. In the same pane you can remove a risk by clicking **Remove**. Clicking **Add** button, the Add risk window opens and allows you to add a risk to a mitigation control. By clicking **Risk** in the Add risks window, you can view the activities aggregated to the selected risk.

In the Add risks window, the following filters can be used to perform a risk search (by clicking **Filter/Hide Filter**):

Table 149. Risk filters

Filter	Description
Name	Name of the risk
Description	Brief description of the risk
Status	Status of the risk: • **Assigned Risk**: Risk already assigned to the mitigation. • **Not Assigned Risk**: Risk not assigned to the mitigation yet.
Type	Types of risk inventoried in the system.

By clicking **Risk** in the **Applicable Risks** tab, you can view the activities aggregated to the selected risk.

Applicable domains

In this section are available the procedures used to aggregate domains to a mitigation.

In the **Applicable Domains** tab are listed all the domains already aggregated to the mitigation control selected in the **Mitigation** tab, on the left. In the same tab, you can remove a domain by clicking **Remove**.

Clicking **Add**, the Add domain window opens displaying the list of all domains listed in the system. From this window, you can add a domain to a mitigation control by clicking **Ok**. In the Add domains window, the **Name** (name of the domain) and **Description** (description of the domain) filters can be used to perform a domain search (by clicking **Filter/Hide Filter**).

Assigned users

In this section are available the procedures used to view users with assigned mitigations.

The filters that can be used to perform a user search (by clicking **Filter/Hide Filter**) are described in the following table:

Table 150. User filters

Filter	Description
Search Identity	This field can contain the name, the surname or the User ID of the user.
Associated	This check box is always selected. The search action is performed only on the user already aggregated to an OU.
Organization Unit	OU to which the user belongs.
Hierarchy	If this check box is selected, the operation is executed starting from the selected OU root down through all branches of the subtree that originate from that root.

Risk definition

The **Risk** tab contains the list of risks defined on the system.

In the **Risk** tab, the following filters can be used for the risk search (by clicking **Filter/Hide Filter**):

Table 151. Risk filters

Filter	Description
Name	Risk name.
Description	Description of the risk nature.
Status	Risk status: • **Assigned Risk**: Risk already assigned to the mitigation. • **Not Assigned Risk**: Risk not assigned to the mitigation yet.
Type	Type of risk.

In the **Risk** tab, a risk can be added or removed by clicking **Add** or **Remove**.

Select a risk to view its details in the **Risk Details** tab. The Risk details are described in the table below:

Table 152. Risk details

Detail	Description
Name	Risk name
Description	Description of the risk nature
Type	Type of risk
Scope Type	Type of visibility scope: • **Model**: Risk is assigned as a user role. • **Scope**: Risk is assigned directly to a user (owner). • **Both**: Risk can be assigned using a model or a scope

Table 152. Risk details (continued)

Detail	Description
Level	Level of risk (measured from 0 to 9)
Impact	Description of the risk impact
Likelihood	Value between 0 and 1
Tolerance	Description of the risk tolerance
Trend	Description of the risk trend
Risk acceptance rational	Description of the manageable risk acceptance. Risk acceptance is a value < tolerance
Owner	Name of the person responsible for an activity in a company. Use the … **User** button on the right side of the attribute box to insert a user (owner)
Creation Date	Date of the risk creation (dd/mm/yyyy; hh/mm/ss)

In the list below are shown the main operations related to the risk definition:

- Risk details
- Activity
- Applicable Mitigation Controls
- Users

Activity

In the **Activity** tab are listed all the activities already aggregated to the risk selected in the **Risk** tab, on the left. In the same pane, you can remove an activity by clicking **Remove**. By clicking **View** in the **Activity** tab, you can view the exact position of the selected activity in the tree structure.

By clicking **Add** in the Add window that opens, you can view all the activities listed in the system (**Tree view** tab or **Search** tab). From this window it is possible to add an activity to a risk by clicking **Ok**. In the Add window, the following filters can be used to perform an activity search (by clicking **Filter/Hide Filter**):

Table 153. Activity filters

Name	Description
Name	Name of the business activity.
Identifier	The univocal identifier of the business activity.
Description	Brief description of the business activity.

Applicable mitigation controls

In the **Applicable Mitigation Controls** tab are listed all the mitigation controls already aggregated to the risk selected in the **Risk** tab, on the left. In the same pane, you can remove a mitigation control by clicking **Remove**.

By clicking **Add**, the Add window that appears contains the list of all the mitigation controls listed in the system. From this window, you can add a mitigation control to a risk by clicking **Ok**. In the Add window, the **Name** (name of the mitigation) and **Description** (description of the mitigation) filters can be used to perform a risk search (by clicking **Filter/Hide Filter**).

Users

From the **Users** tab you can view the list of users already aggregated to the risk selected in the **Risk** tab. In this tab, the following filters can be used to perform a search operation (by clicking **Filter/Hide Filter**):

Table 154. User filters

Filter	Description
Search Identity	This field can contain the name, the surname or the User ID of the user.
Associated	This check box is always selected. The search action is performed only on the user already aggregated to an OU.
Organization Unit	OU to which the user belongs.
Hierarchy	If this check box is selected, the operation is executed starting from the selected OU root down through all branches of the subtree that originate from that root.

Domains

In this section you can define a theoretically unlimited number of domains.

The **Domain** tab contains the list of domains registered in the system. Select a domain to view its details in the **Details** tab.

In the **Domain** tab, a domain can be added or removed.

The filters available for a domain search are name and description (by clicking **Filter/Hide Filter**).

The domain details are described in the table below:

Table 155. Domain details

Detail	Description
Type	Type of domain.
Name	Name of the mitigation action.
Description	Brief description of the mitigation.
Extended Description	Extended description.
Note	This attribute can be used to indicate a specific message.

In the list below are shown the main operations related to the domains:

- Details
- Permissions
- Applications

- Mitigation Controls
- Activities

Permissions

In this section are available the procedures used to aggregate permissions to domains.

In the **Permissions** tab are listed all the permissions already aggregated to the domain selected in the **Domain** tab. In the same pane, you can add or remove a permission by clicking **Add** or **Remove**.

Clicking **Add**, the Add window that opens contains the list of all the permissions listed in the system.

In the **Permissions** tab and in the Add window, the following filters can be used to perform a permission search (by clicking **Filter/Hide Filter**):

Table 156. Permissions filters

Filter	Description
Application	Application of the permission. Use the ... **Set Application** button on the right side of the attribute box to insert an application.
Name	Name of the permission.
Type	Type of permission. Use the ... **Set Permission Type** button on the right side of the attribute box to insert a type.

Applications

In the **Applications** tab are listed all the applications already aggregated to the domain selected in the **Domain** tab.

In the same tab, you can add or remove an application by clicking **Add** or **Remove**.

Clicking **Add**, the Add window that opens contains the list of all the applications listed in the system.

In the **Applications** tab and in the Add window, the **Name** (name of the application) filter can be used to perform an application search (by clicking **Filter/Hide Filter**).

Mitigation controls

In the **Applicable Domains** accordion pane are listed all the mitigations already aggregated to the domain selected in the **Domain** tab.

In the same pane, you can remove a mitigation by clicking **Remove**. The **Add** accordion pane contains the list of all the mitigations listed in the system. From this pane, you can add a mitigation to a domain by clicking **Add**.

The filters available for a mitigation search are **Name** and **Description** (by clicking **Filter/Hide Filter**).

Activities

This section allows you to view the activities aggregated to a domain.

In the **Activities** tab are listed all the activities already aggregated to the domain selected in the **Domain** tab, on the left. In this tab, the following filters can be used to perform an activity search (by clicking **Filter/Hide Filter**):

Table 157. Activity filters

Filter	Description
Name	Name of the activity.
Code	Univocal identifier of the business activity.
Description	Description of the activity.

Configure

Use the following functions for configuring the listed elements:

- Configurations

Configurations

Different configurations can be activated for testing different authorizations patterns.

A configuration is built by:

- A set of business activities
- A set of conflicts that are associated to the activities
- A set of domains

In the **Configuration** tab is listed all the configurations available.

The filters **Name** and **Description** can be used for the configuration search (click **Filter/Hide Filter**).

Select a configuration and click **Actions** > **Current** for setting the ✓ working configuration.

Click **Actions** > **Add** for adding a configuration.

The new configuration can be empty or copied from an existing configuration.

In this last one case, you can decide whether to copy the entire configuration or select only some elements:

- Only the activities
- The activities and all the associated conflicts
- Some specific domain or all registered domains

Select a configuration and click **Actions** > **Edit** for changing the settings of the configuration.

Monitor

Monitoring elements

The functions that are available for monitoring some elements are contained in the following list.

- Dashboard
- Risk Violations
- Business Activities
- Scheduled Tasks
- Configuration Set Comparison
- Reports

Dashboard

The upper part of the Dashboard contains a summary of the following permission statuses:

Linked
The permission is joined to an activity.

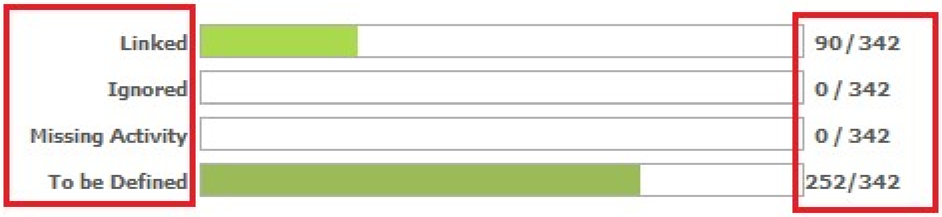
Ignored
The permission is not joined to any activity.

Missing Activity
The operator does not know to which activities to join the permission.

To be Defined (TBD)
The permission is not joined to any activity but is not in the **Ignored** or **Missing Activity** status.

The green status bar and the numbers **X/Y** change according to the number of permissions processed.

For example, the following figure shows 342 permissions to process, where 90 are **Linked**, 0 are **Ignored** or in **Missing Activity**, and 252 are **To be Defined**.



Linked 90 / 342
Ignored 0 / 342
Missing Activity 0 / 342
To be Defined 252/342

Figure 51. Summary of permissions statuses

The upper right part of the page contains information about **Last Changed** and about the user who made them.

The ℹ icon here indicates that the data beyond the green status bar refers to the number of the permissions and not to the association between entities.

The following filters are available by clicking **Filter/Hide Filter**:

Table 158. Dashboard filters

Filter	Description
Application	Clicking ⋯ **Application** opens the Applications window. You can select the available application from the list. The list of available applications changes, depending on the visibility of the user.
Activity	Clicking ⋯ **Activity** opens the Activities window. You can select activities from the **Activity tree** tab or search from the **Activity** tab.
Permission	Name of the permission.
Status	Status of the permission • **To be Defined** • **Linked** • **Ignored** • **Missing Activity**

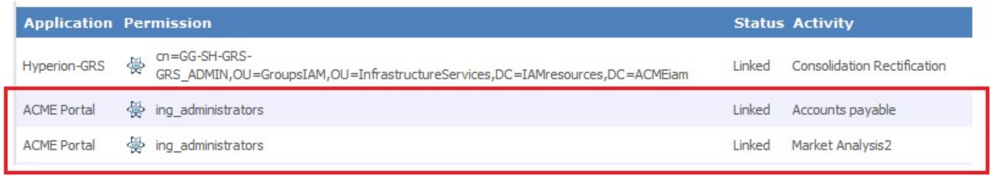
The results are displayed in the same page and summarize the associations made according to the following attributes:

Table 159. Dashboard details

Detail	Description
Application	Name of the application.
Permission	Name of the permission.
Status	Status of the permission.
Activity	Activity that is associated with the permission.

If the same permission is joined to more than one activity, the permission is displayed several times.

Figure 52. Permission-activity relationship



Application	Permission	Status	Activity
Hyperion-GRS	cn=GG-SH-GRS-GRS_ADMIN,OU=GroupsIAM,OU=InfrastructureServices,DC=IAMresources,DC=ACMEiam	Linked	Consolidation Rectification
ACME Portal	ing_administrators	Linked	Accounts payable
ACME Portal	ing_administrators	Linked	Market Analysis2

Risk violations

This section shows the set of ARC violations that can be evaluated by the ARC administrator.

The main sections are listed below:

- User Violations
- Entitlement Violations

Note: Before you begin to work in these sections, you should update the analysis on violations in section **Tools** > **Refresh Violation Detection**.

User violations

This section allows you to view:

- Information on risky or conflicting activities related to the user considered.
- Mitigation actions that can be aggregated to a user and/or with a set of risky/conflicting activities aggregated to the user.
- Domains and activities that are aggregated to a user.

In the **User Violations** tab are displayed all the conflicting users listed by the system.

A user is considered "conflicting" if it has two or more entitlements that are in conflict.

In this tab, the following filters can be used for the user search (by clicking **Filter/Hide Filter**):

Table 160. Conflicting user filters

Filter	Description
Organization Unit	OU to which the user belongs. Use the ⋯ **Organization Unit** button on the right side of the attribute box to insert an OU.
Hierarchy	If this check box is selected, the operation is executed starting from the selected OU root and down through the entire subtree originating from the root.
Search Identity	This field can contain the name, and the surname or the User ID.
DN	Distinguished name of the user.
Search Type	Type of search: • **All**: the search is executed on all users. • **With violations**: the search is executed on conflicting users. • **With mitigated violations**: the search is executed on conflicting user with compensated conflicts. • **With unmitigated violations**: the search is executed on conflicting user with uncompensated conflicts.

Table 160. Conflicting user filters (continued)

Filter	Description
Conflict level	Level of conflict, which can have one of the following three values: 🔴 High 🟠 Medium 🔵 Low These filters are not selectable if the **Search Type** filter is set to **All**.

In the list below are described the main operations related to the user violations:

- Risk info
- Assignment details
- Mitigation Controls

Assignment details

The**Domain** accordion pane list all the domains already aggregated to the user selected in the **User Violations** tab, on the left, while the **Activity** accordion pane contains the list of all the activities aggregated to the user.

Clicking on **View**, you can view the exact position of the activity in the tree structure.

In these accordion panes, the following filters can be used to search information (by clicking **Filter/Hide Filter**):

Table 161. Domains/Activities search filters

Name	Description
Name	Name of the domain/activity.
Description	Description of the domain/activity.

Mitigation Controls

After completing the analysis on a conflicting user, some mitigation actions can be aggregated to that user.

In the **Mitigations** tab is displayed a list of conflicting activities in which the user is involved (upper part).

In the bottom part of the tab, you can find all the mitigation controls already aggregated to the user risk. You can add or remove a mitigation.

Entitlement violations

This section allows you to display and analyze the conflicting entitlements that have been assigned compared to the activities and domains involved.

A conflicting entitlement allows for the execution of conflicting activities. In this tab, the following filters can be used for the entitlement search (by clicking **Filter/Hide Filter**):

Table 162. Conflicting entitlement filters

Filter	Description
Type	Choose one of the following type of entitlement: • **Permission** • **IT role** • **Business role**
Application	Application name according to which conflicting entitlements are filtered.
Name	Entitlement name.
Search type	Choose between: • **All**: the search is executed on all entitlements. • **With Violations**: the search is executed only on conflicting entitlements.
Conflict level	Description of the level of conflict, which can have one of the following three values: 🔵 Low 🟠 Medium 🔴 High These filters are not selectable if the **Search type** filter is set to **All**.

The main operations related to user violations are:

- Risk info
- Assignment details

Assignment details

In the **Domain** accordion pane are listed all the domains already aggregated to the entitlement selected in the **Entitlement Violations** tab, on the left.

The **Activity** accordion pane contains the list of all the activities aggregated to the entitlement selected in the **Entitlement Violations** tab, on the left. Clicking on

View you can view the exact position of the activity in the tree structure. In these accordion panes, the following filters can be used to perform a search (by clicking **Filter/Hide Filter**):

Table 163. Domains/activities filters

Filter	Description
Name	Name of the domain/activity.
Identifier	The univocal identifier of the business activity.
Description	Description of the domain/activity.

Business activities

You can monitor the set of users, entitlements, and group hierarchies associated to a specific business activity and the impact of your decisions of modeling on these associations.

In the left pane of the tab **Business Activity**, two tabs are available.

In the **Tree View** tab, you can browse in the business activity tree for selecting the activity.

In the **Search** tab, you have the filters to search for an activity (by clicking **Filter/Hide Filter**).

The table lists the available filters:

Business activity filters	
Filter	**Description**
Name	Name of the business activity.
Code	The unique identifier of the business activity.
Description	Brief description of the business activity.

The content of the right pane changes depending on the tab that is selected in the upper side of the pane.

The available operations that are related to the business activities are

- “Users”
- “Groups” on page 352
- “Entitlements” on page 352

Users

You can view the users associated to a selected business activity.

In Identity Governance and Intelligence, you can associate a user with one or more business activities, through the permissions hosted by a user.

Permissions can be associated to a business activity through **Manage** > **Business Activities** > **Linked Permissions** tab.

The **Users** tab lists all users associated with a business activity that was selected in the **Business Activities** tab.

Groups

You can view the groups that are associated to a selected business activity.

In Identity Governance and Intelligence, you can associate a group with one or more business activities, through the permissions that are associated with a group (see **Access Governance Core** > **Groups** > **Entitlements** tab).

The **Groups** tab lists all groups that are associated with a business activity that was selected in the **Business Activities** tab.

Entitlements

You can view the entitlements that are associated to a selected business activity.

In Identity Governance and Intelligence, you can associate an entitlement with one or more business activities, through the permissions that are associated with the entitlement.

The **Entitlements** tab lists all entitlements that are associated with a business activity that is selected in the **Business Activities** tab.

A generic entitlement is in the list if at least one of the permissions that are hosted in the entitlement are associated to the business activity selected in the **Business Activities** tab.

Scheduled tasks

In this section are described all the scheduled tasks running or just started.

These tasks are scheduled using the Chapter 28, “Introduction to Task Planner,” on page 637 module.

Configuration comparison

In this section, you can compare two different configurations, and check whether or not the changes performed in a specific configuration alter the model compared to the operating configuration.

In the **Configuration** tab are displayed all the configurations listed by the system.

By selecting the **Compare Configuration** pane and choosing the **Comparative Configuration**, in the **Configurations** tab on the right is displayed the information about the configuration users and the entitlement analysis.

The ✓ icon shows that the analysis completed successfully, the ✘ icon shows that the analysis failed. The bordered green configuration is the operating configuration information.

In the list below are described the main operations related to the mitigation controls:

- Configurations
- Comparison Dashboards
- Comparison Details

Comparison dashboards

Four different default dashboards of two configurations are displayed.

- **Conflicting Business role**
- **Conflicting IT role**
- **Conflicting Permission**
- **Conflicting User**

These dashboards show the structure of the compared configuration.

Comparison details

In this section you can compare detailed reports on paired configurations.

In this situation, more information is provided about changes of numbers and types of conflicts on a single ARC model entity present in both configurations. The **Comparison Details** tab allows you to access the following two tabs:

- **User**
- **Entitlement**

In the **User** tab, you can define the filters to identify the set of conflicting users registered on the system, according to the attributes indicated in the table below:

Table 164. Conflicting user filters

Filter	Description
Organization Unit	OU to which the user belongs.
Hierarchy	Selecting this check box, sets the operation to start executing from the root of the selected OU and down through the hierarchy originating from that root.
Search Identity	This field can host the name, and the surname or the User ID.
DN	Distinguished name of the user.
Conflicting status	**All** All possible conflicting states. **Unaltered** The user remains with the same number of risks in both configurations. **Altered** Every user with a modified number of risks (**Enhanced**, **Worsened**). **Enhanced** In the operating configuration, the user has a lower number of risks compared to the comparative configuration. **Worsened** In the operating configuration, the user has a higher number of risks compared to the comparative configuration.

The risk level distribution provides a view of the qualitative mix of risk levels among the total number of risks.

For example: a user has 11 total risks, 4 have a low risk level and 7 have a high risk level. Therefore, the user is characterized by the low/high qualitative mix of risk levels.

In the **Entitlement** tab, you can define the filters to identify the set of conflicting entitlements registered on the system, according to the attributes indicated in the table below:

Table 165. Conflicting entitlement filters

Filter	Description
Type	Choose one of the following type of entitlement: • Permission • IT role • Business role
Application	Application name by which the conflicting entitlements are filtered.
Name	Entitlement name.
Conflicting status	**All** All possible conflicting status. **Unaltered** The entitlement remains in a conflicting status with the same qualitative mixed conflict level values (High, Medium, Low), in both configurations. **Altered** Every user with a modified number of risks (**Enhanced**, **Worsened**). **Enhanced** In the operating configuration, the entitlement has a lower number of risks compared to the comparative configuration. **Worsened** In the operating configuration, the entitlement has a higher number of risks compared to the comparative configuration.

The concept of risk level distribution, which was addressed in the **User** tab, applies also here.

Report

You can request and download reports.

Scheduling and downloading are the main functions in Reports.

- Request schedules reports.
- Download downloads reports.

For unauthorized users, this menu is not available.

Tools

Tools help to speed up and facilitate some tasks.

Several functions speed up and facilitate the tasks of the following modules:
- Refresh Violations Detection
- Bulk Data Load

Bulk Data Load

You can load large amounts of data.

You can run several types of bulk data-loading in the AG Core database.

The **Actions** tab (left) shows the supported operations.

After you select an operation in **File Batch**, select one of the following options:
- **Download** to get a template (XLS file), related to the currently selected operation.
- **Browse** to search in the file system for an XLS file for the selected loading operation.

When the operation is completed, an information record is appended in the lower-right pane to the list of the previously completed operations.

In the same pane, you can select:
- **Input File** to get the file used in the operation.
- **Log File** to get the operation report.
- Add Permission to Activity
- Add Permission to Domain
- Remove Permission from Activity
- Insert Activities Hierarchy
- Risk Definition
- Remediations to Risks
- Remove Risks
- Remove Activities
- Business Activity Mapping Bulk Load
- Business Activity Mapping Import

A generic record track distinguishes between **Mandatory** and **Optional** fields.

If a mandatory field is empty or populated with unexpected values, the row is skipped unless specified otherwise in the documentation.

According to the data load behavior, populating an Optional field with unexpected or wrong values could cause a row to be skipped.

For information about the procedure, see “Creating a bulk load operation” on page 89.

Add permission to activity record track

This batch procedure can be used to aggregate a permission to an activity. It verifies that the mandatory fields are populated.

Add permission to activity track		
Information	**Description**	**Validation**
APPLICATION	Application name	Mandatory
PERMISSION_TYPE	Permission type identifier	Optional
PERMISSION	Permission name	Mandatory
PERMISSION_CODE	Univocal identifier of a permission	Optional
ACTIVITY_REF	Reference to activity on sheet 2 of the XLS file	Mandatory
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Mandatory
ENVIRONMENT	Environment name	Optional

The XLS source file is organized into two sheets.

The ACTIVITY_REF column on sheet 1 refers to the same column on sheet 2.

Values possibly contained in the ACTIVITY_REF column on sheet 1 must also be present in the same column on sheet 2. Conversely, the ACTIVITY_REF column on sheet 2 might contain values that are not present or referenced in sheet 1.

The APPLICATION field contains the name of the application.

If there is no such application, the row is skipped.

The PERMISSION field contains the name of the permission. A permission with this name, that is aggregated to the above application, must exist. If not, the row is skipped.

PERMISSION_TYPE is an optional field.

However, according to the best practices, this value should be specified to avoid the ambiguity of permissions having the same name (PERMISSION) but different types (PERMISSION_TYPE) .

The following scenario is correct:

PERMISSION = P1 ; PERMISSION_TYPE = T1

PERMISSION = P1; PERMISSION_TYPE = T2

but

PERMISSION = P1 ; PERMISSION_TYPE = T1

PERMISSION = P1; PERMISSION_TYPE =undefined is ambiguous, resulting in the record being skipped and the logging of a warning message:

```
Permission not unique.
```

You can specify PERMISSION_CODE and leave empty APPLICATION, PERMISSION_TYPE and PERMISSION.

Conversely, PERMISSION_CODE can be empty if you fill the columns APPLICATION, PERMISSION_TYPE and PERMISSION.

Activity existence is verified using the given code (CODE field) and name (ACTIVITY field). If there is no such activity, the row is skipped.

The optional ENVIRONMENT field contains the name of the environment.

Environment existence is verified using the given name.

If the ENVIRONMENT field is empty, the default environment is used.

Add permission to domain record track

This batch procedure can be used to aggregate a permission to a domain. It verifies that the mandatory fields are populated.

Add permission to domain track		
Information	**Description**	**Validation**
APPLICATION	Application name.	Mandatory
PERMISSION_TYPE	Permission type identifier.	Optional
PERMISSION	Permission name.	Mandatory
PERMISSION_CODE	Univocal identifier of a permission.	Optional
DOMAIN	Domain name.	Mandatory
ENVIRONMENT	Environment name.	Optional

The APPLICATION field contains the name of the application. If there is no such application, the row is skipped.

PERMISSION_TYPE is an optional field.

However, according to the best practices, this value should be specified to avoid the ambiguity of permission having the same name (PERMISSION) but different types (PERMISSION_TYPE).

The following scenario is correct:

PERMISSION = P1; PERMISSION_TYPE = T1

PERMISSION = P1; PERMISSION_TYPE = T2

but

PERMISSION = P1; PERMISSION_TYPE = T1

PERMISSION = P1; PERMISSION_TYPE = undefined is ambiguous, resulting in the record being skipped and the logging of a warning message:

```
-Permission not unique-.
```

The PERMISSION field contains the name of the permission.

A permission with this name, that is aggregated to the above application, must exist. If not, the row is skipped.

You can specify PERMISSION_CODE and leave empty APPLICATION,PERMISSION_TYPE and PERMISSION.

Conversely, PERMISSION_CODE can be empty if you fill the columns APPLICATION, PERMISSION_TYPE and PERMISSION.

The optional ENVIRONMENT field contains the name of the environment. The environment existence is verified using the given name. If the ENVIRONMENT field is empty, the default environment is used.

The DOMAIN field contains the name of the domain. Domain existence is verified using the given domain name. If no such domain exists, it is created in the default environment.

Remove permission from activity record track

This batch procedure can be used to remove a permission from an activity.

The structure of the record track is described in Add Permission to Activity.

Also in this case, you can specify PERMISSION_CODE and leave empty APPLICATION, PERMISSION_TYPE and PERMISSION.

Conversely, PERMISSION_CODE can be empty if you fill the columns APPLICATION, PERMISSION_TYPE and PERMISSION.

Insert activity hierarchy record track

This batch procedure can be used to insert activities. It verifies that the mandatory fields are populated.

Insert activity hierarchy track		
Information	**Description**	**Validation**
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Mandatory
ENVIRONMENT	Environment identifier name	Optional
DESCRIPTION	Activity description	Optional
PARENT_CODE	Activity parent code	Optional

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used (Working Environment).

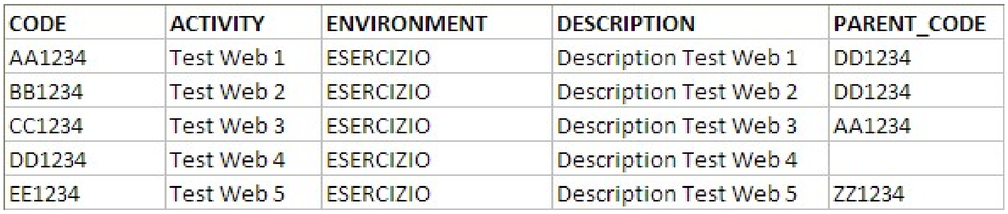
The CODE and ACTIVITY fields contain the activity code and name, respectively.

The existence of an activity with the given code is verified. If the given name does not match the activity name, the row is skipped. If there is no such activity, it will be inserted.

The PARENT_CODE field is used for positioning the activity in the hierarchy.

If this field is left blank, the activity will be inserted as a child of the root activity.

If there is no such activity associated to the given parent code, the activity is inserted as a child of a technical activity called "Undefined", which will be created as needed.



CODE	ACTIVITY	ENVIRONMENT	DESCRIPTION	PARENT_CODE
AA1234	Test Web 1	ESERCIZIO	Description Test Web 1	DD1234
BB1234	Test Web 2	ESERCIZIO	Description Test Web 2	DD1234
CC1234	Test Web 3	ESERCIZIO	Description Test Web 3	AA1234
DD1234	Test Web 4	ESERCIZIO	Description Test Web 4	
EE1234	Test Web 5	ESERCIZIO	Description Test Web 5	ZZ1234

Risk definition record track

This batch procedure can be used to insert risks and aggregate activities to them. It verifies that the mandatory fields are populated.

Risk definition track		
Information	**Description**	**Validation**
RISK_NAME	Risk identifier name	Mandatory
DESCRIPTION	Risk description	Optional
TYPE	Risk type. Default values are: • SOD • RISK	Mandatory
LEVEL	Risk level. Allowed values are: • HIGH • MEDIUM • LOW	Mandatory
ENVIRONMENT	Environment identifier name	Optional
ACTIVITY_CODE	Activity identifier code	Mandatory
HIERARCHY	Hierarchy check. Default values are: • YES • NO	Optional

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used.

The RISK_NAME field contains the name of the risk. If this field is left blank, the row is skipped. Otherwise, if no such risk exists in the selected environment, it is created. The TYPE and LEVEL fields are used for risk insertion.

SOD and RISK are the default values for the TYPE field. The operator can use previously inserted custom risk types. If the custom risk type is not found in the system, the row is skipped and the risk is not inserted.

HIGH, MEDIUM and LOW are default values for the LEVEL field. Anything different from these values automatically sets the risk level to LOW.

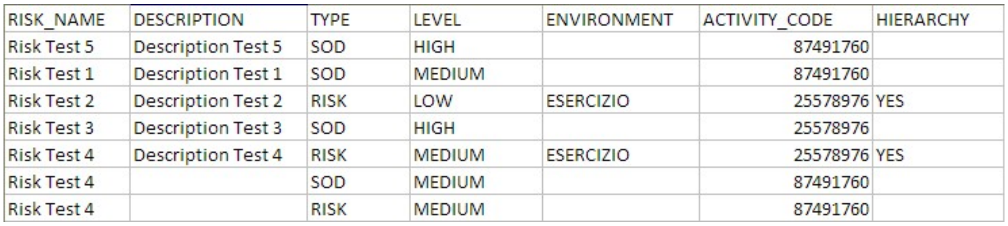
To aggregate activities to the risk, the existence of the activity specified in the ACTIVITY_CODE field is verified. If the field is blank, the row is skipped.

If no such activity is found, aggregation is skipped but the risk is still inserted.

The HIERARCHY field is an optional field that can be used to specify whether the activity-risk aggregation is hierarchical or individual.

If the field value is set to YES, the aggregation involves the specified activity and its subbranches.

If the field value is set to NO, the aggregation involves only the specified activity.



RISK_NAME	DESCRIPTION	TYPE	LEVEL	ENVIRONMENT	ACTIVITY_CODE	HIERARCHY
Risk Test 5	Description Test 5	SOD	HIGH		87491760	
Risk Test 1	Description Test 1	SOD	MEDIUM		87491760	
Risk Test 2	Description Test 2	RISK	LOW	ESERCIZIO	25578976	YES
Risk Test 3	Description Test 3	SOD	HIGH		25578976	
Risk Test 4	Description Test 4	RISK	MEDIUM	ESERCIZIO	25578976	YES
Risk Test 4		SOD	MEDIUM		87491760	
Risk Test 4		RISK	MEDIUM		87491760	

Remediation to risk record track

This batch procedure can be used to insert remediation aggregated to the risk. It verifies that the mandatory fields are populated.

Remediation to risk track		
Information	**Description**	**Validation**
REMEDIATION	Remediation name	Mandatory
CODE	Remediation code	Mandatory
DESCRIPTION	Remediation description (short)	Optional
EXT_DESCR	Remediation description (extended)	Optional
RISK_NAME	Risk name	Mandatory
ENVIRONMENT	Name of environment in which the risk has been defined	Optional

The CODE and REMEDIATION fields contain the remediation code and name, respectively.

The existence of a remediation with the given code is verified. If there is no remediation, it will be inserted.

In the RISK_NAME field, enter the risk name. If there is no existing remediation with this name, the record is skipped.

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped.

If left blank, the default environment is used (Working environment).

Remove risk record track

This batch procedure can be used to delete risks. It verifies that the mandatory fields are correctly populated.

Remove risk track		
Information	**Description**	**Validation**
RISK_NAME	Risk identifier name	Mandatory
DESCRIPTION	Risk description	Not used
TYPE	Risk type	Not used
LEVEL	Risk level	Not used
ENVIRONMENT	Environment identifier name	Optional
ACTIVITY_CODE	Activity identifier code	Not used
HIERARCHY	Hierarchy check	Not used

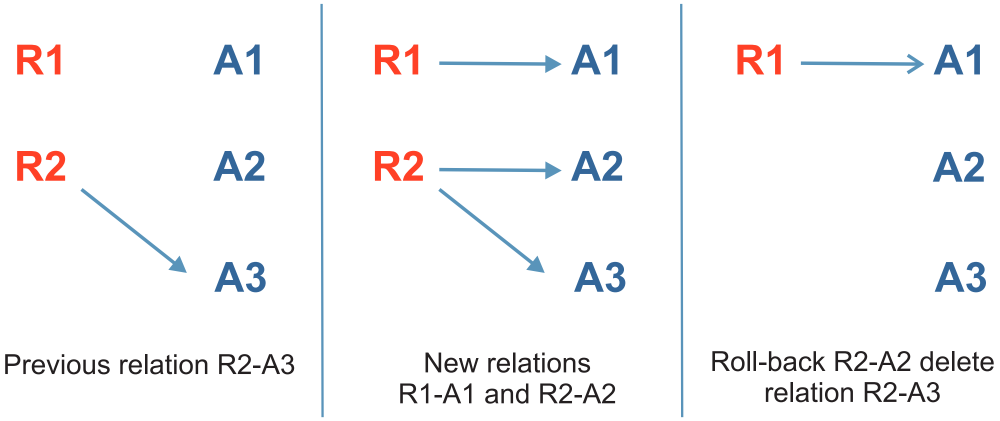
The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used.

The RISK_NAME field contains the name of the risk. If the risk does exist in the selected environment, it is deleted along with all its activity aggregations.

Note:

The record track indicated in the table above is the same as that of the risk definition record track. It is not recommended to use this bulk procedure as a rollback action for the risk definition procedure.

The figure below displays a tricky situation where the removal of risk R2 can have a deceptive side effect:


R1
A1
R2
A2
A3
Previous relation R2-A3
R1
A1
R2
A2
A3
New relations R1-A1 and R2-A2
R1
A1
A2
A3
Roll-back R2-A2 delete relation R2-A3

A rollback action on R2 (on R2-A2 just defined) has a side effect on a relation R2-A3, which was already present before the definition of R2-A2 occurred.

Remove activities record track

This batch procedure can be used to delete activities. It verifies that the mandatory fields are correctly populated.

Remove activities track		
Information	**Description**	**Validation**
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Not used
ENVIRONMENT	Environment identifier name	Optional
DESCRIPTION	Activity description	Not used
PARENT_CODE	Activity parent code	Not used

The ENVIRONMENT field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used.

The CODE field contains the code of the activity to delete. If the existence of an activity with the given code is verified, the activity is deleted.

Business activity mapping bulk load record track

This process provides mapping between activities and permissions.

Permissions of a group can be associated in a AND/OR logical relation.

Groups can be nested up to any level and also nested groups can be associated in a AND/OR logical relation.

This batch procedure can be used to load permissions, permission rights, groups, subgroups, group AND/OR types and group hierarchies.

It can be used:

- After you install Identity Governance and Intelligence.
- At the start up of the project.
- Any time during the production lifetime.

Permissions can be aggregated into groups.

Data imported to Identity Governance and Intelligence is automatically converted into a mapped structure connected to the already available business activity tree structure.

Data should be loaded into an empty structure: if there are some mapping already defined, this will not be removed. The result will be the merging of the two structures.

The business activity tree must be already defined, and all activities linked by the activity business mapping must already be in the system.

If an activity business mapping object in the input excel file (such as an activity or a permission) is not present in the already available target environment, an exception is generated, and the loading process fails.

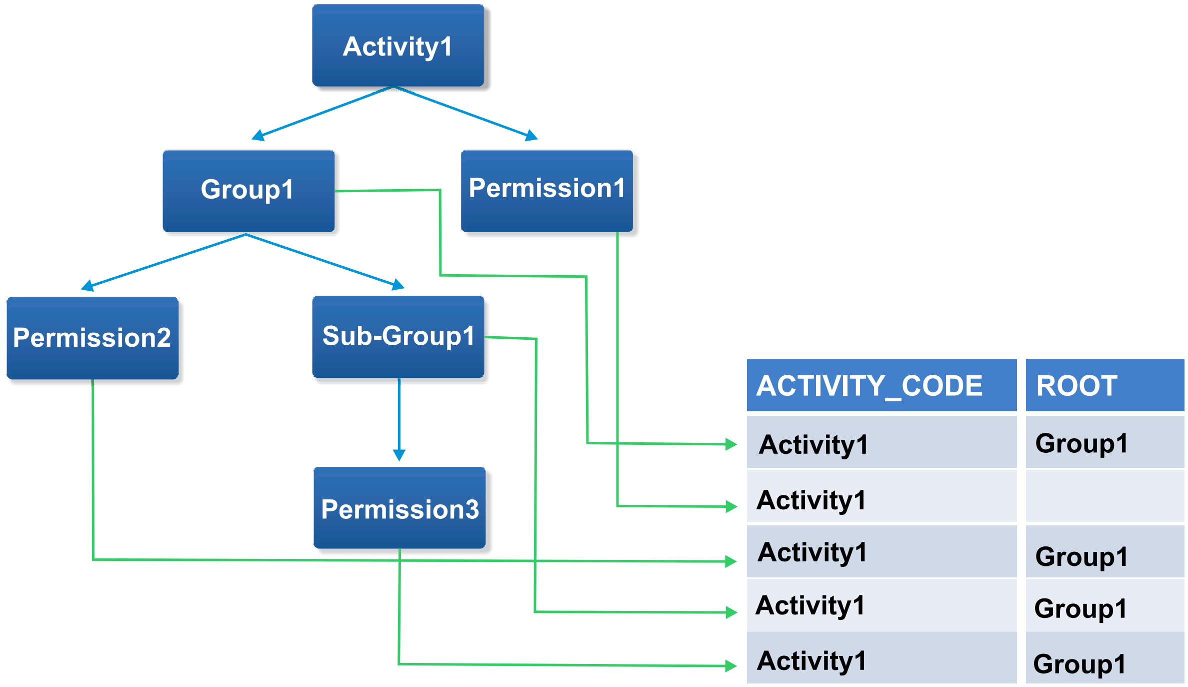
If there are conflicts with existing objects in the TT, the process does not overwrite the existing structure but renames the conflicting objects to allow anyway the loading of the TT structure. The result is the integration of the two TT structures.

The process verifies that the mandatory fields are populated.

Technical transformation bulk load track		
Information	**Description**	**Validation**
ENVIRONMENT	Working environment on which the TT structure is loaded.	Mandatory
ACTIVITY_CODE	Activity (from the activity tree) of the TT to be loaded.	Mandatory
ROOT	If a group hierarchy is present, the root group of the hierarchy.	Optional
COND	And/Or condition. The value OR is the default, also for "single" items.	Optional
ENT_REF	Unique reference of the item in this position.	Mandatory
ENT_PARENT_REF	Direct hierarchical parent of the item.	
TYPE	Allowed values are: • Group • Permission • Right • Right Value For permissions directly linked to the activity, this field must be empty.	Mandatory
PERMISSION	Name of the permission.	Optional
PERMISSION_APP	Application related to the permission. It is empty for groups, subgroups, rights and right values.	Optional
PERMISSION_TYPE	Permission type (as configured in AG Core). It is empty for groups, subgroups, rights and right values.	Optional
RIGHT	Right possibly associated to the permission (if any).	Optional
RIGHT_VALUE	Actual value of the right (if any).	Optional

The ROOT column can be empty only for permissions that are directly linked to the activity.

For data linked to the activity through a structure, the name of the first level group (the group directly linked to the activity) must be set.



ACTIVITY_CODE	ROOT
Activity1	Group1
Activity1	
Activity1	Group1
Activity1	Group1
Activity1	Group1

Figure 53. Graphical representation of Activities-permissions mapping (1).

The COND column can be empty only for permissions that are directly linked to the activity.

In case of a group and a subgroup, the cell content must reflect the selected logic: AND or OR.

For permissions linked to a group or subgroups and for rights and right values, the cell must be set to OR.

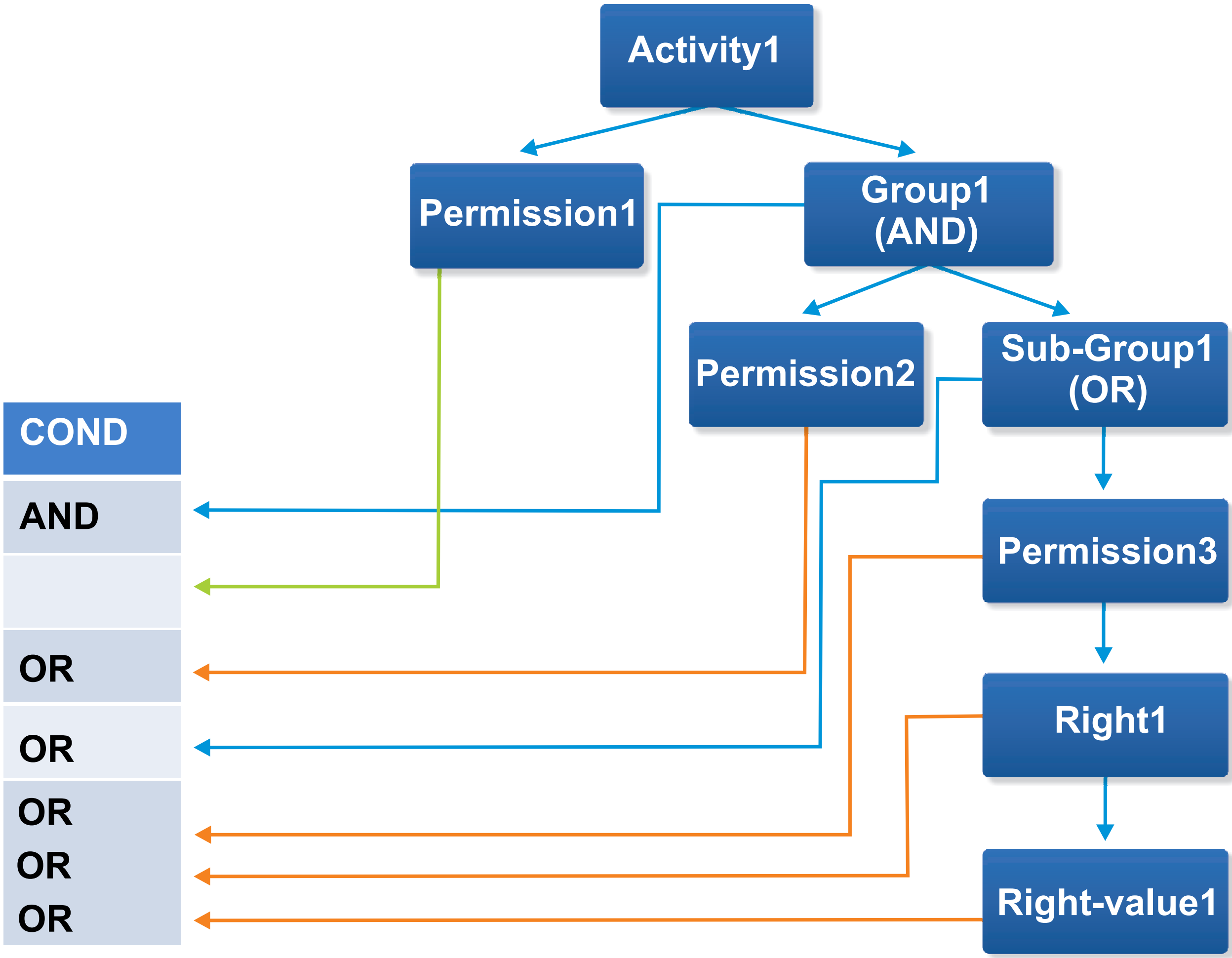


Figure 54. Graphical representation of Activities-permissions mapping (2).

ENT_REF is a unique reference of an item (Group, subgroup, permission, right or right value)

It is mandatory as it is required to identify that item in that precise position inside the TT structure.

For example *Permission1* (PERMISSION column) might be present in several parts of the tree, while the ENT_REF info allows the precise identification of *Permission1* in that specific position.

According to the value of TYPE, is mandatory to fill the columns shown in the table below:

Column set according TYPE	
Filter	**Column set**
Group	ENT_REF
Permission	ENT_REF - PERMISSION
Right	ENT_REF - RIGHT
Right Value	ENT_REF - RIGHT VALUE

To check on the outcome of a bulk load, in the ARC web interface:

1. Select Manage/Business Activities
2. Select the ACTIVITY_CODE activity
3. In the right frame, select the **Linked Permissions** tab
4. Check if the permissions/groups structure linked to that activity is as expected.

If you need to, fix exceptions and reload data according to the same record track.

Generally, the most common error is:

```
Object not found
```

that refers to a missing permission of an activity.

Business Activity Mapping import record track

This process needs to be fed by the output file of the related report Export Tech Transformation.

This report is reachable by clicking **Monitor** > **Reports** in the web interface.

In the left frame, select **Status** > **Export** > **Export Tech Transformation** and run the report shown in the wizard in the right frame.

The output file (`Export Tech Transformation[`*`DD-MM-YYYY HH-MM-SS`*`].XLSX`) can be used for importing a set of Business Activity Mapping data from a system to another.

Analysis

You can check the progress of the analysis of four specific model entities: users, entitlements, groups, and business activities.

This analysis is performed in the operating configuration that is set.

It is executed on all domains that are related to this configuration.

The configuration can be changed by performing **Configure** > **Configuration Set**, selecting **Actions** > **Current**.

A configuration can comprise several domains. A domain can have several activities aggregated to it, and every activity is aggregated to a set of permissions.

After any update of these associations, you have to run a complete analysis on all available entities, upgrading the conflicting relationships between the data model elements related to the mentioned configuration.

All operations available here can be carried out simultaneously. The analysis can be started with **Actions** > **Start**.

Note: If this operation is not active (click **Refresh** to update the green progress bar), the task **Housekeeping** might be stopped (see **Task Planner** > **Manage** > **Task**). In this case, you have to start the task **Housekeeping**.

Chapter 23. Introduction to Process Designer

The PD module helps you design and define the authorization processes.

Process Designer provides a modeler capable of outlining every type of workflow finalized for implementing custom authorization processes, that can be accessed from the Access Requests front end module of IBM Security Identity Governance and Intelligence.

The Process Designer strength lies in its ability to describe an authorization process using an instrument of visual design, that supports the administrator from the beginning of the process to the end, which is marked by the automatic production of front end graphical pages associated with every single activity.

This module, together with Access Governance Core (AGC), which implements the role-based access control engine of IBM Security Identity Governance and Intelligence, provides all the tools and functions needed for managing effectively:

- Requests to access the system application
- Allocation/revocation of authorization profiles
- Password lifecycle
- Notifications that are sent to users during different phases of the authorization process
- Temporary delegations of personal roles associated with users of the system
- Definition of the visibility range associated with an administrative figure.

Process Designer is a highly configurable module that can be used by system integrators or administrators of an organization to plan an authorization workflow.

For every administrative figure (IAM actors), it is possible to define a visibility range that only includes parts of the organization (hierarchy of organizational units and its associated users) that are directly involved and the applications with which it can deliver the necessary authorization.

The integrated workflow engine in this module enables you to create appropriate combinations of authorization actions, with the aim of defining groups of permissions (condensed into roles) for every single user registered by the system.

You can create approval processes for the allocation or revocation of a user role, established by different intermediate levels, each one pertaining to a distinct actor within the process.

Access Requests directly communicates with the Access Governance Core for the allocation and the revocation of user roles and for the propagation of permissions on potential target systems.

An example of the structure of a possible authorization flow, implemented by Process Designer, is shown in the following diagram:

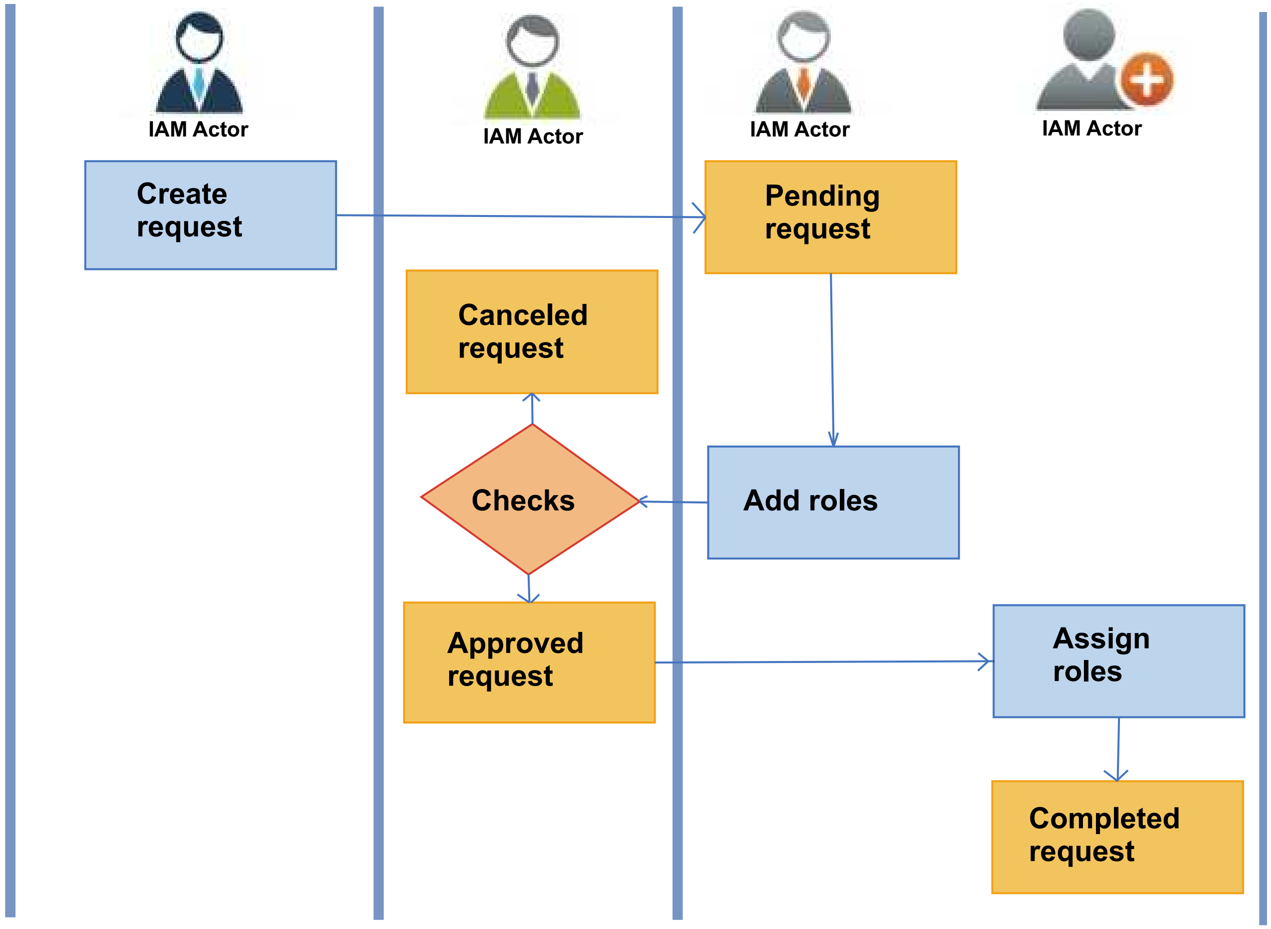


Figure 55. Workflow based on four IAM actors

Authorization process roadmap

The provisioning of access permissions to resources and applications of an organization require a well-defined authorization procedure.

This procedure begins with the generation of a request that some IAM actors take responsibility for; they, in turn, provide additional information and/or authorizations until a final set of conditions is confirmed, according to which the request is processed.

After that, the final user receives the permission (or has it revoked) to access the relevant applications/resources.

In the role-based access control IAM model developed by the IBM Security Identity Governance platform, enabling/disabling user access to an application/resource matches with the allocation/revocation of one or more roles for that user.

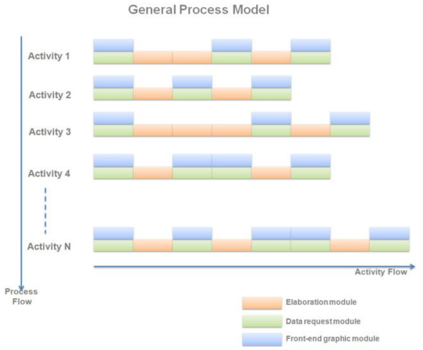
This authorization procedure is structured as a process, which consists of N activities, that in turn run the lifecycle of a request.

From the administrator point of view, designing a process means design a sequence of steps.

Each step matches with the production of an activity.

Every activity will be supported by one or more web pages which represent the graphical front end for the I/O operation which the activity needs. An activity is linked to a role that detects the IAM actor responsible for that activity.

The result of this work is represented by an authorization workflow, conceptually displayed in the following diagram:



Using Process Designer visual wizard, you can define all aspects of an authorization process.

The list below suggests a reference roadmap that follows a best practice to define a process:

1. Define a set of activities.
2. Define a process, structured as a group of activities.
3. Associate an Admin role to each Activity.
4. Associate the operating menu with each bundle role-activity.
5. Change the process status and setting it on line.

External authorization

External authorization is a special case of authorization activity in a **User Access Change** workflow. It is implemented when the organization prefers to use an external target system to approve or reject requests instead of using the Identity Governance and Intelligence request authorization engine.

Configuration

In the **Administration Console** > **Process Designer** module, when configuring an authorization request activity for a **User Access Change** workflow:

1. Select **External Request Authorization** as **Functionality** to authorize the request with the external system.
2. In the **Activity scope** > **Required Data** tab, select **External Authorization** and specify the mechanism to use.

   External authorization can be integrated with the following mechanisms:

   REST APIs

   This mechanism can be used only if there is a web server that exposes the External Authorization Services API.

   Create a RESTful web service with the following External Authorization Services API.

   - /extAuthRest/{realm}/formal

- /extAuthRest/{realm}/informal

See the `External Authorization Services.html` file for information on how to implement the service.

Java implementation

This mechanism can be used only if there is a Java class that implements the IExternalRequest interface (`AccessRequestClient.jar`), which enables direct communication with Identity Governance and Intelligence.

Create a new class that implements the IExternalRequest interface. This interface consists of the sendRequest4ExternalAuthorizaton method.

See the `javaDocAccessRequestClient` file for more information.

External authorization process using REST APIs

When an Employee or Manager creates and submits an access request from the **Service Center** > **Access Requests** module, the request is sent to the external target system. Identity Governance and Intelligence uses the RESTful web service to communicate with the external target system for request authorization.

There are 4 types of responses that the external target system can communicate with the Identity Governance and Intelligence RESTful web service.

`1 = AUTHORIZED`
This code authorizes the request.

`2 = REJECTED`
This code rejects the request.

`3 = WAITING_ASYNCHRONOUS`
This code tells Identity Governance and Intelligence not to call the external target system again but the target system will communicate the response to Identity Governance and Intelligence. The target system calls the Identity Governance and Intelligence RESTful web services that are described in the `IGI External Authorization Services.html` file.

`4 = WAITING_SYNCHRONOUS`
This code tells Identity Governance and Intelligence to invoke the external target system after a period of time because it does not have a valid response.

Code `1 = AUTHORIZED` and `2 = REJECTED` can be used from the external target system to finish the user access request lifecycle immediately. However, if the external target system is not able to return a valid response immediately, it can use codes `3 = WAITING_ASYNCHRONOUS` or `4 = WAITING_SYNCHRONOUS`.

Accessing the REST API documentation

Complete these steps to access and view the guidelines for writing External Authorization Services API or Identity Governance and Intelligence External Authorization Services API:

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Custom File Management**.
2. In the Custom File Management page, select **All Files** > **directories** > **sdk**.
3. Select the `sdk.zip` file and click **Download**.

4. Extract the file and navigate to **sdk** > **RESTDoc**. The folder contains the following REST APIs:

   External Authorization Services API

   Manages the request related to a list of permissions or roles that can be added, removed, or renewed according to the request type.

   See `External Authorization Services.html` for complete information about creating the correct RESTful web service for external authorization.

   Identity Governance and Intelligence External Authorization Services API

   Accepts or refuses the received request. Use these REST APIs when the RESTful web server returns `3 = WAITING_ASYNCHRONOUS`.

   The RESTful web service must meet the requirements that are specified in the `IGI External Authorization Services.html` file. Otherwise, external authorization cannot work.
5. Open either the `External Authorization Services.html` or `IGI External Authorization Services.html`, whichever is applicable.
6. Click the **GET** or **POST** button, where applicable, to view how the **Request** and **Response** must be implemented for the REST API.

   For information about **User Access Change** workflow, see the following topics:

   "User access: generating a request" on page 849
   Select this tab to add role access to one or more selected users.

   "Insert/Update user: processing a request" on page 876
   You can view a summary of the generated requests.

   "Insert/Update user: executing a request" on page 884
   For this type of authorization workflow the execution step is an empty step.

Modeling an activity

An activity is an aggregation of functional attributes.

An activity is characterized by a set of attributes that define all its aspects.

An activity can be schematically represented as a function with N attributes, depending on the value of its attributes:

$$ACTIVITY = f\ (ATTR_1,\ ATTR_2,\ ATTR_3,\ ...\ ATTR_N...)$$

The attributes can be classified as identifying attributes and operating attributes (scope attributes), as shown in the following table:

Table 166. Activity attributes

Attributes	Category	Description
Identifying attributes	**Type**	Type of process that involves the activity
	Mode	Category of action of the activity
	Name	Name of the activity
	Context	Set of homogeneous functions that are used to manage an authorization process
	Functionality	Name of the function that is related to the Context field set
Operating attributes	**Beneficiary**	Visibility for users who are affected by the request
	Delegator	Visibility for users who delegated the request
	Application	Visibility set by application access. Only administrators with access to the specified applications can see the request.
	Entitlement	Visibility set by entitlement access. Only administrators with access to the specified entitlements can see the request.
	Request Scope	Type of request
	Required Data	Specifies data that is required for an activity
	Email Data	Specifies email template to use
	Entity Scope	Model entity scope of a specified activity

Use the Activity details pane to model activities.

Type attribute

The Type attribute specifies the type of process to use with the activity.

Table 167. Type attribute values

Type	Description
Direct	Process that consists of a single EXE activity
Workflow	Process that consists of an appropriate set of GEN, AUTH, and EXE activities
Escalation	Process that consists of an appropriate AUTH activity

Mode attribute

The following table describes the Mode attribute:

Table 168. Mode attribute values

Category	Description
GEN: Generation	Generation request activity. This activity typically opens an authorization workflow.
AUTH: Authorization	Authorization activity. This activity is typically assigned to a IAG officer for authorizing a request.
EXE: Execute	Activity that executes what was indicated in the previously authorized request or a one-shot action.

Context attribute

The following table describes the context attributes of an activity:

Table 169. Context attribute values

Context	Description
Account Change	Related to account creation operations
Admin Access Change	Related to operations for the modification of the administrative role
Admin Delegation Change	Related to administration delegation operations
Delegation Change	Related to delegation renewal operations
Entitlement Management	Related to creating and modifying a model entity Entitlement
Incompatibility Management	Related to incompatibility management operations
Redirect Management	Related to the management of requests that are escalated after they expire
Request Report	Related to the request report operations
User Access Request	Related to the activities used to manage a user transfer
User Management	Related to creating and modifying a model entity User

Functionality attribute

Each Functionality value corresponds to a Context value, Type value, and Mode value.

Table 170. Functionality attribute values

Context	Type	Mode	Functionality	Description
Incompatibility Management	**Escalation**	**AUTH**	Authorize Incompatibility In Delegation	Authorize Incompatibility Request

Table 170. Functionality attribute values (continued)

Context	Type	Mode	Functionality	Description
Redirect Management	**Escalation**	**AUTH**	Redirect for Expiration	Manage expired requests
Account Change	**Workflow**	**GEN**	Detailed Request	Account Change
	Workflow	**AUTH**	Request Authorization	Authorization
	Workflow	**EXE**	Request Execution	Account Change Assignment
User Access Change	**Workflow**	**GEN**	Formal Request	Formal Request
	Workflow	**AUTH**	Request Authorization	Request Authorization
	Workflow	**AUTH**	External Request Authorization	Authorize Request with external system
	Workflow	**EXE**	Request Execution	Role Assignment
Admin Access Change	**Workflow**	**GEN**	Formal Request	Formal Request
	Workflow	**AUTH**	Request Authorization	Request Authorization
	Workflow	**EXE**	Request Execution	Request Execution
Delegation Change	**Workflow**	**GEN**	Application Filtered Request	Delegation that is filtered by Application
	Workflow	**AUTH**	Request Authorization	Authorization
	Workflow	**EXE**	Request Execution	Delegation Assignment
Admin Delegation Change	**Workflow**	**GEN**	Formal Request	Formal Request
	Workflow	**AUTH**	Request Authorization	Request Authorization
	Workflow	**EXE**	Request Execution	Request Execution

Table 170. Functionality attribute values (continued)

Context	Type	Mode	Functionality	Description
User Management	**Workflow**	**GEN**	Insert User	Insert User Request
	Workflow	**AUTH**	Insert User	Insert User Request Authorization
	Workflow	**EXE**	Execute Insert User	Insert User Request Execution
	Workflow	**GEN**	Update User	Update User Request
	Workflow	**AUTH**	Update User	Update User Request Authorization
	Workflow	**EXE**	Execute Update User	Update User Request Execution
Entitlement Management	**Workflow**	**GEN**	Insert Entitlement	Insert Entitlement Request
	Workflow	**AUTH**	Authorize Insert Entitlement	Authorize Insert Entitlement Request
	Workflow	**EXE**	Execute Insert Entitlement	Execute Insert Entitlement Request
	Workflow	**GEN**	Update Entitlement	Update Entitlement Request
	Workflow	**AUTH**	Authorize Entitlement Update	Authorize Entitlement Update Request
	Workflow	**EXE**	Execute Insert User	Insert Entitlement Request
Request Report	**Direct**	**EXE**	Request Report	Request Report
	Direct	**EXE**	Daily Work	Daily Work

Operating attributes

Operating attributes (grouped under the tab **Activity scope**) determine the behavior of an activity.

All these attributes set the scope of the activity, thus the set of data model objects under the control of the activity.

Operating attributes are shown in the following tabs:

- Beneficiary
- Delegator

- Application
- Entitlement
- Request Scope
- Required Data
- Redirect Scope
- Email data
- Entity Scope

Beneficiary tab

This attribute specifies sets of users that are associated with different scopes in the organizational structure.

Table 171. Visibility levels by Beneficiary

Visibility type		Description
By Organization Unit Tree	**All Users**	Visible to all the OUs in the realm (all users in the organization)
	Actor	Visible only to the IAM actor involved in the activity (logged in user)
	All Users belonging to an OU	Visible to a selected OU, thus to the users associated with that OU
	All Users belonging to an OU (including hierarchy)	Visible to a selected OU and the entire subtree, thus to all users associated with the hierarchy
	All Users belonging to logged OU	Visible to all OUs that are visible to the IAM actor involved in the activity
	All Users belonging to logged OU (including hierarchy)	Visible to all OUs visible to the IAM actor involved in the activity and to the entire subtree, thus to all users associated with the hierarchy
	All Users belonging to logged Hierarchy	Visible to all groups of a specific hierarchy that are visible to the IAM actor involved in the activity

Delegator tab

A delegator assigns its own access rights to another user for a limited time. The scope criteria are the same as the ones described in Beneficiary.

This type of visibility is involved in processes of delegation.

Application tab

An application represents an external system that is connected to the IAM system. A single target (for example, Active Directory) can manage more than one application.

An IAM actor in the authorization process usually acts only on a subset of applications (Application scope).

The Process Designer administrator sets the application visibility for every IAM actor that is involved in the process.

The following table lists the different levels of user visibility that you can specify on applications:

Table 172. Visibility levels by application

Visibility type	Description
All Applications	All registered applications
Specific Applications	Group of applications that are selected by clicking **Specific Applications**
User owned Applications	Applications that are owned by the user that is involved in the management of the activity.

Entitlement tab

Entitlements determine access to applications.

An IAM actor that manages the authorization process, usually acts only on a subset of entitlements (entitlement scope).

The Process Designer administrator sets the entitlement visibility levels for every IAM actor that is involved in the process.

Table 173. Visibility levels

Visibility type	Description
All Entitlements	All registered entitlements
Specific Entitlements	A group of entitlements that are selected by clicking **Specific Entitlements**
User owned Entitlements	Entitlements that are owned by the user that is involved in the management of the activity.

Request scope tab

For some activities, you can select **Request type** and **Request status** as additive filters to use. They specify the **Request scope**. The activity can manage requests of the indicated type and status.

If the **Ownership** check box is selected, the IAM actor can manage owned requests.

A parent request can generate child requests. Each has its own independent flow and status. The parent request state depends on the state of its child requests.

The parent request is completed if its child requests are completed. The parent request status is partially completed until the child requests are completed.

Required data tab

Data needed to configure the activity is specified in the **Required Data** tab.

The filter value is set in the **Required Data Value** field.

Table 174. Activity identifiable attributes - required data

Field	Description
Active Data	Check box to activate the data filter
Required Data	Name of the data filter
Required Data value	Value of the data filter. The value can be edited
Description	Description of the data filter

The required data depends on the activity that you are configuring.

Table 175. Required data items

Required Data	Assignable Values	Description
Role Operation	• Assign • Remove • Renew	Select the operation that is related to the entitlement involved in the activity.
Account Operation	• Change Password • Suspend/Restore	Select the operation that is related to the account password.

Table 175. Required data items (continued)

Required Data	Assignable Values	Description
User identification	• None • Security questions • Security questions or by other means	Specify how to verify the identity of a user that needs a password change or account restoration. **None** Is not verified. The identity verification step is omitted in Access Requests. **Security questions** Must be verified by asking security questions and matching the answers with answers that are provided at first login. **Security questions or by other means** Is verified either by the answer to security questions or by some other process. The wizard step that displays the questions in Access Requests includes also a check box that can be selected to skip the security questions.
Applicant's IGI password	• True • False	If `true`, the applicant is requested to enter the password. In this context, `applicant` is a manager or Help-desk who makes the request for a user (the `beneficiary`).

Table 175. Required data items (continued)

Required Data	Assignable Values	Description
Change password mode	- Entered by applicant - Entered by applicant with no show/hide option - Created by system	Select one of the following options: - The applicant enters a new password for the beneficiary and: – The password characters are concealed when the applicant types them. – Applicant can choose between showing or hiding the password characters as they are being typed. - The password is created automatically when the applicant clicks **Generate**.
Email password to beneficiary	- Do not email - To editable address - Only if address exists	Specify a rule for emailing the new password to the beneficiary. The password - Is not to be emailed. Other means of communication are used. - Is to be emailed to an address that the applicant can enter or edit. - Is to be emailed only if the beneficiary's email address is recorded.
Suspend/Restore account suspending codes	- Authoritative - Expire - Maintenance - Security - Technical - Terminated	Select a subset of Account suspending codes to use.
Entity Operation	N.A.	Select the entity operation to use.
Role Type Assignable	- Business Role - Application Role - Permissions - External Role	Select the entitlement type to use.
IT Autopopulate Operation	- True - False	Autopopulate Application Entitlements.
IT Open Filter Operation	- True - False	Set open filter for Application Search form.
Entity Data Type	- Details - Structure	Select the entity data type to use.

Table 175. Required data items (continued)

Required Data	Assignable Values	Description
Self Authorization	• True • False	If `true`, self-authorization is enabled (when the beneficiary is the Authorizer).
Branch one shot Authorization	• True • False	If `true`, one-shot authorization is enabled, otherwise parallel authorization (Business Role) is used.
Split Entitlement	• True • False	If `true`, the entitlement that is involved in the request is split in its own Permissions.
External Authorization	Free text	External call for authorization. You can specify a ReST implementation with a URL or a Java implementation with a Java class name.
Enable Like Mike	• True • False	If `true`, the AR workflow panel includes the ability to select Like Mike functionality. You can assign the entitlements of one user directly to another use.
Show user's business activities	• True • False	If `true`, the AR workflow panel displays the business activities that are associated with the users that are listed in the request.
Enable dashboard	• True • False	If `true`, displays a dashboard view of this activity in the Service Center. This option is available for the following functionalities: • Formal Request in the User Access Change context. • Daily Work in the Request Report context.

Redirect Scope tab

This attribute specifies a set of users to whom the authorization of a request can be redirected by the original assignee. Within each set, the users to whom the authorization task can be redirected must have the Redirection Approver administrative role.

This tab is present only within the authorization activity of a WorkFlow process.

Table 176. Visibility levels for redirection

Visibility type		Description
By Organization Unit Tree	**All Users**	Visible to all the OUs in the realm (all users in the organization)
	Actor	Visible only to the IAM actor involved in the activity (logged in user)
	All Users belonging to an OU	Visible to a selected OU, thus to the users associated with that OU
	All Users belonging to an OU (including hierarchy)	Visible to a selected OU and the entire subtree, thus to all users associated with the hierarchy
	All Users belonging to logged OU	Visible to all OUs that are visible to the IAM actor involved in the activity
	All Users belonging to logged OU (including hierarchy)	Visible to all OUs visible to the IAM actor involved in the activity and to the entire subtree, thus to all users associated with the hierarchy
	All Users belonging to logged Hierarchy	Visible to all groups of a specific hierarchy that are visible to the IAM actor involved in the activity

See also Enabling authorization requests to be redirected to other approvers.

Email data tab

For some activities, you can define the action of sending an email.

Click **Template email** to choose the email template to use. Click **Preview** to see the template. Templates are managed in **Access Governance Core** > **Configure** > **Email**.

Entity Scope

For some activities of type GEN, if you choose the context **Entity Change**, you define the data model entity by clicking **Entity**.

Click **Repository** to define the target repository where you read the user attributes.

Repositories are managed in **Access Governance Core** > **Settings** > **User Virtual Attributes**.

When you choose a repository and click **Load**, repository attributes are shown at the bottom of the panel.

Table 177. Repository attributes

Attribute	Description
Visibility	If selected, the related field in the **Field** column is visible in output.
Mandatory	If selected, it is a mandatory field.
Order	Select a field and use the Up and Down arrows to position it in the list.
Field	Field to be shown/hidden. See **Visibility**.
Localization	All fields can be localized. For this localization task, see **Access Governance Core** > **Settings** > **Core Configuration** > **User Virtual Attributes**.
Default Value	Select **Editable** to allow a user to specify a default value.
Editable	If selected, this field is editable in the output panel (Access Request activity).
UI Rendering	Specifies the rendering of the related **Field**. See **Access Governance Core** > **Settings** > **Core Configuration** > **User Virtual Attributes**. The available controls are • **Textfield** • **Textarea** • **Checkbox (true, false)** • **Checkbox (1, 0)** • **Passwordfield** • **Date** • **Date-hours** • **Date-hours-seconds**

Manage

The following functions for managing the main entities of this module are available:

- Process
- Activity

Activity

Select this tab to define the activities that can be associated with a process.

Refer to Modeling an Activity to learn the attributes of an activity.

Select **Activity** on the left to identify all the activities registered in the system.

To find a specific activity, click **Filter** and use the filters described in the next table:

Table 178. Activity filters

Filter	Description
Name	Activity name

Table 178. Activity filters (continued)

Filter	Description
Mode	The activity can be one of the following modes: - **Generation** - **Authorization** - **Execute**
Type of Activity (derived by the type of processes)	The activity can be one of the following types: - **Direct** - **Workflow** - **Escalation**

Select an activity from the list to view its details in the right pane. Click **Actions** to do any of the following actions on the activity:

- Synchronize all
- Copy
- Add
- Remove

Synchronize all

The Process Designer and the Access Request modules use two distinct databases.

After you defined an activity in Process Designer, you must propagate the changes to the Access Requests database.

Select **Actions** > **Synchronize all** to synchronize one or more activities that you selected from the Activity list.

Copy

When you decide to modify an activity, the suggested action is to clone the activity and to modify the copied version. This option is preferred to changing directly the original version of the activity.

If you must change an activity considerably, this option becomes less useful and it probably makes more sense to do an Add action.

Follow these steps to copy an activity:

1. Select the activity from the Activity list.
2. Click **Actions** > **Copy**.
3. In the **Activity Copy** tab on the right, edit at least fields **Name** and **Description**.
4. Click **Save** to save the cloned activity.

Add

Defining an activity implies defining its identifying and operating attributes.

A solid knowledge of the concepts that are described in “Modeling an activity” on page 371 can facilitate this task.

Follow these steps to define an activity:

1. Select **Actions** > **Add**.
2. Select a **Type** and a **Mode** from the lists in the Select Activity Modality window and click **Ok**.
3. Set the required attributes in theInsert Activity pane. The values that you can select for **Context** depend on the type and mode you set in the preceding step. Also, the **Functionality** value is filled based on the value specified in **Context** . See “Modeling an activity” on page 371 for details.
4. After you defined the attributes, the **Activity Scope** tabs are displayed in the lower section of the pane. The tabs vary based on the selected activity, and depend on your selections of **Context** and **Functionality**.
5. Click **Save** to save the activity definition.

Remove

Follow these steps to remove an activity:

1. Select the activity from the Activity list.
2. Click **Actions** > **Remove**.
3. Click **Ok** to confirm the operation.

Note: You cannot delete an activity that is already linked to a process. If you try, the web interface displays a message that informs you about the inability to remove the activity.

Before you remove an activity, get a clear knowledge of how many processes host the activity that you want remove. To learn this information, follow these steps:

1. After you selected the activity from the list, click **Processes using this activity** on the right, where all the processes that are linked to the activity are listed.
2. Select **Show Process** to be redirected to **Manage** > **Process** where you get a full view of the process and of the position of the activity within the process.

Managing processes

A visual tool and a wizard guide you through the definition and management of authorization processes.

In the **Process** tab, on the left, you can identify the processes registered in the system.

A process is characterized by a set of main attributes that are shown in the **Details** tab and are described in the next table:

Table 179. Process attributes

Attribute	Description
Name	The name of the process. If the process name is in italics, the process is not synchronized.
Code	A numerical and univocal code that is associated to the process for logging and reporting activities.
Context	A context that identifies a set of homogeneous functions that are used to manage an authorization process.

Table 179. Process attributes (continued)

Attribute	Description		
Type	Workflow		A process composed of an appropriate combination of GEN, AUTH, and EXE activities.
	Escalation		A process composed by a sequence of AUTH activities (at least, only one AUTH activity).
	Direct		A process composed of a single EXE activity.
Status	Off Line	❗	A process is **Off Line** during its initial planning stages, which include the design and configurations of activities, followed by the association of any activity with one or more IAM actors. From this state, the process can move only to the **On Line** state.
	On Line	✓	A process is in this state when it is ready to be run. From this state, the process can move only to the **Maintenance** state.
	Maintenance	🛠	A process is in this state when some modifications must be made to the starting structure of the process or to the configuration of one or more activities. From this state, the process can move only to the **On Line** state.

Some of these attributes, **Name**, **Type**, and **Status**, can be used for filtering processes.

The next table lists the activity types that you can define for building a process:

Table 180. Activity block-types

Icon	Type	Description
🧩	Generation (GEN)	A request generation function that is used to obtain something such as a VPN access, a role on a target system, or an account or different credentials.
📄	Authorization (AUTH)	A serial approval function for a previously entered request.
⚙	Execution (EXE)	A function that runs the requested operation. It is not used for target systems that are automatically synchronized with the IAM system. It is necessary if the activity on the target is fulfilled manually. The execution step automatically produces an event for the operator who manually acts on the target. This event might be used to trigger external applications such as help desk applications.

Select **Actions** to do one of the following actions:

- Copy
- Add
- Remove
- "Export" on page 388
- "Import" on page 388
- Maintenance
- Online

Note: Copy and **Add** are useful with the configuration of a process.

Remove

To remove a process, follow these steps:

1. Select the process in **Process**.
2. Click **Actions** > **Remove**.
3. Click **Ok** to confirm the operation.

Note:

You cannot delete an ✓ **On Line** process.

Export

To export a process, follow these steps:

1. Select the process in **Process**.
2. Click **Actions** > **Export**.
3. If the process is **On Line** or in **Maintenance**, the Assign - Process name window displays the roles that are assigned to the activities. Click **Ok.**
4. A system-based window opens where you can save or open the `.zip` file that contains the XML file that describes the process.
5. Click **Ok** in the window that shows the outcome of the operation.

Import

To import a process, follow these steps:

1. Click **Import**.
2. In the window Select file to be imported, click **Browse** and select the file to import.
3. Click **Ok** in the window that shows the outcome of the operation.

Maintenance

To place a process in the **Maintenance** state, follow these steps:

1. Select a process in **Process**.
2. If the process is ✓ **On Line**, click **Actions** > **Maintanance**.
3. The status icon of the process is updated to 🛠 **Maintenance**.

Online

To place a process in the **On Line** state, follow these steps:

1. Select a process in **Process**.
2. If the process is in 🛠 **Maintenance**, click **Actions** > **On Line**.
3. The status icon of the process is updated to ✓ **On Line**.

Defining and configuring a process

The definition of a process includes activities that were previously defined and optional steps.

Activities that make up a process

Different types of processes are made up by different sets of activities. The next table describes what activity modes go into a specific process.

Table 181. The activity modes that make up a process

Process Type	Activity Modes
Workflow	1. A starting GEN activity 2. Any number, including 0, of AUTH activities 3. A final and single EXE activity
Direct	A single EXE activity
Escalation	At least one AUTH activity

Defining a process

To define a process, follow these steps:

1. In the **Process** tab, select **Actions** > **Add**.
2. In the **Details** tab, set the main attributes for the new process and click **Next**.
3. Depending on the process type that you specified in the previous step, the **Configuration** tab is populated with a set of activity icons.

   A vertical bar of the activity block types is displayed on the left side of the pane. It shows the blocks that you can select based on the process type that you are defining.
4. For a **Workflow** process, select the GEN activity block type (🧩) on the left to place the block in the center of the window. Select this block to configure the activity.

   The activity configuration pane is displayed.
5. In this pane, you can:
   - Create a filter in the activities set, choosing a registered context in **Context**.
   - Select one of the activities in the list.
   - Click **Details** to view the configuration of the activity.
   - Click **Create** to create a new activity (see how to configure an Activity).
6. Click **Ok** to close the Activity window and to confirm the previous operations.
7. Click → if you need to add one or more extensions to the activity that you defined.
8. For a **Workflow** or **Escalation** process, select the AUTH activity block type (📄) on the left to place the block in the center of the window. Select this block to configure the activity.

   The activity configuration pane is displayed.
9. Repeat steps 5, 6, and 7 for this block.
10. Repeat steps 8 and 9 for every AUTH activity added to the process.

11. For a **Workflow** or **Direct** process, select the EXE activity block type (⚙) on the left to place the block in the center of the window. Select this block to configure the activity.

    The activity configuration pane is displayed.
12. Repeat steps 5, 6, and 7 for this block.
13. Click **Save**.

In a Workflow process, the GEN activity sets the context. All the activities that can be selected in the steps that follow, inherit the activity context defined in the first step.

You must associate each block that describes the flow of a process with a specific activity context. If you do not make this association, you can still select the next block.

After you saved the process, you can at anytime click any of its activity blocks to view and optionally modify the setup of the activity.

You can add an extension to each activity to make the behavior of the activity more flexible. To add an extension, right-click the arrow➔, that you find on the upper right of the activity block. A box menu is displayed. It contains options that are shown depending on the settings of the activity. The options are described in the next table.

Table 182. Activity extensions that you can define

Action	Extension	Description
Add	Pre-action	Displays the Insert Rule window where you can add a rule that was previously defined in Access Governance Core. The rule is carried out before the activity starts. Appends a **Pre-action** icon, → , on the left of the activity block.
	Post-action	Displays the Insert Rule window where you can add a rule that was previously defined in Access Governance Core. The rule is carried out after the activity completed. Appends a **Post-action** icon, ← , on the right of the activity block.
	Notification	Displays a Notification window where you can define the details of an email or of an SMS message that is sent after the activity completed. Appends a **Notification** icon, ✉ , on the right of the activity block.
	Escalation	Adds the possibility to escalate the authorization activity to another user. This action might be needed when the request presents a segregation of duties conflict. Displays the Select Escalation Process window where you can select an escalation process from the ones that were already defined in Process Designer. These processes are based on the Incompatibility Management activity context. These processes are not based on the Redirect Management activity context, which is time based. Appends an **Escalation** icon, 🚩 , on the left of the activity block.
Remove	Pre-action	Removes the pre-action from the activity. The rule is no longer run. The icon is removed from the activity block.
	Post-action	Removes the post-action from the activity. The rule is no longer run. The icon is removed from the activity block.
	Notification	Removes the notification from the activity. The notification is no longer sent. The icon is removed from the activity block.
	Escalation	Removes the link to the escalation process. The icon is removed from the activity block.

Table 182. Activity extensions that you can define (continued)

Action	Extension	Description
Remove Activity		Removes the activity block from the process. The activity block is removed.
Required Auth	True	Applies to authorization activity blocks. It specifies that the authorization step is required to complete the activity. The frame of the authorization activity block shows in green.
	False	Applies to authorization activity blocks. It specifies that the authorization step is not required to complete the activity. The frame of the authorization activity block shows in gray.

When you finished building the process in the **Configuration** tab, select one of the following actions.

- To return to the **Details** tab, select **Previous**.
- To proceed with the definition of a WorkFlow process, select **Next** and set up policies that manage the expiration of the associated authorization request.
- To proceed with the definition of an Escalation process, select **Next** and choose an action for the associated escalation request.
- To proceed with the definition of a Direct process, select **Next** and assign a role (with the **Assign** tab) to the activities of the process that you built.

Copying a process

If you need to modify a process that is online, your best option is to clone the project and to modify its copied version. In this way, you can keep the process online while you modify its clone and, when you are finished, replace the process online with the modified version.

Note: The activities of a process are copied along with the process.

Copying a process does not include these items:

- The roles that are associated with the activities that form a process (see **Process** > **Assign**).
- The user menu that is associated with the roles and activities (see **Configure** > **Menu**).

For this reason, after you copied a process, ensure that you associate the roles to the activities and create the menu for linking activities.

To copy a process, follow these steps:

1. In the **Process** tab, select the process.
2. Select **Actions** > **Copy**
3. In the **Details** tab, change the **Name** and the **Description** of the process. The system automatically changes the process name from *Process Name* to *Process Name-Copy*
4. Click **Save**.

Assigning an expiration reminder policy to a WorkFlow process

In this step, assign a priority and the associated expiration reminder policy to the WorkFlow process. You also provide instructions for handling requests that reach their expiration time without being processed.

The selections that you make in this pane apply to the steps of the requests that are generated with this process. For example, take a process that comprises three steps - Generation, Authorization, and Execution. The action and other options that you specify here apply at the end of each step, if the associated request is not processed by the appointed manager or operator.

Make your selections for the options that are described in the following table.

Table 183. Options for the Reminder pane in the definition of a WorkFlow process

Option	Description
Priority	Assign a priority level. The priority level specifies the time that the step of the request reaches its expiration. It also determines the expiration reminder policy that is taken before this time. The priority goes from High to Unassigned. It must be already configured in Workflow Priority under **Settings**.
Action at expiration	Select which action is taken for the request if it expires and remains unprocessed.
Enable Priority override	Flag this option to specify that the manager or the operator, who submits the request in Service Center, can change the priority. In this case, the **Priority** field in the panes of the request in Access Requests is enabled.
Escalation Process	Choose an escalation process if you selected the **Escalate** action after the request step expires. The escalation process must be already defined, based on the Redirect Management context and on the Redirect for Expiration functionality.
Send Notification after the Action at expiration	Select to send a notification, when the action is triggered at expiration time. If you flag this option, the options that follow are enabled.
Template	Select the template that is used to assemble the text and the placeholder keys for the notification that is sent. The template must be of type Reminder and must be already defined. **Remember:** Depending on the definition of the template, the notification can be sent by email, SMS, or both.

Table 183. Options for the Reminder pane in the definition of a WorkFlow process (continued)

Option	Description
Email Recipients	If the notification is sent by email, select the recipients. Flag one or more types of recipients. **Requested For** Send the email to the beneficiary of the request. **Requested By** Send the email to the generator of the request. **Approvers** Send the email to the approvers involved into the process. **Fixed Addresses** Send the email to other users. Specify the email addresses, separating them with semicolons, in the related field. For each type, select if the recipient is direct, carbon copy, or blind carbon copy. Select **Preview** to display a preview of the email.
SMS Recipients	If the notification is sent by SMS, select the recipients. Flag one or more types of recipients. **Requested For** Send the SMS message to the beneficiary of the request. **Requested By** Send the SMS message to the generator of the request. **Approvers** Send the SMS message to the approvers involved into the process. **Fixed Phone Numbers** Send the SMS message to other users. Specify the mobile telephone numbers, separating them with semicolons, in the related field. Select **Preview** to display a preview of the SMS message.

Select **Next** to assign a role (with the **Assign** tab) to the activities of the process.

Select **Save** to save your process definition.

Assigning an expiration reminder policy to an Escalation process

In this step, define an action for an escalated request and instructions for sending a notification after the action completed.

The escalation request is triggered by an authorization request that either involves a segregation of duties conflict or becomes expired. In the first case, the underlying escalation process is based on the Incompatibility Management context. In the latter case, it is based on the Redirect Management context.

An escalation process that is based on the Incompatibility Management context is started when you add the Escalation extension to an activity block of a Workflow process.

An escalation process that is based on the Redirect Management context is started when you select the Escalate **Action at expiration** in the Reminder pane of a Workflow process.

Make your selections for the options that are described in the following table.

Table 184. Options for the Reminder pane in the definition of an Escalation process

Option	Description
Action at expiration	Select which action is automatically taken for the escalated request if it expires and remains unprocessed. **No Action** **Approve** **Reject** The time count of an escalated authorization request, whose underlying Workflow process is defined with a priority, is inherited by the escalation process. When the request goes into the escalation phase, the time count is restarted from 0 for the duration that is defined by the priority.
Send Notification after the Action at expiration	Select to send a notification, when the action is triggered at expiration time. If you flag this option, the options that follow are enabled.
Template	Select the template that is used to assemble the text and the placeholder keys for the notification that is sent. The template must be of type Reminder and must be already defined. **Remember:** Depending on the definition of the template, the notification can be sent by email, SMS, or both.

Table 184. Options for the Reminder pane in the definition of an Escalation process (continued)

Option	Description
Email Recipients	If the notification is sent by email, select the recipients. Flag one or more types of recipients. **Requested For** Send the email to the beneficiary of the request. **Requested By** Send the email to the generator of the request. **Approvers** Send the email to the approvers involved into the process. **Fixed Addresses** Send the email to other users. Specify the email addresses, separating them with semicolons, in the related field. For each type, select if the recipient is direct, carbon copy, or blind carbon copy. Select **Preview** to display a preview of the email.
SMS Recipients	If the notification is sent by SMS, select the recipients. Flag one or more types of recipients. **Requested For** Send the SMS message to the beneficiary of the request. **Requested By** Send the SMS message to the generator of the request. **Approvers** Send the SMS message to the approvers involved into the process. **Fixed Phone Numbers** Send the SMS message to other users. Specify the mobile telephone numbers, separating them with semicolons, in the related field. Select **Preview** to display a preview of the SMS message.

Select **Next** to assign a role (with the **Assign** tab) to the process activity.

Select **Save** to save your process definition.

Assign

In this section, you associate an administrative role to an activity of the process.

Administrative roles are registered in the system in **Access Governance Core** > **Configure** > **Admin Roles**. Go this section also to define new administrative roles that might be required for a company process.

The **Assign** tab includes a variable number of other tabs, depending on how many activities are in the process.

Use these tabs to associate one or more administrative role to each activity of the process.

Every activity in the process must be assigned at least one administrative role. If you fail to do this, a diagnostic message is displayed when the you set the process to **Online**.

AUTH activities can be assigned only one role. More roles can be associated to the other types of activities.

Select **Actions** to manage the associations.

- Add
- Remove
- Activites associated to an Admin Role

Adding a role to an activity

Take these steps to link an administrative role to the activity.

1. Make sure the process is in the Offline or Maintenance status.
2. Select the activity to which you intend to assign a role.
3. Select **Actions** > **Add**.
4. In the Roles pane, find the available roles. You can use**Filter** to make your search quicker.
5. Select one or more roles from the list. You can use the Ctrl or Shift keys for a multiple selection.
6. Click **Ok**.

The selected roles are added to the activity.

Removing a role from an activity

Take these steps to remove an administrative role from the activity.

1. Make sure the process is in the Offline or Maintenance status.
2. Select the activity from which you intend to remove a role.
3. In the list of roles, select one or more roles. You can use the Ctrl or Shift keys for a multiple selection.
4. Select **Actions** > **Remove**.

The selected roles are removed from the activity.

Managing activities associated to an Administrative Role

Select a role in the list to display a tree structure on the right of your screen.

In the tree, the root represents the role that you selected and the branches - at one level only - represent the activities that are associated to that role.

The branches might display more than one instance of the same activity. This is because there might be several processes with activities that have the same name and are associated to the selected role.

You can select a number of actions from the bottom of the right panel.

Localize
To localize the label of a selected node.

Move Up
To reposition a selected node.

Remove
To delete a selected node.

Save To validate any sequence of the previous actions.

You can also right-click an activity to display a menu that includes the **Move Up/Down** and **Localize** actions.

Select **Details** to display more data about the activity.

Select **Menu Link Disabled** to hide one or more activities and to change their selection color from green to gray.

Defining a Redirect for Expiration escalation process

Define an escalation process that is based on the Redirect for Expiration functionality to manage requests that need to be escalated when they become expired.

This type of process is triggered when you select the Escalate action in the Reminder step of the definition of a WorkFlow process. It implies that if a request that is generated by the WorkFlow process expires without being processed, the request is automatically escalated to an assigned manager.

You can then assign this process to a Risk Manager, or similar administrative role, who is authorized to pick up the Expired request and to accept or reject it.

Take the following steps to define a Redirect for Expiration escalation process.

1. In the **Process** pane, select **Actions** > **Add**.
2. In the **Details** pane, enter a name for the new process, select **Escalation** in **Type**, and click **Next**.
3. In the **Configuration** pane, click the **Sequential authorization** activity block type ( ) on the left to place the block in the center of the window. Select this block to configure the activity.

   The Activity configuration pane is displayed.
4. In the Activity pane, select **Redirect Management** in **Context**.
5. Select **Create**.
6. In the Insert Activity window, select **Redirect for Expiration** in **Functionality**.
7. Set the **Activity scope** by clicking the Beneficiary, Application, and Entitlement tabs and selecting an option for each one.
8. Click **Close** and then **Ok** to complete the **Redirect Management** activity configuration part.

9. Optionally, right-click ➔ on the right of the activity block to add one or more extensions to the activity that you defined.
10. Select **Next** to move to the Assign pane.

    In this pane, you select one or more administrative or business roles that are authorized to process requests defined by this process.
11. Click **Actions** > **Add** to display the Roles window and select a role to whom the process is assigned.

    Repeat this step for as many roles as you deem necessary.
12. Click **Save** to save your definition and to return to the Details pane.
13. To activate the process, set **Status** to **On Line** in the Details pane. Alternatively, in the Process pane, select the process from the list and select **Actions** > **Online**.

The process is now defined and active.

Take these steps to link this Escalation process to a WorkFlow process.
1. Go to the Reminder page of the WorkFlow process definition.
2. Select **Escalate** as the **Action at expiration**.
3. Click **Escalation Process** and select the name of the process that you defined here.

Managers who are authorized to this process can now use **Service Center** > **Access Requests** to process the expired requests that are generated by the WorkFlow process.

Configure

Use the following functions for configuring the listed elements:
- Menu
- "Rules" on page 401

Menu

After a process was defined and structured into a group of activities, each activity is associated to an administrative role.

To run such activities, any authorized user (thus, any user with a specific administrative role) have to access to a front end web that support the execution of this set of activities.

The **Menu** operation allows you to associate, to each administrative role, a group of activities associated with that role.

This menu is interpreted by the page constructor engine of Process Designer to assemble the front end graphic that will support each user in the management of the different activities (Access Request module).

Consider a process called P1, which is composed by the activities GEN1, AUTH1, EXE1.

Similarly, we can have a process called P2, made up of: GEN2, AUTH2, EXE2.

Assume that you have associated the activities AUTH 1 and AUTH 2 to an administrative role ADMIN_ROLE_1.

If the user Mike Brown has the role ADMIN_ROLE_1, the front end web shows to him the activities AUTH 1 and AUTH 2.

Note: The following indications can be implemented only for the processes that are found in the offline or maintenance status.

On the left tab **Process** you find the list of all registered process.

Click **Filter/Hide Filter** and enter the filter data, then click **Search**.

After selecting a process, in the right tab **Menu** are available two combo box, **Roles** and **Activities**.

In the **Roles** combo box are listed all administrative roles involved in the process previously selected.

Selecting one of listed roles, a tree structure is shown where the root is the role selected and the leafs (only one level) are the activities associated to that role.

The list of leafs can display more than one instance of the same activity. This is because you can have several processes, with activities that have the same name, associated to the selected role.

In the **Activities** combo box are listed all the activities involved in the process selected.

Selecting one of listed activities, in the tree on the left is highlighted the instance involved in the process previously selected (other instances possibly present are related to other processes).

If the activity selected is not present, you can add it to the hierarchy with the **Add** button.

At the bottom side of the **Menu** tab you can run one or more of the following actions:

- Click **Localize** to localize the label of a selected node.
- Click **Move Up/Move Down** to reposition a selected node.
- Click **Remove** to delete a selected node.
- Click **Save** to validate any sequence of previous actions.

In addition, selecting one activity, through a mouse right-click button, a service menu opens with some functions already indicated above (**Move Up/Down** and **Localize**).

Through the function **Details**, the Details pop-up shows data related to the activity.

If you want to hide one or more activities, tick the check box **Menu Link Disabled**, changing from green to gray the selection color of the activity.

Rules

In this context, rules are used to define customized processes that can be linked to a work flow activity.

Only one Rule Class is available:

- **Workflow** groups all the **Rule Sequence** available for pre-action and post-action processes.

The **Actions** menu of the tab **Rules** in the left frame lists the following actions:

Import
For importing the XML representation of a Rule or of a Rule Sequence (Rule Flow).

Export For exporting a Rule or a Rule Sequence (Rule Flow).

Add Adds a Group of Rules (function that is maintained for legacy reason).

Remove
Removes a Rule or a Group of rules (for Groups, function that is maintained for legacy reason).

Enable/Disable
Enable or disable a Rule execution into a sequence.

Move Up/Down
Move the Rule up/down in the Rule sequence.

In the right frame, you can find two main accordion panes

Rules Package
In this accordion pane is available all functions for managing a Rule that is selected in the left frame.

Package Imports
In this accordion pane is present all functions for managing packages of rules.

Related concepts:

Chapter 16, “Rules introduction,” on page 129
One of the angle stones of IBM Security Identity Governance and Intelligence concern the concept of rule. An IGI Administrator can write rules for different goals. Rules are used for extending the native capabilities of the product.

Rules Package

This pane includes functions that manage rules with the Rules editor.

Based on your selections in the left tab **Rules**, a set of rule are listed in this pane.

The **Actions** menu lists the following actions:

Verify Checks the formal structure of the code that defines a rule (needs the selection of one of the rule listed).

Modify
Opens the Rules editor to modify a rule.

Delete Deletes a selected rule.

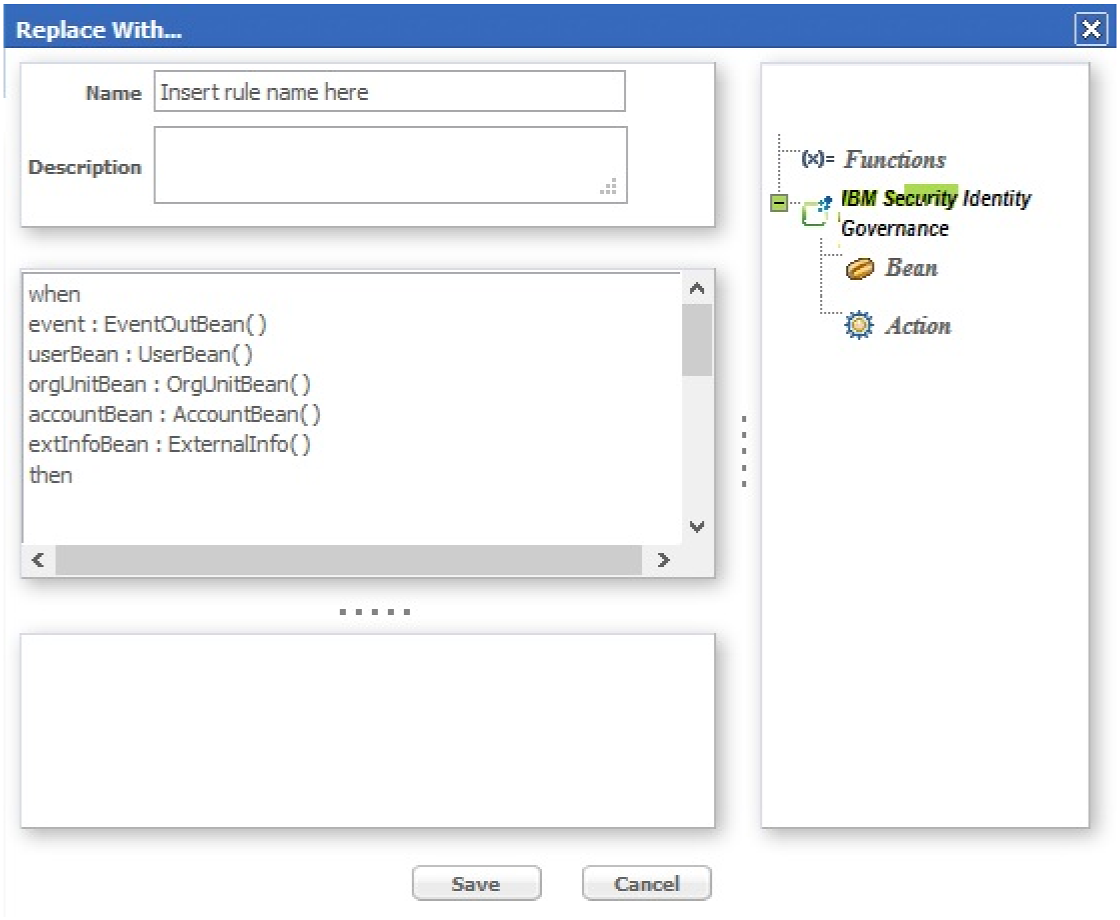
Create Creates a rule.

Add
Adds a rule that is selected in the list to a **Group** (legacy versions) or **Rule Sequence** that is selected in the **Rules** tab, on the left.

Rules Editor

The Rules Editor speeds up the writing of code contained in a Rule.

The next figure shows the Rules Editor panel:



Name: Insert rule name here

```
when
event : EventOutBean()
userBean : UserBean()
orgUnitBean : OrgUnitBean()
accountBean : AccountBean()
extInfoBean : ExternalInfo()
then
```

Figure 56. The Rules Editor panel.

The next table shows what buttons and icons are present in the Rules editor:

Table 185. Symbols of the Rules editor.

Icon	Description
C	Import a Java class
C	Java class
▤	New variable
(x)=	New function
●	Bean

Table 185. Symbols of the Rules editor. (continued)

Icon	Description
⚙	Action
	Associated rule: rule that is associated to a rules group
	Split: used to construct flow processes in situations that require a branch point.
◇	Constraints
📁	Rules group
	Flow process

All the Rules must have the following structure:

- **Condition Area** (between "when" and "then")
- **Action Area** (immediately after "then").

The word **when** identifies the beginning of the conditions area.

Any number of conditions can be inserted and the actions will be executed only if all the conditions are verified (logic AND between each condition)

The word **then** identifies the beginning of the actions area.

Actions are written in normal Java code; all classes making up the libraries delivered with the product are available for writing actions.

A complete list and descriptions are available in the **Replace with...**.

The conditions are written according to Drools syntax.

Every condition verifies, within the Working Memory, whether or not there are one or more objects identified by the Beans. If such objects are actually found, the actions described above will be executed on them.

The **Replace with...** window contains the code obtained from the Editor.

From the frame on the right side of the window, predefined code blocks can be selected and placed directly into the **Replace with...**.

The objects are grouped in a hierarchy and managed through a tree structure.

The **Object** frame contains the nodes corresponding to the higher level object categories. The two initial main categories are:

- Functions
- Ideas

Based on the selection, the objects can be **Functions**, **Bean** or **Action** and their methods are visible below the selected object (fourth level of the tree):

Now, select a leaf object (a method) and insert it into the **Replace With...** frame (left) using the **Actions**>**Add** button.

This operation can be performed to modify or create a Rule.

Note: The name of a Bean can be written without its system path ONLY if it has been imported into the Package that contains the Rule.

Functions

The Functions category contains functions for fundamental Rule-writing constructs; the same frame lists the following four elements:

- if
- ifelse
- ifelseif
- for

Select one of the functions and click **Add** to insert the related parametric code into the **Replace with...** frame, at the end of the already-listed code. The parameters to edit are easily recognized because they are between two '$' symbols.

For example, in the IF ELSE construct, you have to edit the parameters CONDITION1, ACTION1 and ACTION2.

Proceed in one of two ways to edit the parameters:

- Directly write the code instead of the corresponding symbolic string (e.g., CONDTION1 included between two '$' characters);
- Use the editor again.

In this last case, click **Field** > **Bean** > **AccountBean** and select one of the objects listed, then click **Add**:

Selecting $ACTION2$ places the selected code block in the position that was covered by $ACTION2$. If none of the parameters in the window are selected, click **Ok** to place the code block at the end of the already-present code. To eliminate a potentially wrong insertion, cancel the corresponding code directly in the **Replace With...** frame.

Bean and Action Elements

The IBM Security Identity Governance folder contains the following two folders:

- Bean
- Action

These folders contain ALL the Beans and Actions imported into the Rules Package; in particular, the Bean folder contains the Beans imported into the Package that are part of the libraries delivered with the product. Client users of the AG Core can create additional personalized Beans.

This paragraph analyzes how to use a Bean in the Bean folder. By selecting Bean, the content of the Bean folder is presented in the form of a tree, where every Bean is a node and its child nodes represent its methods.

After selecting the Bean, click Add to insert it into the **Replace With...** frame.

Be sure to insert a semicolon (;) at the end of each line and put the code in order.

Be sure to assign the String parameter a string that makes sense.

The Action folders contain ALL Actions imported into the Package of the selected Rule; in particular, the Action folder contains all Actions imported into the Package that are part of the libraries delivered with the product.

The procedure for inserting Actions (even custom Actions) is exactly the same as that for inserting Beans.

Package Import

This pane includes functions that import and configure rule packages.

From the tabs bar, select **Configure** > **Rules** then click on the **Package Import** accordion pane on the right.

Configuring a Package consists of declaring certain objects available to all Rules in the Package.

Such a declaration consists of specifying an appropriate Java code in the allotted text box.

To make configuration of the Packages easier, insert blocks of predefined code (on the right side of the frame there is a small vertical toolbar with buttons).

The following actions are available for each Package:

- Import specific classes
- Insert variables
- Insert functions

The Rules programmer can write the Rule's code to directly call the objects that are set up for the Package containing the Rule.

Importing a class into a Package adds a class to a Rule without having to specify the entire path.

For example, after importing the class UserBean() into the Package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

Package Editor

An administrator familiar with programming languages can insert any object in the Package by writing the code directly in the text box.

A Package Editor is also available to assist administrators to accomplish this task.

The Editor uses the following buttons, located on the right-hand side of the text box:

- New Import
- New Variable
- (x)= New Function

Variables usually support objects that are already instanced with global visibility to all the Rules of the Package; if, for example, there is an object that contains all the parameters required to connect to the DB, the object can be assigned to an "sql" variable (always visible to the Package's Rules) and can be used in the Rule code, as shown in figure above.

Lastly, it is possible to create Functions that always have global visibility to all the rules of a package. For example, if several rules request an operation for the arithmetic average of two numbers, this can be created directly in the Package instead of in each single rule.

Import a Class

To import a class, click on **New Import** button in the vertical toolbar on the right-hand side of the Package Imports pane.

The Classes window opens (figure below) with a list of available classes

Choose a class, then click **Ok**.

The Java code corresponding to the selected class is written in the text area on the right-hand side of the Replace With... window.

Enter a New Variable

To insert a new variable, click on **New Variable** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Insert the object (specify entire system path) in the space <your class here>.

Insert a variable name in the space <variable name>; this name can then be used in every Rule of the Package.

Enter a New Function

To insert a new function click on (x)= **New Function** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Edit the parameters as follows:

- Replace <return Type> with the type of objects that result from processing the function (e.g. an integer, a string, a class, etc.).
- Replace <args here> with the list of parameters given to the function at input.
- {} needs to contain the body of the function, i.e., all the code that implements the function.

How to schedule a rule sequence

You can link a sequence of rules to a scheduled job.

The Task Planner module is dedicated to scheduling several types of jobs that optimize different tasks in the Identity Governance and Intelligence platform.

After you create a rule flow in Access Governance Core or in other modules, open the upper toolbar and click 🕒.

In Task Planner, select **Manage** > **Jobs** to access the Job Classes GUI.

From the list of **Job Classes**, choose AdvancedRuleFlow or DeferredEventsRuleFlow (depending on what your requirement is) and choose a relevant job from the resulting list.

In the lower frame of the **Details** tab, you find the parameters of the Job Class that you can set with the suitable values.

Monitor

The functions that are available for monitoring some elements are contained in the following list.

- Requests
- Global Statistics

Statistics

This is the default entry point of the Process Designer module.

From this section, you can access:

- Global Statistics
- Requests

Global statistics

The **Global Statistics** web interface is composed by the following panes:

- Activity
- Localization Code
- Process
- Functionality

In some panes, the **Clear** button is available. Select it to remove items from the database.

Requests

The requests web interface is shown below:

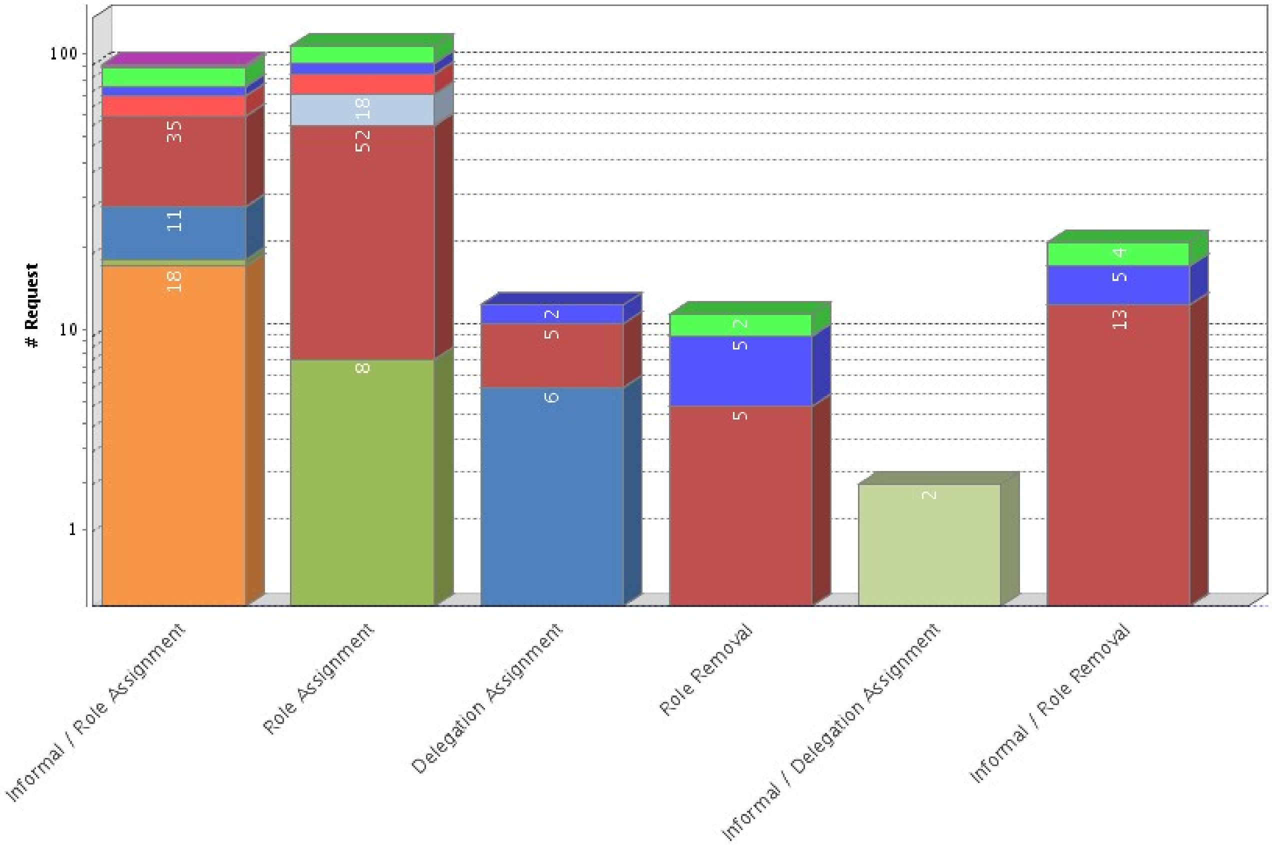


Figure 57. The Requests web interface of Process Designer.

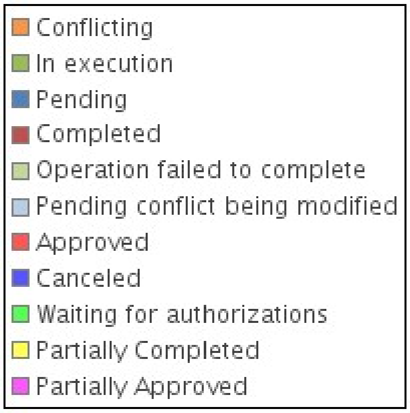
The requests web interface is composed by two axes:

- Request
- Type of request

The Request axis defines the quantity of the requests in an x state.

The Type of request axis defines the type of the requests.

Different colors show the state of the request as described in the legend below:



🟧 Conflicting
🟩 In execution
🟦 Pending
🟥 Completed
🟩 Operation failed to complete
🟦 Pending conflict being modified
🟥 Approved
🟦 Canceled
🟩 Waiting for authorizations
🟨 Partially Completed
🟪 Partially Approved

Figure 58. Colors show the state of request.

Settings

You can use this tab to set up some features of this module.

- "Language management"
- "Entity display"
- Workflow Priority

Language management

In this section, the PD administrator can modify the default language used to load the label groups associated with the various application objects.

The settings described in this section are not related to the language settings of the browser. The browser language affect the labels on the tab bar only.

The **Languages in use (Browser)** text box displays the language that is currently set for the browser.

The **Default Language** text box displays the language that is currently set.

To modify the language, proceed as follows:

1. Click **Change** near the **Default Language** text box.
2. Choose one of the languages from the Default Language window.
3. Click **Ok** to confirm the selected default language.

To add languages to the list of available languages (from right to left), proceed as follows:

1. Select the desired language from the available languages list box on the right.
2. Click ◀ **Add to Table** to move the selected language to the **Languages in use** list box on the left.

To remove a language from the list of languages in use (from left to right), proceed as follows:

1. Select the desired language from the languages in use list box on the left.
2. Click ▶ **Remove Languages** to move the selected language to the **Available languages** list box on the right.

Entity display

For some attributes of some ISIG model entities, it is possible to choose if the attribute will be shown (and in which position) in Access Request processes.

On the left tab **Entities** are listed the model entities available for settings.

Selecting one entity form the list, in the right tab **Entity Fields** you find all related fields.

Ticking the check-box **Visible** you can determine if the field it's shown into the Access Request processes.

Through the arrows **Position** you can determine the relative position of the field.

Configuring the priority and the expiration reminder for WorkFlow processes

Select this tab to set up the priority type and the details of expiration reminders for requests that are defined by processes of type WorkFlow. The reminders are sent to selected users when the requests approach their expiration time and are not yet processed. Here, you define priority levels and their corresponding reminder specifications. You later assign the priority levels when you define the processes.

In this window, match each Priority Level with specifications for the reminders that are sent before each step of a request that is defined by the authorization process expires. For every priority level, you can specify the expiration time for the step of the request and how soon and how frequently reminders are sent before this time. You specify also the notification template, and the recipients of the reminders.

These specifications are applied when you select the Priority in the Reminder pane in the definition of a WorkFlow process. The priority level that is selected in Priority determines when, how often, and to whom a specific reminder is sent as the expiration time is approached.

To set up the priority levels and the related reminder details, take the following steps:

1. Select the **Enable Reminder** check box to enable this feature.
2. Select each priority level - starting from **High** - and define its details in the right pane.

Table 186. Details for priority levels

Detail	Description
Expiration	Specify after how many hours or days the step of the request reaches its expiration time after its submission. For the High priority level, this period is shorter than the ones for the other levels. The Unassigned priority level implies that no expiration time and no reminder policy are wanted. The default value for each priority level is next. **High** 5 days **Medium** 10 days **Low** 10 days **Unassigned** -1 day

Table 186. Details for priority levels (continued)

Detail	Description
Reminder Schedule	Specify the time - in hours or days - that a first reminder is sent before the expiration time, and the frequency that other reminders are sent before the request expires. The default values for each priority level are next. **High** **Start Before Expire** 3 days **Frequency** 1 day **Medium** **Start Before Expire** 3 days **Frequency** 1 day **Low** **Start Before Expire** 5 days **Frequency** 2 days **Unassigned** **Start Before Expire** -1 day **Frequency** -1 day
Reminder Template	Select the template that is to be used to assemble the notification text and the placeholder keys for the reminders that are associated with the priority level. The template must be of type Reminder and must be already defined.

Table 186. Details for priority levels (continued)

Detail	Description
Email Recipients	If the reminders are sent by email, select the recipients. Flag one or more types of recipients. **Requested For** Send the email to the beneficiary of the request. **Requested By** Send the email to the generator of the request. **Approvers** Send the email to the approvers involved into the process. **Fixed Addresses** Send the email to other users. Specify the email addresses, separating them with semicolons, in the related field. For each type, select if the recipient is direct, carbon copy, or blind carbon copy. Select **Preview** to display a preview of the email.
SMS Recipients	If the reminders are sent by SMS, select the recipients. Flag one or more types of recipients. **Requested For** Send the SMS message to the beneficiary of the request. **Requested By** Send the SMS message to the generator of the request. **Approvers** Send the SMS message to the approvers involved into the process. **Fixed Phone Numbers** Send the SMS message to other users. Specify the mobile telephone numbers, separating them with semicolons, in the related field. Select **Preview** to display a preview of the SMS message.

Chapter 24. Introduction to Enterprise Connectors

Enterprise Connectors (ERC) is the module delegated to achieve the alignment between the centralized database of IBM Security Identity Governance and Intelligence and the peripheral target systems.

A generic organization decides to adopt IBM Security Identity Governance and Intelligence after experiencing the difficulties found in managing different and heterogeneous IAM systems, layered over time, sometimes without a clear vision of the integration issues.

Usually, the final result of a “patchwork strategy”, is a multi-repository system that stores the authorization attributes of the organization, based on different data models and approaches, with different authorization systems that cannot be easily interfaced.

During the transition phase from an existing (and often chaotic) authorization model to an RBAC model such as IBM Security Identity Governance and Intelligence, it is not possible to abruptly switch off all the other existing IAM systems and to use only the AG Core centralized repository.

Ensuring business continuity is always a priority for large organizations but, during the transition phase to Identity Governance and Intelligence, this requires additional effort since:

- The Identity Governance and Intelligence platform must be integrated with the current layout of the enterprise.
- Tuning and customization activities are possibly needed.
- Staff needs to be trained on the features and characteristics of Identity Governance and Intelligence.

During the transition phase it is important that the following objectives be harmonized:

- Granting the normal behavior of all the business activities of the organization, maintaining all the preexisting IAM systems (targets) active.
- Updating the AG Core centralized repository of Identity Governance and Intelligence and keeping it aligned with the peripheral target systems.

Also after the transition phase is over, when all authorization issues are filtered and managed by the AG Core centralized repository, it may be necessary to maintain a relevant number of target systems active. This is the most common situation, when more than one target system is linked to the AG Core of Identity Governance and Intelligence.

Enterprise Connectors (ERC) is the module of the IBM Security Identity Governance and Intelligence platform that answers the following concerns:

- Synchronizing the AG Core repository with a target system when on the target system identity attributes are modified.
- Replicating on a target system changes that were made in the AG Core repository.

A connector *connects* the AG Core centralized repository with a particular IAM system, so that identity governance data can be imported and kept synchronized. In particular, the ERC module provides a set of functions that enable an administrator to:

- Define a connector
- Define a connector's channel mode
- Define the configuration rules for a specific connector
- Start and stop a connector, either manually or by schedule

The Identity Governance and Intelligence ERC model

The Integration Interface (II) of Identity Governance and Intelligence provides an efficient way to connect the AG Core module with a wide range of external target systems.

The figure below displays the structure of II:

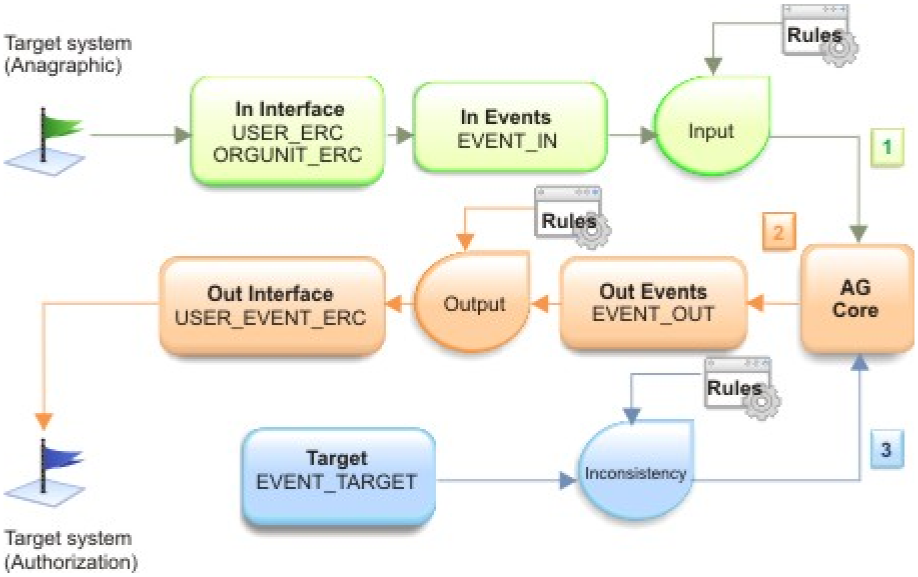


Figure 59. The structure of the Integration Interface.

The ERC module is the logical layer that is positioned between the target systems and II, as displayed below:

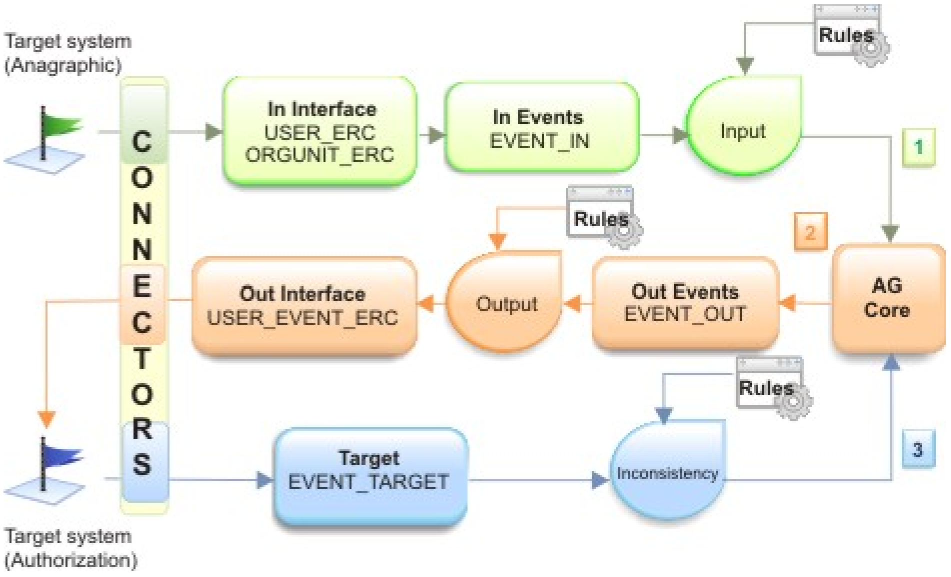


Figure 60. The ERC layer.

In the figure above, you can easily distinguish three different logical channels colored in light green (**Read From** channel), light orange (**Write To** channel) and light blue (**Reconciliation** channel).

The standard structure of a connector block is displayed below:

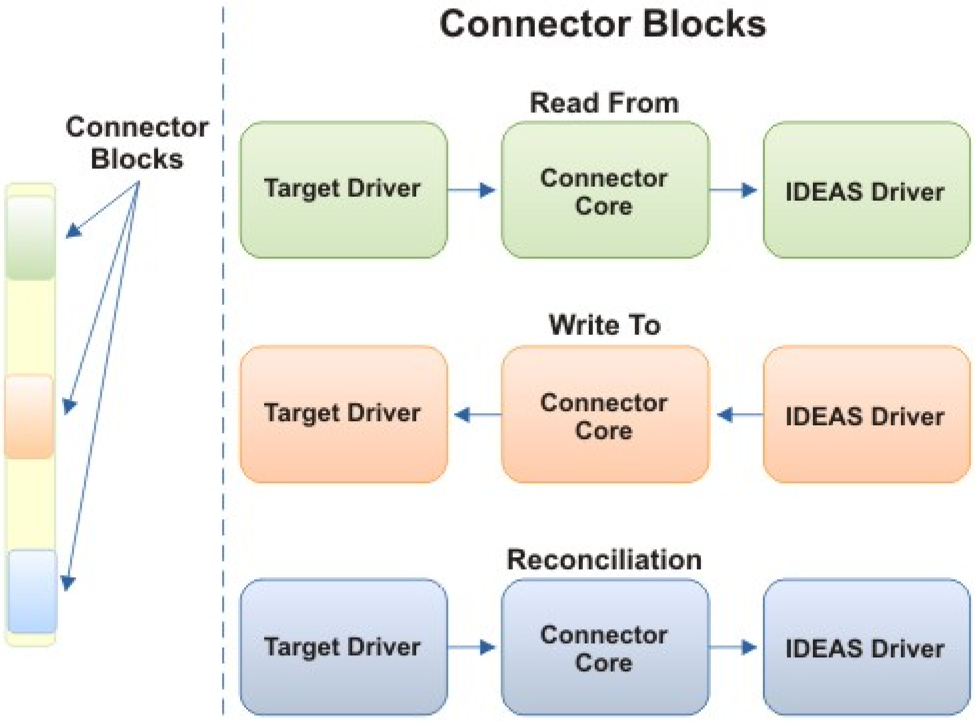


Figure 61. The general structure of a connector block.

A connector consists of three basic blocks:

- Target driver

- Connector core
- Identity Governance and Intelligence (IDEAS) driver

The target driver is the boundary element between Identity Governance and Intelligence and the external targets.

This block hosts all configurations settings needed to communicate with a specific target system.

The connector core block hosts the connector engine, mainly characterized by a set of rules.

The Identity Governance and Intelligence (IDEAS) driver is the interface between the connector core and the II.

Channel mode of the connector

For any connector, you must define at least one channel mode.

It is possible, however, to define a connector that operates in every channel mode. The channel modes are:

- Write to
- Read from
- Reconciliation

Write to

This channel option allows you to propagate to a generic target system every change registered into the AG Core repository. The logical workflow of this channel mode is displayed below:

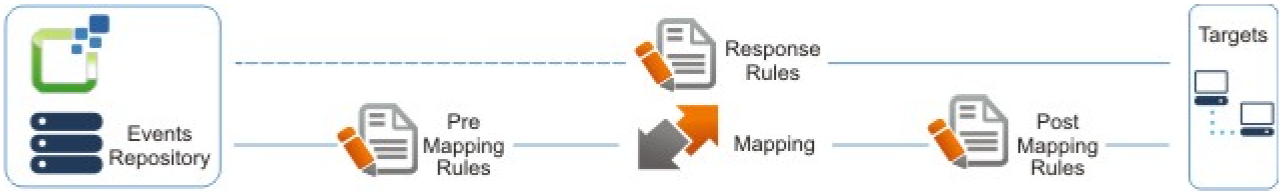


Figure 62. The logical workflow of the `Write to` channel mode.

Read from

This channel option allows you to read the input events and user data coming from the generic target system. The logical workflow of this channel mode is displayed below:

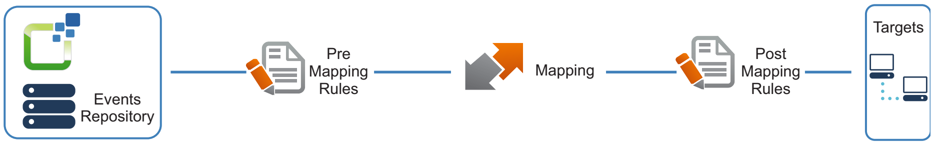


Figure 63. The logical workflow of the `Read from` channel mode.

Reconciliation

This channel option allows you to realign the data changed in a generic target system with the data registered into the AG Core repository. The logical workflow of this channel mode is displayed below:

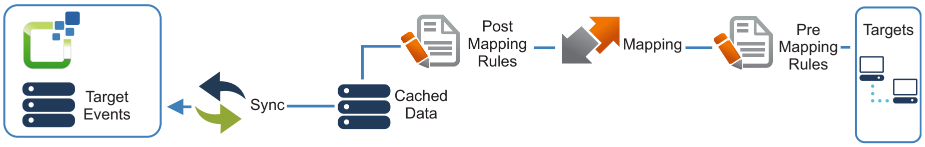


Figure 64. The logical workflow of the `Reconciliation` *channel mode.*

Building a connector

A short roadmap to build a connector is provided.

You can build a connector using the ECONN module with only four basic steps:

1. Configure a driver.
2. Link the connector to the driver configured in step 1.
3. Choose one or more channel modes for the connector, according to step 2.
4. Set the appropriate mapping for the connector.

Driver configuration

In the ERC model, there are two types of drivers:

Target driver
Is the boundary element between IBM Security Identity Governance and the external environment, and is part of a connector block.

IBM Security Identity Governance driver
Is the boundary element between a generic connector block and the IBM Security Identity Governance II.

IBM Security Identity Governance driver is a built-in default driver ECONN module. For the IBM Security Identity Governance driver, no configuration activities are needed.

A generic target driver must be accurately configured:

- To get data from an external target system (Read from channel).
- To send data to an external target system (Write to channel).

ECONN allows the management of a multi-target driver.

A driver is identified by three sets of data:

- Driver details
- Driver properties
- Driver attributes

Multi-target driver

This option is very useful in very common situation, when is present a specific type of target system (for example, Active Directory) and several instances of AD, possibly running on workstations.

In this case, the driver configuration is characterized by:

- A set of common data that can be shared among all instances.
- A reduced subset of data related to the specific instance (for example, the IP address or the SSL certificate).

In this situation, it can be useful to specify the driver common data once and to clone it for several instances. Therefore, for every instance will be easy to specify only the specific data subset for the specific instance.

The logical structure of a multi-target driver is displayed below:

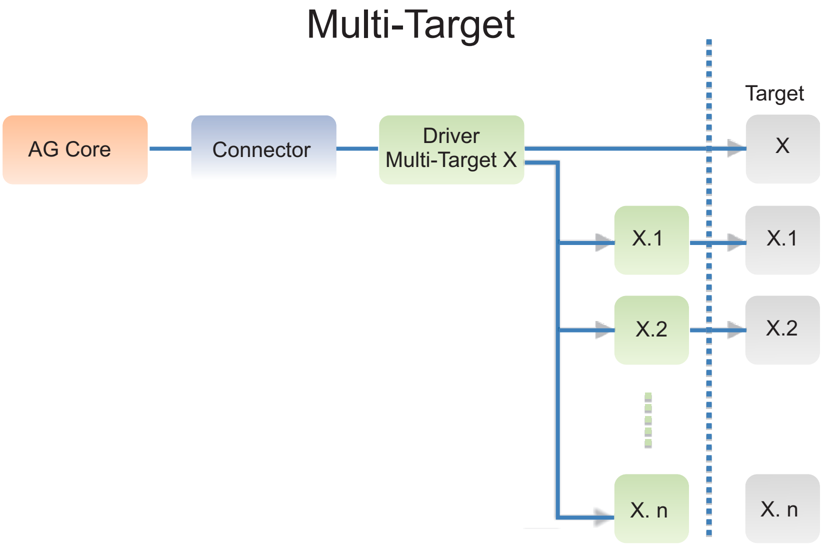


Figure 65. General structure of a multi-target driver.

Adding a new connector

To add a new connector means, basically, to link a connector module to a specific driver. This operation allows you to establish the real implementation of a communication channel between a target system and IBM Security Identity Governance II (see The IBM Security Identity Governance Connector model).

For details about the actions needed, see "Manage connectors" on page 420.

Connectors

You can configure all the characteristics of the connectors that are needed for exchange data with target systems.

The Connectors frame, contains the list of inventoried connectors.

The following filters can be used for connector search (click **Filter/Hide Filter**):

Table 187. Connector filters.

Filter	Description
Name	Name of the connector.
Enabled	✓ enabled or disabled connector.

The following **Actions** are available:

- **Import** provides to import a Connector from an XML files format.
- **Export** provides to export a Connector in XML files format.
- **Add** provides to add a Connector.
- **Remove** provides to delete a Connector.

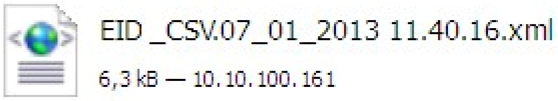
The connectors frame lists the results, according to the following attributes:

Table 188. Connectors attributes.

Attribute	Description
Enabled	✓ for a connector enabled. ✗ for a connector not enabled.
Name	Connector name.
Driver	Name of the driver that is associated to the connector.
Connector/Reconciliation	Presence of active status • **Connector**: the Connector is running. • **Reconciliation**: the Connector is running in reconciliation mode. Presence of inactive status • **Connector**: the Connector is stopped. • **Reconciliation**: the Connector is stopped in reconciliation mode.

You can click the **Import** to import connectors in the XML file format.

The XML file name format is *`ConnectorName.dd_mm_yyyy hh.mm.ss`*`.xml`:



EID _CSV.07_01_2013 11.40.16.xml

6,3 kB — 10.10.100.161

Figure 66. The import XML file name of a Connector.

Note: If an imported connector has the same name as an existing one, a Warning window appears, displaying a diagnostic message.

Attempting to import a file that is not in XML format generates a Warning window, which displays a diagnostic message about the outcome of the operation.

After a connector is selected in the left frame, the **Connector Details** tab (right) shows the related data:

Table 189. Connector details.

Detail	Description
Name	Name of the connector.
Description	Description of the connector.
Driver	Name of the associated driver.
Enabled	Enable or disable the connector.
Channel Mode	Type of active channel. The Reconciliation Channel is always active.
Polling Group	Label of the polling group that is associated to one or more connectors.
Trace ON	If this check box is flagged, the log of the selected Connector is written into a specific file (Connector name.log).
Trace Level	From this text box is possible to choose between three levels of logs • INFO • DEBUG • ERROR

After the selection of a connector in the left frame, edit all needed information and click **Save** to validate the changes.

The Connector Properties frame displays the properties of the connector:

Table 190. Connector properties.

Property	Description
Property Name	Name of the Connector property.
Property Value	Value of the Connector property.
Property Description	Description of the property.

In this frame, you can add a property by clicking the **Add** button and setting the **Property Name** and the **Property Value** in a dedicated window (for removal, click the **Remove**).

Note: You can disable this type of mapping by setting the value of the **`disableMapping`** property to `TRUE`.
CAUTION:
The removal of one or more properties, can lead to possible malfunctions in the functioning of the Connector.

Each Connector can have one or more configured Channels. The display of one or more Channels tabs depends on the configuration of the selected Connector.

Manage connectors

Use this tab to define and manage connectors, their driver, and channel mode.

The Connectors frame on the left displays a list of defined connectors. You can select the **Filter** button and enter the following information to refine the list of connectors or to find specific ones:

Table 191. Available filters to search connectors

Filter	Description
Name	The name of the connector
Enabled	**Yes** The connector is enabled **No** The connector is not enabled

The list of connectors shows a connector name and:

- Whether the connector is enabled (✓) or not (blank). An enabled connector is ready to run.
- The channel mode of the connector. A channel is the logical representation of the communication path that can be established between the AG Core module (through an annexed connector) and a generic target system. There are three channel modes, represented as:

  WTO Write to: Used to send data from the AG Core repository to a target.

  RFROM
  Read from: Used to import data from a target to the AG Core repository.

  RECON
  Reconciliation: Used to re-align data that for some reason was changed in a target system with the data recorded in the AG Core repository.

  A connector can operate in any or all of these modes, depending also on its type. The channel modes enabled for a connector are marked by the ✓ icon.

You can click the **Actions** button to select any of the following:

Add To add a new connector implies linking a connector module to a specific driver. This operation results in the implementation of a communication channel between a target system and IBM Security Identity Governance and Intelligence.

The **Channel Mode** check boxes are not displayed the first time you define the details of a new connector. You must first save the new connector.

Remove
Deletes a selected connector definition

Import
Imports a connector definition as an XML file.

The XML file name format is:

`*ConnectorName.dd_mm_yyyy hh.mm.ss*.xml`

Export Exports a selected connector definition as an XML file.

The XML file name format is:

`*ConnectorName.dd_mm_yyyy hh.mm.ss*.xml`

When you select a connector in the list, the **Connector Details** frame on the right shows the following connector properties:

Table 192. Connector details

Detail	Description
Enabled	When checked, it shows that the connector is ready to run.

Table 192. Connector details (continued)

Detail	Description
Channel Mode	A checkbox is displayed for every channel mode available. There can be up to three channel modes, depending on the type of connector. A check mark indicates that the connector is ready to run in the specific channel mode. All channel modes can be enabled concurrently.
Name	The name of the connector.
Description	An optional description that states the function of the connector.
Type	The connector type. The following connector types are ready for use: Active Directory, CSV, IDEAS, JBDC, LDAP, SAPHR, SAPR3, Unix, WorkGroup, XLS, XML.
Driver Class	The name of the associated driver, based on the connector type.
Trace ON	When this check box is flagged, the connector is traced and logged in the `*connnector_name*.log` file.
Trace Level	This text box is enabled when you flag the `Trace ON` checkbox. Choose one of these trace levels: **INFO** Records informational messages that highlight the progress of the application at coarse-grained level. **DEBUG** Records fine-grained informational events that are most useful to debug an application. **ERROR** Records error events that might still allow the application to continue running.
History ON	Flag this checkbox to save usage history of this connector.

The **Global Config** accordion pane lists a number of connector properties that apply to all connectors, independently of their type. These properties are shown with their default values. You can change these values, or use the **Actions** button to remove any of them or to add new ones, making sure that none of these changes upset the performance of the connector.

Table 193. Global configuration properties for connectors.

Property Name	Default Value	Description
rightNameValueSeparator	=	The character used for separating a name and its corresponding value in
reconciliationCode	1	A counter that is updated by the system each time reconciliation takes place. You can reset the number to a value of your preference.

Table 193. Global configuration properties for connectors. (continued)

Property Name	Default Value	Description
ModifyToAdd	true	During the reconciliation process, adds a record in the database in lieu of modifying it as done in the target. For example, if a record was modified in the target, but the record is not found in the AGC database, the record is created in the database. If the value is set to `false`, an error is logged when the record is not found.
disableMapping	false	Change to `true` to disable the mapping of connector object class fields.
Manage Event Target on error	false	Change to `true` to be able to manually handle error events generated by the target.

After the selection of a connector in the left frame, edit all needed information and click **Save** to validate the changes.

To complete or view all connector-related information, continue to the following tabs:

- Driver Configuration
- Driver Attributes List
- Tabs corresponding to the enabled channels (Read From, Write To, or Reconciliation)

Driver configuration

Enter in this panel the properties of the driver that the connector runs on.

The properties differ according to the type of driver, but they generally specify information such as:

- Details for connecting with the target
- Identification data
- Details on the format used to send and receive data

This panel includes the following accordion panes:

Driver Lists the properties of the driver that runs the connector selected in the left fame.

Fanout
If you have more than one instance of the target system, this is where you can specify driver properties for the additional instances.

These panes are described next.

Driver

This pane is displayed in `Browse` mode when you select the Driver Configuration tab, unless you are defining a new connector. Click **Edit** if you need to update values.

The Driver pane collects the following information:

Events Marker
This dropdown list shows the event marker selected for this driver. An event marker represents the target system linked by this driver (and connector) as the sender or recipient of events to or from Identity Governance and Intelligence. Event markers are defined in the **Manage** > **Account** panel of the Access Governance Core module. Each marker is closely associated to the account linked with an application. With an exception for the IDEAS event marker, an event marker cannot be associated with more than one driver.

When you access this pane in `Edit` mode, click the arrow to list the available markers.

Driver Properties frame
Displays a list of driver properties as shown in the following table. The properties shown are specific to each type of driver.

Table 194. Driver properties

Name	Description
Mandatory	If the ✓ icon is shown, you are required to provide a value for the property in the row.
Name	The name of the property.
Value	A working value for the property.
Description	Position your mouse on the ⓘ icon so that a tooltip displays a description of the requested value.

The following buttons enable you to specific actions:

Reset Resets the driver cache. Select it to delete the hash file of the driver. This action can be run only on drivers that do not use a trigger.

Conn. Checks the state of the connection configured for the driver.

Query Checks the driver query values.

Dump Applies to drivers used in Reconciliation mode. An operating system window is opened to save the file created with the values of the Reconciliation process.

Fanout

Expand this pane to configure properties for additional instances of the target addressed by this driver and connector.

This option is useful to address multiple instances of a target system (for example, Active Directory) that run on different computers. In this case, the driver configuration is characterized by a set of common data that can be shared for all instances and by a subset of data related to the specific instance (for example, the IP address or SSL certificate). This pane is where you specify the data subset for the specific instances.

To specify the properties for additional target instances, click **Actions** and select **Add**. The following items appear in the attached table:

Table 195. Adding targets

Event Marker	Enabled	Operations	Properties
The events marker associated with the target instance.	Click to enable the driver to run for the target instance.	The same operations available in the Driver pane.	Click **Conf.** to display the **Driver properties** window. This is similar to the Driver Properties frame in the Driver pane and specific to the instance.

Click **Actions** > **Save** when you are finished. You can add as many rows as there are instances.

To remove the driver configuration of a particular target instance, flag the associated checkbox and select **Actions** > **Remove**.

Driver Attributes List

In this panel you enter the Object Class nodes and Object Class Field nodes that you will later map within the channel modes of the connector.

Object Class nodes and Object Class Field nodes make up the structure in which information, such as user names, roles, groups, accounts, passwords, and any other type of data used in your security model is mapped in the model. An Object Class node contains several Object Class Field nodes and every node displays its fields in a tree structure in this pane.

The IDEAS driver already comes with its own list of attributes, but you can define additional attributes to this driver as well as to all the other drivers that you use. You can also edit and remove these attributes to comply with the changes of your security model.

With a connector selected in the left pane, you can click **Actions** > **Add** to add:

- A New Object Class node
- An Object Class Field node

If you click **Add** with nothing selected in the Driver Attributes List panel, you are shown the `Add node` window with the following fields:

Table 196. New Object Class node attributes.

Name	Description
Name	The name of the Object Class node
Description	A description of the Object Class node

If you click **Add** with a selected Object Class node, the `Add node` window gives you the choice of specifying the attributes of another Object Class node or those of a field of the selected node (`Add Object Class Field node to` *`node_name`*). If you opt for adding an Object Class Field node, the attributes you must specify are:

Table 197. Object Class Field node attributes.

Name	Description
Name	The name of the Object Class Field node
Description	A description of the Object Class Field node
Type	Click the arrow to display a list of Java data codes to choose from
Multivalued	Flag this check box if the field will have more than one value

The Object Class Field nodes are added as hierarchy leafs to the Object Class node. You can add as many field nodes to an Object Class node as required. Ultimately, each Object Class node is displayed with all its field nodes in a tree structure.

If you click **Actions** > **Automatic Add** for a selected Object Class node, depending on the driver configuration the Object Class Field nodes are added based on the driver properties.

To edit or remove an Object Class node or an Object Class Field node, select the object and click the appropriate item in the **Actions** menu.

Remember: Before you modify the Type of an Object Class Field node, verify that the new value is compatible with the mapped value in the **Connectors** > **Channels** > **Mapping** button.

Channels and Rules

This is where you map the Object Class fields stored in the AG Core repository of Identity Governance and Intelligence with those of the target system. It is also where you define and manage rules that make adjustments to the data exchanged between the two parties to adapt it to the data layout of each system.

After selecting a connector (left), you can click on the related channel tabs on the right:

Channel-Write To
Propagates every change registered into the AG Core repository to the target system.

Channel-Read From
Reads the events and user data arriving from the target system and bound for the AG Core repository.

Channel-Reconciliation
Realigns the data changed (for various reasons) in the target system and the data recorded in the AG Core repository.

Important: Each connector can have one or more configured channels. The display of one or more Channel tabs depends on the configuration of the selected connector (driver).

Every channel is provided with an infographic made up by icons that you select to take specific actions:

- Events Queue: available for every channel (Write To, Read From, and Reconciliation).

- Pre Mapping Rules: available for every channel.
- Mapping: available for every channel.
- Post Mapping Rules: available for every channel.
- Response Rules: available only for the Write To channel.
- Target: available for every channel.
- Sync.: available only for the Reconciliation channel.
- Cache: available only for the Reconciliation channel.

The infographic provided for every channel suggests the logical workflow of the channel.

Events Queue

Click the**Events Queue** icon, to view the list of authorization events that transited through your selected connector. The following window opens, depending on the channel mode:

Target Events Queue
For Read From and Reconciliation channels

IDEAS Out Events
For Write To channels

The window displays all or some of the following fields, depending on the driver configuration:

Table 198. Event fields

Field	Description	Events Queue window	
		IDEAS Out Events (WTO)	**Target Events Queue (RFROM and RECON)**
ID	Event identifier.	x	
Account ID	The identifier of the account associated with the application impacted by the event.		x
Application	The name of the application impacted by the event.	x	
Operation Cod	Operation identifier.	x	
Operation	Indicates the type of operation made.	x	x
Target	The name of the target system to which the outbound event is directed.	x	
Status	The state of the event. It can be one of the following: • Unprocessed • Success • Error	x	x
User ID	The identifier of the user affected by the event.	x	
Trace	A description of the error.		x

Table 198. Event fields (continued)

Field	Description	Events Queue window	
		IDEAS Out Events (WTO)	Target Events Queue (RFROM and RECON)
Event Marker	The marker of the event. It may coincide with the identifier of the target system.		x
Permission	Indicates the assigned/removed permission.		x
Permission Type	Indicates the type of assigned/removed permission.		x
Free Attribute 1	Sensitive data 1.	x	x
Free Attribute 2	Sensitive data 2.	x	x
...	...	x	x
Free Attribute N	Sensitive data N.	x	x
Event Date or **Date Event**	Indicates the event generation date.	x	x
Process Date	Indicates the date in which the event must be processed by the RE (generally coincides with the event date but can be subsequent if the event processing was postponed).		x
Ownership	Indicates the user who caused the event on the external table.		x

Click **Ok** to close the window.

Pre Mapping and Post Mapping Rules

Pre Mapping Rules are used to prepare data inbound from a target driver (in the Read From and Reconciliation channels) or outbound from the Identity Governance and Intelligence driver (in the Write To channel) for the application of the Mapping process. For example, you write a pre mapping rule for the Write To channel that changes an event or sets a particular value for it and then writes on the log the content of the event.

Conversely, Post Mapping Rules are used to adjust data, after the completion of the Mapping process, before it is stored in the AG Core repository of Identity Governance and Intelligence (Read From and Reconciliation channels) or sent to the target driver (Write To channel).

Select the**Pre Mapping Rules** and **Post Mapping Rules** icons to specify actions on data or events before and after the Mapping process takes place. As you do so, the icon you selected is highlighted and the following panes are displayed below:

- The pane on the left contains a **Run** tab that lists one or more packages of rules charted in a tree structure. The rules are either imported from another Identity Governance and Intelligence module or created within the Rules Package on the right.

  The pane includes an Actions button with the following items:

Table 199. Rule Package Actions

Action	Description
Import	Imports a rule class or rule flow previously exported from Access Governance Core or Process Designer. Opens the Import Rule Class/Flow window where you choose the item to import and select the rules file with the help of a `Browse` option.
Export	Not used.
Modify	Not used.
Enable/Disable	Not used.
Up	Moves the selected rule one place up in the rule package tree.
Down	Moves the selected rule one place down in the rule package tree.
Remove	Removes the selected rule from the package tree.

- The Rules Package accordion pane on the right lists the rules defined within the pane with the help of the “Rules” on page 253.

  The pane includes an Actions button with the following items:

Table 200. Rules Package pane Actions

Action	Description
Verify	Checks the integrity of the rules listed in the pane.
Modify	Opens the selected rule for editing in the “Rules” on page 253.
Delete	Removes the selected rule from the pane.
Create	Opens the “Rules” on page 253 for the definition of a rule.
Cr. Def	Not used.
Add	Adds a selected rule to the tree structure of a selected package in the left pane.

- The Package Imports accordion pane, also on the right, contains the Java code of the rules package selected in the left pane.

  The Java code is shown in the “Package Editor” on page 258 text box, where you can edit the Java code to change the configuration of the rules package.

  Configuring a package consists in declaring certain objects and making them available to all the rules of the package. This is accomplished by specifying the appropriate Java code in the allotted text box.

  The “Package Editor” on page 258 assists you in changing the Java code by enabling you to add blocks of predefined code. These blocks are made available by three buttons located on the right-hand side of the text box. The buttons start the following actions:

  New Import
  Imports a rule class selected from a list. Importing a class in a package adds a class to a rule without having to specify the entire path. For example, after importing the class UserBean() into the package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

  New Variable
  Adds a variable block at the end of the code.

  New Function
  Adds a function block at the end of the code.

More helpful information about rule building is described in the Rule Classes section **AGC** > **Configure** > **Rules**.

Mapping

In this part of the infographic, you map the Object Class fields of Identity Governance and Intelligence with those of the target system.

Click the **Mapping** icon in the infographic displayed for your selected channel to view the two panes with the Object Class fields you want to map. The IDEAS pane lists the Object Class fields of the particular authorization event on Identity Governance and Intelligence, while the TARGET pane lists those on the target system. The panes vary depending on the channel mode:

- In the Write To channel mode, the Object Class fields of TARGET (**Operation** = Source) are mapped on the ones of IDEAS (**Operation** = Destination).
- In the Read from and Reconciliation channel modes, the Object Class fields of IDEAS (**Operation** = Source) are mapped on the ones of TARGET (**Operation** = Destination).

The pane where **Operation** equals Source shows the following columns:

Table 201. Mapping pane columns when Operation = Source.

Column	Description
Field	The name of the Object Class field mapped to the fields of the **Operation** = Destination pane. The fields can be selected individually by flagging the nearby checkbox or globally by flagging the checkbox next to **Field**.
Operation	Source
Type	Can be: • Mapped • Not Mapped Mapped fields are placed on top of the list.
Value	If **Type** = Not Mapped, it is blank. Otherwise, it is the name of the Object Class field on the counterpart that this field is mapped to: • For an Identity Governance and Intelligence field mapped to a target field, **Value** is the name of the target field preceded by the name of the driver. • For a target field mapped to a Identity Governance and Intelligence field, **Value** is the name of the Identity Governance and Intelligence field preceded by the Object Class name.

Table 201. Mapping pane columns when Operation = Source. (continued)

Column	Description
Key	The ✓ icon displayed next to one of the fields shows that the field is used as the matching key for the mapping process. This matching enables an event to check that the current object exists on the application target, according to the relation defined between Object Class Fields and Value.

In this pane click **Actions** to do any of the following:

Set Key
Makes a flagged field the matching key for the mapping process.

Change Map
Displays a list of defined Object Class Nodes where you choose the node whose fields you want to use for mapping.

Custom Map
Opens a window where you can enter a constant value or variable attribute field as the **Value** of a selected field.

Reset Resets the flagged fields to the Not Mapped **Type**.

The pane where **Operation** equals Destination shows the following columns:

Table 202. Mapping pane columns when Operation = Destination.

Column	Description
Operation	Destination
Name	The name of the Object Class field mapped upon by one of the fields of the **Operation** = Source pane.
Type	The Java data code of the Object Class field. For example, `java.lang.String`.
Multi	The ✓ icon displayed next to a name shows that the field can have more than one value.

To map a field:

1. Click the **Source** button next to the field that you want to map.
2. In the adjacent pane, click the **Destination** button next to the field that you want to match.

As a result, the attributes of the mapped fields will populate the corresponding fields whenever an exchange of data occurs between Identity Governance and Intelligence and the target system.

Response Rules

This step is similar to the one described in Pre/Post Mapping Rules.

The Response Rules section shows the outcome of the action run on the target. It enables you to view the status of the target following the completion of that particular action.

To learn the result of an operation, you need a rule that handles the results of the procedure. This type of rule helps you control the objects addressed by the rule.

Select **Actions** > **Create** in the Rules Package accordion pane to define rules that enable you to learn the results of operations.

To learn more about how to build rules, see **AGC** > **Configure** > **Rules**.

Target

Click this icon to view information about the target driver. This information is also available when you click **driver Configuration** on a selected connector.

Synchronize (Sync.)

This icon, available only in the **Channel-Reconciliation** tab, is currently not active.

Cache

Click the **Cache** icon to view the data used for the Reconciliation process and read by the target.

Use any of the following filters (after selecting **Filter**) to find a target cache:

Table 203. Target Cache filters

Filter	Description
Account	Account ID on Identity Governance and Intelligence.
Permission	The name of the permission of the account.
Status	Flag this checkbox to search for inactive target caches only.

The target caches are listed in the **Target Cache** tab. The primary target cache attributes displayed are:

Table 204. Main Target Cache attributes

Attribute	Description
Account	The user ID on Identity Governance and Intelligence.
Permission	The name of the permission of the account.
Events Marker	The events marker associated with the target.
Load Date	The data loading date.
Status	✓ : the account is active. ✗ : the account is not active.

Monitor

The functions that are available for monitoring some elements are contained in the following list.

- Connector Status
- Reconciliation Status

Connectors status

This section enables you to start, stop, and schedule your defined connectors.

The Connector Status pane contains the list of inventoried connectors and filters for the connectors search (click **Filter/Hide Filter**), as summarized in the table below:

Table 205. Connector filters

Filter	Description
Name	The name of the connector.
Active	**Yes** The connector is currently active. **No** The connector is not currently active.

The results produced are characterized by the attributes summarized in the table below:

Table 206. Connector attributes

Attribute	Description
Active	**Local/External Scheduling** The connector is running in Local/External scheduling. **Stopped** The connector is stopped.
Name	The name of the connector.
WTO	If the ✓ icon is shown, the `Write to` channel is enabled.
RFROM	If the ✓ icon is shown, the `Read from` channel is enabled.
Status	The available status for the connectors are: **Running** The connector is running. **Pending** The connector is waiting to be started. **Error** There was an error while the connector was running **Stopped** The connector is stopped.
Last Run / Start	The last start date of the connector (*dd-Month-yyyy*; *hh*:*mm*:*ss*).

To start or stop a connector, select the connector and click **Start** or **Stop** in the **Actions** menu.

The **Connector Status Details** tab includes the following boxes:

Details

Shows the following information:

Table 207. Details box attributes.

Attribute	Description
Name	Th name of the connector.
Description	A description of the connector.
Message	The message that you want to be displayed when an error occurs in the execution.
Last Run/Start	The last start date of the connector (*dd-Month-yyyy*; *hh*:*mm*:*ss*)
Last Run/Elapsed	The elapsed time of execution (*hh*:*mm*:*ss*.).

Scheduling

Is where you enter the following information if you want to schedule connector runs:

Table 208. Scheduling box attributes

Attribute	Description
Local Scheduling/ External Scheduling	Selecting the **Local Scheduling** radio button, the runs are scheduled from the **Connector Status** tab. Selecting the **External Scheduling** radio button, the runs are scheduled from the Task Planner module and all the options that follow become unavailable in this pane.
Frequency	Use this combo box to set the frequency of the connector runs.
Immediately	Select this check box to start the connector immediately. This selection overrides any date you specify in the field below.
Date	Select the date (*dd*/*mm*/*yyyy*) and time (*hh*:*mm*) of the connector start.

You can edit the content of these boxes, thus click **Save** to confirm your updates.

The **Connector History** tab is where you can view a history of the outcomes of the past runs of a selected connector, based on the channel mode.

You can enter the following information to filter your search for past runs:

Table 209. Connector History filters

Filter	Description
Start Date from	Shows all runs started from this date onwards.
Start Date to	Shows all runs started until this date.
Result	Can be: • Blank (all) • Completed • Error

The list of connector runs in Reconciliation mode is shown in the following columns:

Table 210. Connector History attributes

Attribute	Description
Channel Mode	Can be `Write to` or `Read from`.
Result	Completed or Error.
Message	The message displayed in the **Message** text box.
Start Date	The starting date and time the connector run started.
Elapsed Time	The completion (if successful) or ending (if in error) time of the run.

To delete a particular run history line from the list, select the line and click **Actions** > **Remove**. To delete all run histories, click **Actions** > **Remove All**.

Reconciliation status

This section enables you to start and schedule connectors in Reconciliation mode.

The Reconciliation Status pane contains the list of inventoried connectors and filters for the connectors search (click **Filter/Hide Filter**), as summarized in the table below:

Table 211. Connector filters

Filter	Description
Name	The name of the connector.
Active	**Yes** The connector is currently active. **No** The connector is not currently active.

The results produced are characterized by the attributes summarized in the table below:

Table 212. Connector attributes

Attribute	Description
Active	**Local/External Scheduling** The connector is running in Local/External scheduling. **Stopped** The connector is stopped.
Name	The name of the connector.
Status	The available status for the connectors are: **Running** The connector is running. **Pending** The connector is waiting to be started. **Error** There was an error while the connector was running **Stopped** The connector is stopped.
Last Run / Start	The last start date of the connector (*dd-Month-yyyy; hh*:*mm*:*ss*).

To start or stop a connector, select the connector and click **Start** or **Stop** in the **Actions** menu.

The **Reconciliation Status Details** tab includes the following boxes:

Details

Shows the following information:

Table 213. Details box attributes.

Attribute	Description
Name	Th name of the connector.
Description	A description of the connector.
Message	The message that you want to be displayed when an error occurs in the execution.
Last Run/Start	The last start date of the connector (*dd-Month-yyyy*; *hh*:*mm*:*ss*)
Last Run/Elapsed	The elapsed time of execution (*hh*:*mm*:*ss*.).

Scheduling

Is where you enter the following information if you want to schedule connector runs:

Table 214. Scheduling box attributes

Attribute	Description
Local Scheduling/ External Scheduling	Selecting the **Local Scheduling** radio button, the runs are scheduled from the **Connector Status** tab. Selecting the **External Scheduling** radio button, the runs are scheduled from the Task Planner module and all the options that follow become unavailable in this pane.
Frequency	Use this combo box to set the frequency of the connector runs.
Immediately	Select this check box to start the connector immediately. This selection overrides any date you specify in the field below.
Date	Select the date (*dd*/*mm*/*yyyy*) and time (*hh*:*mm*) of the connector start.

Advanced Settings

Is where you specify the following advanced settings for local scheduling:

Table 215. Advanced Settings box attributes

Attribute	Description
Mode	Select one of the following: **Synchronization** Generates a short report and places it in the **Message** text box. In addition, the detailed list of associated events can be viewed in one of these places: • By selecting **Manage** > **Connectors** > **Channel-Reconciliation** > **Events Queue** after selecting the connector. • By going to **AGCore** > **Monitor** > **Target Queue**. **Simulation** Generates the report and places it in the **Message** text box.
Used Data	Select one of the following actions on the cached data after it is processed: **Refresh from Target** Processed data is deleted from the cache table of the connectors and reloaded from the target. **Cached data** Processed data is maintained.

You can edit the content of these boxes, thus click **Save** to confirm your updates.

The **Connector History** tab is where you can view a history of the outcomes of the past runs of a selected connector, based on the channel mode.

You can enter the following information to filter your search for past runs:

Table 216. Connector History filters

Filter	Description
Start Date from	Shows all runs started from this date onwards.
Start Date to	Shows all runs started until this date.
Result	Can be: • Blank (all) • Completed • Error

The list of connector runs in Reconciliation mode is shown in the following columns:

Table 217. Connector History attributes

Attribute	Description
Channel Mode	Reconciliation.

Table 217. Connector History attributes (continued)

Attribute	Description
Result	Completed or Error.
Message	The message displayed in the **Message** text box.
Start Date	The starting date and time the connector run started.
Elapsed Time	The completion (if successful) or ending (if in error) time of the run.

To delete a particular run history line from the list, select the line and click **Actions** > **Remove**. To delete all run histories, click **Actions** > **Remove All**.

Settings

In this panel you can update the Object Class nodes and Object Class Field nodes of the IDEAS driver which map the layout of data in your Identity Governance and Intelligence security model.

Object Class nodes and Object Class Field nodes make up the structure in which information, such as user names, roles, groups, accounts, passwords, and any other type of data used in your security model is mapped in the model. An Object Class node contains several Object Class Field nodes and every Object Class displays its fields in a tree structure in this pane.

The IDEAS driver already comes with its own list of attributes, but you can define additional attributes to this driver, as well as edit and remove these attributes to comply with the changes of your security model.

The Settings panel displays the list of the Object Class nodes defined in the IDEAS driver. Each Object Class node can be expanded to display its Object Class Field nodes. The information is shown in the following way:

Table 218. **Settings** > **IDEAS driver** *panel layout.*

Name	Description
Field Name	The name of the Object Class nodes and, when expanded, of their Object Class Field nodes.
Description	A description of the Object Class node.
Type	The Java data codes of the Object Class Field nodes.
Is Multivalue	Shows if the field can have more than one value. Can be `true` or `false`.

Click **Actions** > **Add** to add:

- A New Object Class node
- An Object Class Field node

as follows:

- If you click **Add** with no selected Object Class nodes in the list, you are shown the `Add node` window with the following fields:

Table 219. New Object Class node attributes.

Name	Description
Name	The name of the Object Class
Description	A description of the Object Class

- If you click **Add** with a selected Object Class node, the `Add node` window gives you the choice of specifying the attributes of another Object Class node or those of a field of the selected node (`Add Object Class Field node to` *`node_name`*). If you opt for adding an Object Class Field node, the attributes you must specify are:

Table 220. Object Class Field node attributes.

Name	Description
Name	The name of the Object Class Field node
Description	A description of the Object Class Field node
Type	Click the arrow to display a list of Java data codes to choose from
Multivalued	Flag this check box if the field will have more than one value

The Object Class Fields are added as hierarchy leafs to the Object Class node. You can add as many fields to an Object Class node as required. Ultimately, each Object Class node is displayed with all its fields in a tree structure.

To edit or remove an Object Class node or an Object Class Field node, select the object and click the appropriate item in the **Actions** menu.

If you click **Actions** > **Automatic Add**, the list is updated with the latest changes in the layout of the AG Core repository.

Introduction to IRA agent

The Remote Agent (IRA) is part of the Identity Governance and Intelligence platform that lets you receive user events on Windows Active Directory (AD) and Workgroup (WG) from the AD and WG Identity Governance and Intelligence connectors. These events are related to creation/deletion/modification operations of user data.

The component, from the architectural point of view, is a server that listens the connectors and performs the required operations from IBM Security Identity Governance.

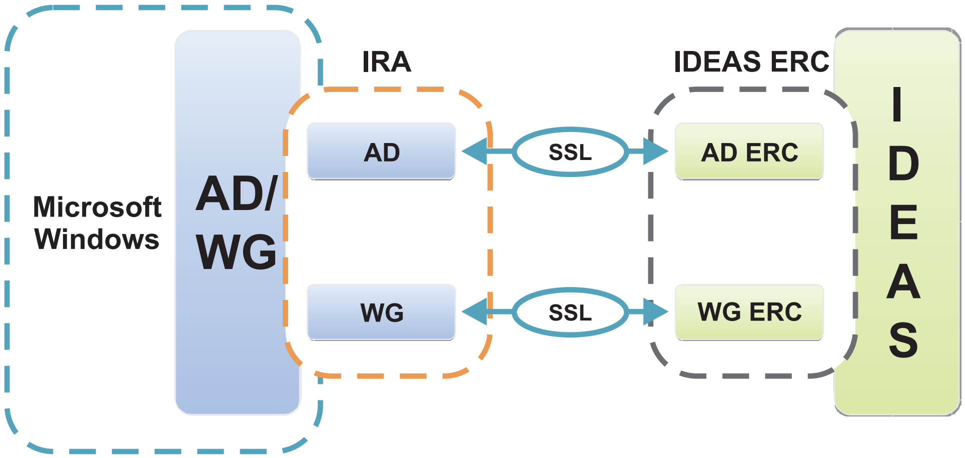
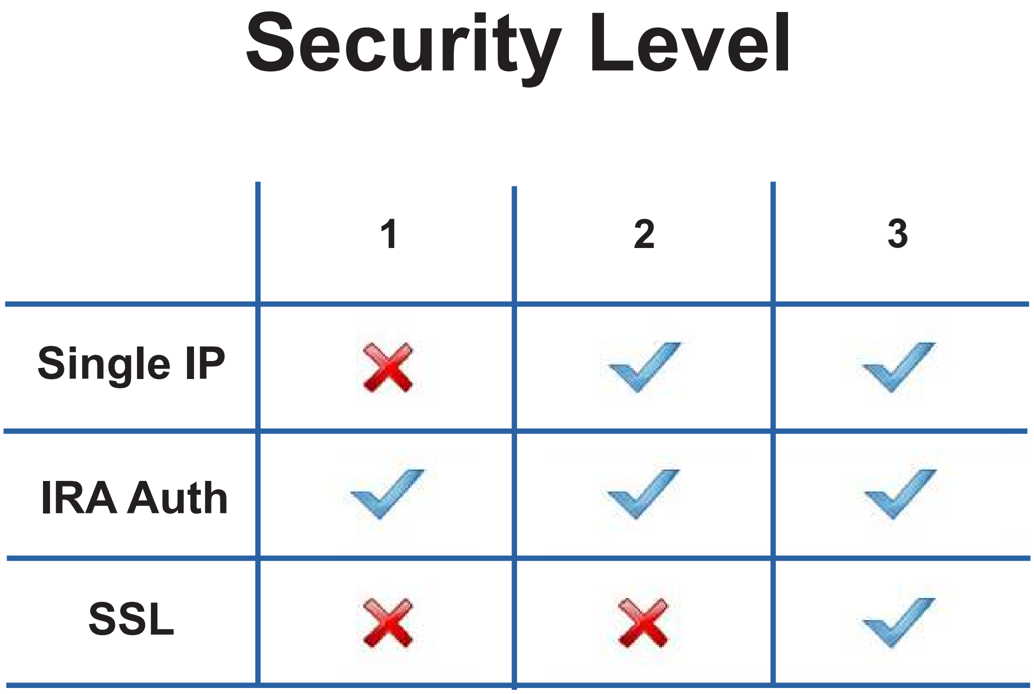


Figure 67. The communication process between AD/WG and Identity Governance and Intelligence.

Several levels of security are provided:

- Define the source IP address
- Choose the IBM Security Identity Governance password for authentication to IRA
- Enable the encryption SSL channel



Security Level

	1	2	3
Single IP	✗	✓	✓
IRA Auth	✓	✓	✓
SSL	✗	✗	✓

Figure 68. Security levels.

For further details, see:

- Prequisites HW/SW
- Setup options
- Install procedure (example)

- Uninstallation procedure

Prerequisites

Before proceeding with the installation of IBM Security Identity Governance IRA on the host workstation where AD/WG is located, it is recommended to verify the base hardware and software requirements.

The base hardware and software requirements are described in the tables below:

Hardware requirements		
Element	**Description**	**Note**
Server	RAM > = 4 GB	Not applicable
	CPU Cores > = 2	Not applicable
	Storage: 30 MB	Not applicable

Software Requirements		
Element	**Description**	**Note**
Operating System	Microsoft Windows 2003 Standard Server SP2 Microsoft Windows 2008 R2 Standard SP1	Not applicable
Microsoft .NET	.NET Framework 3.5 SP1	Not applicable

IRA setup and patches

Two different types of setup are provided, one for the management of the target Active Directory, and one for Workgroups.

Each of them with two versions depending on the type of platform, 32- or 64-bit.

The version of the Active Directory matches, in terms of setup, with the previous version 4.2.1. For this reason, the patches are only for Active Directory versions 32- and 64-bit.

The available setups are four:
- Active Directory 32-bit
- Active Directory 64-bit
- Workgroup 32-bit
- Workgroup 64-bit

Each setup has an associated GUID product. None of these setups can be run on a workstation if another version was previously installed.

ℹ	**Note:** Every setup must be used for the first installation. If there is a previous version already installed, an error message is displayed.

Table 221. IRA setups.

Setup name	Description
setupirac32AD.exe	Installs the Active Directory version for 32-bit workstations.
setupirac64AD.exe	Installs the Active Directory version for 64-bit workstations.
setupirac32WG.exe	Installs the Workgroup version for 32-bit workstations.
setupirac64WG.exe	Installs the Workgroup version for 64-bit workstations.

The following are the IRA patches:

Table 222. IRA patches.

Patches name	Description
patchirac32AD.exe	Updates the Active Directory version for 32-bit workstations.
patchirac64AD.exe	Updates the Active Directory version for 64-bit workstations.

ℹ	**Note:** Patches can only be used to update a previous installation. If no version of IRA is installed, an error message is displayed.

To distinguish the different options available for setup and patches, see the sections below:

- First installation
- Patch updates

First installation

The first installation is always made in two steps; the basic setup (setup X.0) and the latest patch (patch X.N).

If the patch installed is not the latest, you can directly install the latest patch.

Patch updates

After the first installation, the version evolution of IRA is managed using a patching process, displayed in the figure:

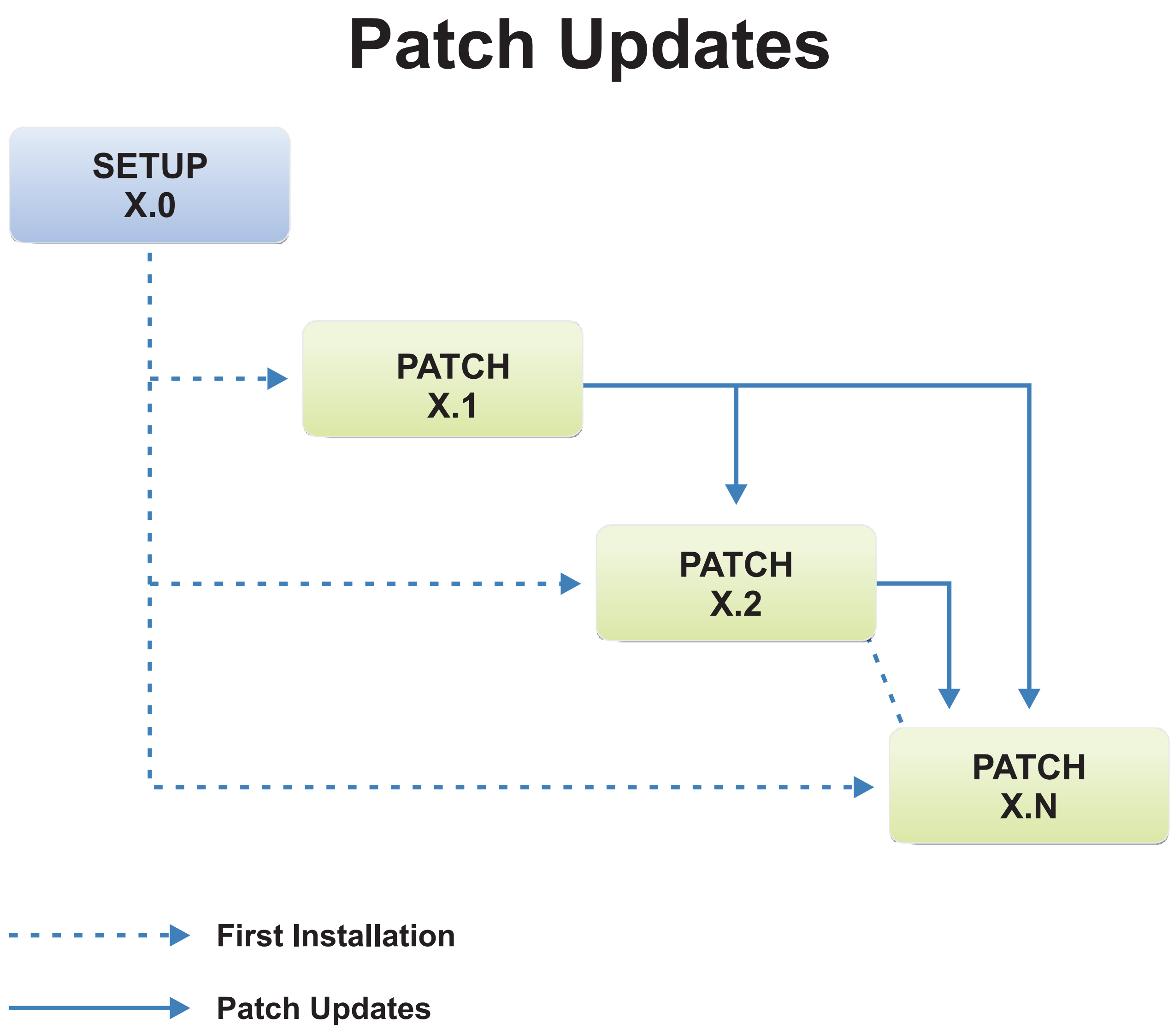


Figure 69. Patch updates.

Installation procedure

This section shows an example of a remote agent setup.

The following is a setup example for the Identity Governance and Intelligence (IDEAS) remote agent (x64) for Active Directory (`setupirac64AD.exe`):

1. Click `setupirac64AD.exe`. The first Warning window opens.
2. Click **Yes** to confirm the operation. The second Warning window opens.
3. Click **Yes** to confirm the operation. The Identity Governance and Intelligence Remote Agent for Active Directory - Installation Shield Wizard window opens.
4. Click **Next** to move to the second step.

   Click **Change** if you want to change the default directory, thus click **Next** to move to the third step.
5. Tick the check-box **IBM Security Identity Governance remote agent (core)**

Note: IRA contains an optional module (to be selected during the set up) that allows IBM Security Identity Governance to implement the system password change notification. This option requires the Microsoft Windows Password-Filters option. If the administrator decides to install the password change notification service, it is recommended to reboot the workstation both during installation and uninstall phases.

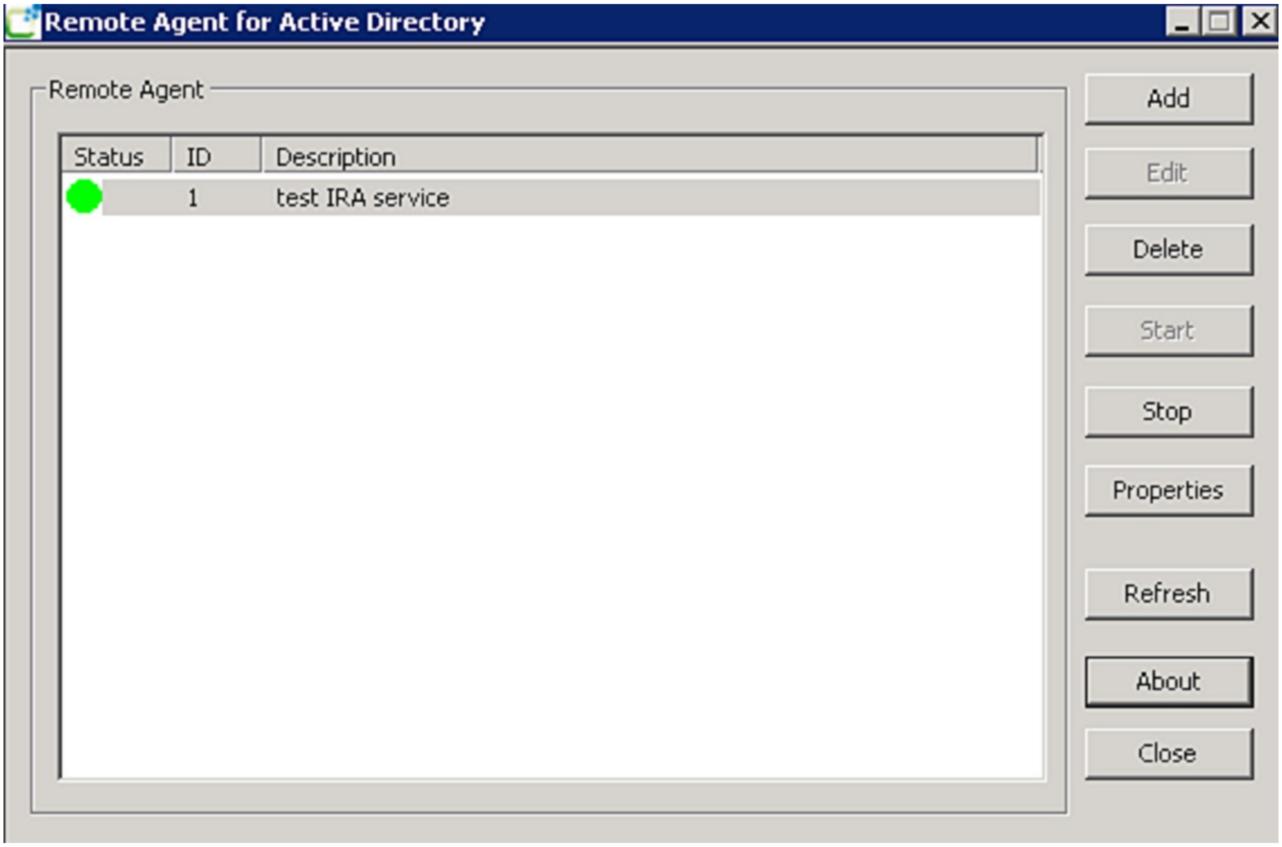
6. Click **Next**, thus click **Install**to start the installation.

After the installation completes, click **Finish** for terminating the installation process.

Remote agent for active directory

The Remote Agent for Active Directory window is described.

After selecting the IRA console from **Starts**, the Remote Agent for Active Directory window displays:



Status	ID	Description
●	1	test IRA service

Figure 70. The Remote Agent for Active Directory window.

From this window, the administrator can perform the following main operations:

- Add Service
- Edit
- Start/Stop
- Properties
- Refresh
- About

- Close

Table 223. Administrator actions

Note	**Text**
ℹ	**Note:** For some platforms, you might need to start the IRA console by clicking “Run as Admin”.

Add service

Clicking **Add** on the right part of the window, the Add Service window displays. You can fill the fields described in the table below:

Table 224. **Add Service** *window fields*

Field name	**Description**	
Remote Agent ID	Univocal identifier of the remote agent (settled by default).	
Description	Brief description of the remote agent (mandatory).	
Communication	**Client**	IP of the IBM Security Identity Governance server (mandatory if the **All** check box is not selected).
	All	Selecting this check box is not mandatory to specify the IP address of the IBM Security Identity Governance server (the **Client** field will be disabled).
	Port	Listening port of the IBM Security Identity Governance server (mandatory).
Service Account Properties	**Modify service account properties**	Selecting this check box allows you to modify the service account properties.
	Domain Name	Name of the domain.
	User Name	Name of the administrator.
	Password	Enter the administrator password.
	Confirm	Confirm the password.
Remote Agent Password	**Password**	Remote agent password (mandatory).
	Confirm	Confirm the password (mandatory).
Secure Socket Layer (SSL)	**SSL**	Select this check box to enable the server certificate fields.
	SSL Server Certificate Common Name	Enter the certificate name.
	Select Certificate	Click this button to choose the available certificates from the list of the certificate store MY of the workstation.

Table 224. **Add Service** *window fields (continued)*

Field name	Description	
Log File	**Log**	Select the check box to enable the **Log File** field.
	Log File	Enter the path name of the log file.
	Folder button	Click this button to choose the folder where to save the log file. This sets the name of a log file (`ira_N.log`).

Add service fields

Table 225. **Add service** *fields*

Note	Text
ℹ	**Note:** The IBM Security Identity Governance ERC administrator must enter the same **Remote Agent Password** in the **Driver Connector property** fields. From the IBM Security Identity Governance ERC module, select: **IBM Security Identity Governance ERC** > **Manage** > **Connectors** > **Driver Configuration** > **Driver**. Properties involved are: • `adRemoteConnectionPassword` for AD IBM Security Identity Governance ERC • `wgRemoteConnectionPassword` for WG IBM Security Identity Governance ERC

Click **Ok** to confirm the operation.

Edit

Click **Edit** to modify the service properties.

Delete

Click **Delete** to remove one or more services.

Table 226. Remove services

Note	Text
ℹ	**Note:** Before deleting a service, it is not necessary to turn it off.

Start/Stop

Click **Start** to turn on the service. The service status is characterized by a 🟢 green icon.

Click **Stop** to turn off the service. The service status is characterized by a 🔴 red icon.

When a service is stopped, an Information window displays.

Properties

Clicking **Properties**, the Service Properties window displays. You cannot modify any properties.

Refresh

Clicking **Refresh**, you can update the graphical status of the service (🟢 / 🔴 green/red icons) in case of errors or if someone stopped/started the service from Windows.

About

Click **About** to view the version and copyright information.

Close

Click **Close** for closing the IRA console. This action does not affect the status of the service (**Started**🟢 or **Stopped**🔴).

Chapter 25. Introduction to Access Optimizer

Access Optimizer (AO) is a powerful and comprehensive tool for risk analysis and role mining in medium and big size companies.

IBM Security Identity Governance and Intelligence Access Optimizer (AO) is a powerful and comprehensive tool for risk analysis and role mining in medium and big size companies.

Access Optimizer is fully integrated with IBM Security Identity Governance and Intelligence role management facilities, to support continuous role development and optimization as business processes evolve. New roles can be automatically passed to a role management workflow where the role is approved and deployed to production.

The main advantages of the Access Optimizer engine are:

- Innovative pre-mining analysis finalized to generate intuitive business roles.
- Cost driven role mining with a rich set of parameters to tune the role mining process, minimizing the administrative cost of generated roles.
- Interactive graphical optimization to visually optimize roles with useful information to facilitate coverage analysis of user-privilege relations to identify potential side effects of analysis changes.
- Role lifecycle support integrated with role management for role deployment to production.
- Comprehensive management of risk analysis focused on identifying a certain type of risk for the company to find the right solutions.

Architecture and components

This section describes the main blocks of the Access Optimizer (AO) architecture and specifies the essential peculiarities of each component module.

The following figure summarizes the overall architecture of the AO module:

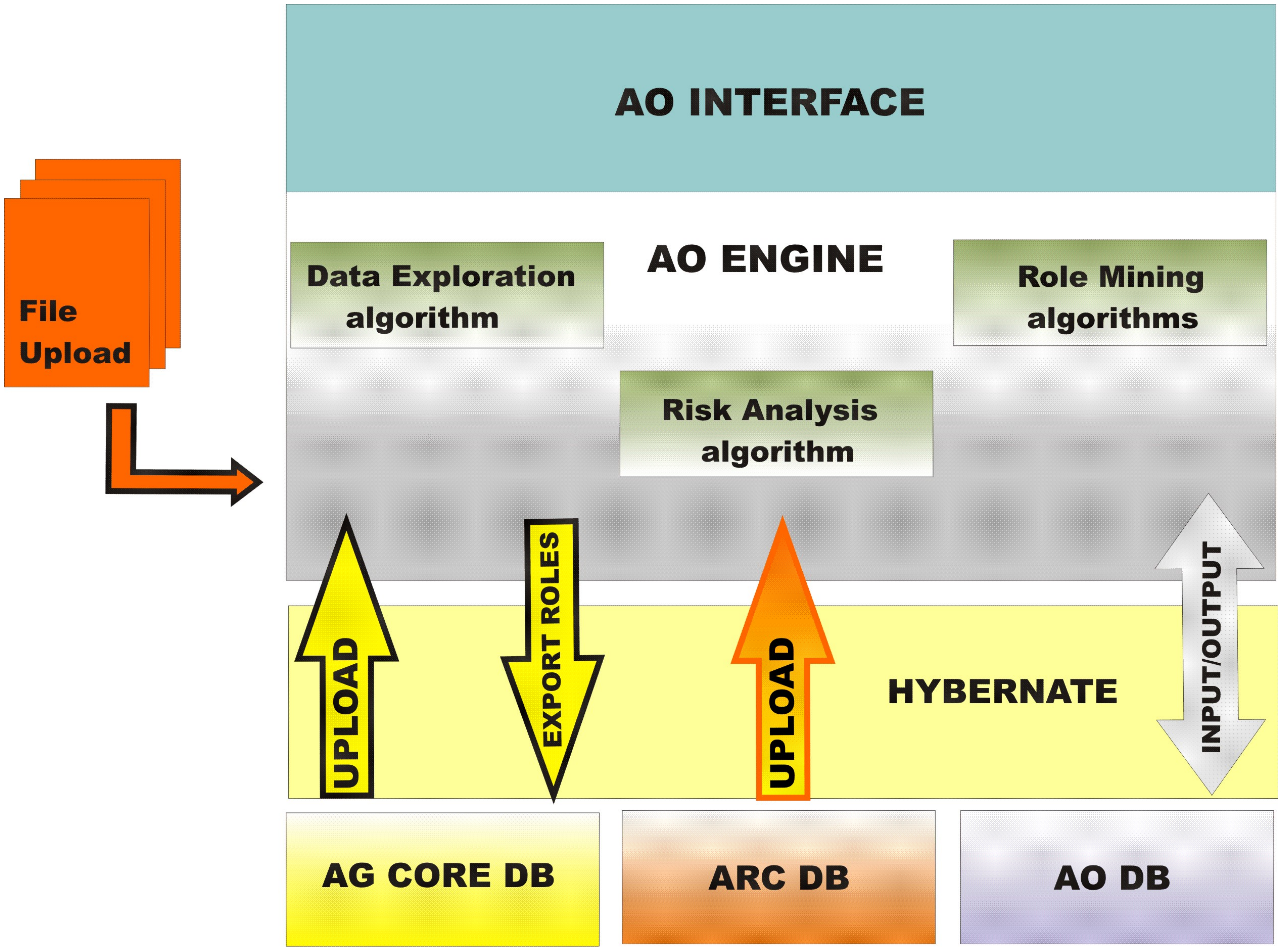


Figure 71. Access Optimizer: Components and architecture.

The following sections describe the features of all modules displayed in the figure above. The main sections are listed below:

- AO Module
- AO Engine
- Access Governance Core Module
- Access Risk Controls Module
- Hibernate Layer

AO module

The AO module represents the user interface for administering the AO functionality.

More specifically, using this interface you can:

- Load the model dimensions (mainly organization units, users, entitlements, applications and assignments)
- Configure a large set of data model attributes
- Perform the data exploration processes
- Perform risk analysis processes
- Perform role mining processes

- Export the validated candidate roles to the main Access Governance core repository.

For more details about the main characteristics of this module, see Access Optimizer: Guide to Modeling.

AO engine

The AO engine implements the data exploration, risk analysis and role mining processes, based on advanced algorithms.

Access Governance core module (AG Core)

The Access Governance core (AG Core) is the Identity Governance and Intelligence module that manages digital identities, and delineates and implements access rights/control.

Access risk controls module

Access risk controls (ARC) is the Identity Governance and Intelligence module that, in the context of authorization definition based on the AG Core RBAC model, implements SOD mechanisms based on the concept of conflicting roles.

Hibernate layer

Hibernate is an ORM (Object Relational Mapping) framework that manages information persistence in the database.

ORM is a group of management methods and techniques that enable an object-oriented paradigm to interact with a relational paradigm of the Relational Database Management Systems (RDBMS). The goal of ORM is to program this interaction using a pure object-oriented paradigm that conceals the relational paradigm translation from the developer.

The Access Risk approach

Granting access to resources in a medium or large company can raise the probability of incurring into several types of threats.

To measure and reduce such probability, the Identity Governance and Intelligence model follows the Access Risk approach.

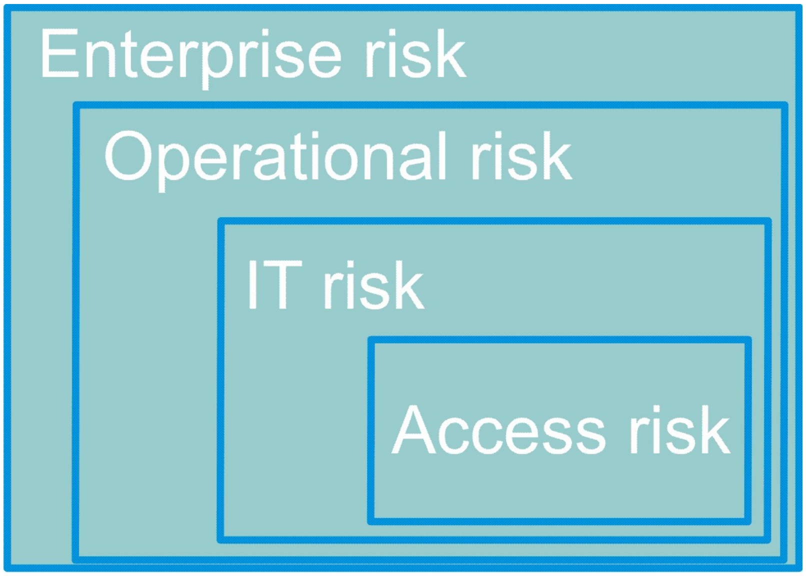


Figure 72. The Access Risk approach.

The Access Risk approach relies on a tagging process of the potential risks related to assigned accesses whereby the key entities managed by the IAG solution are assigned a score. The process provides the capability to drive the most effective remediation measures.

Assigning a score to an access risk, the Access Risk analysis process makes the risk measurable and likely to be mitigated.

Access Risk scoring is based on a viable methodology for modeling, measuring, and reducing the threats to an access, as the next figure shows:

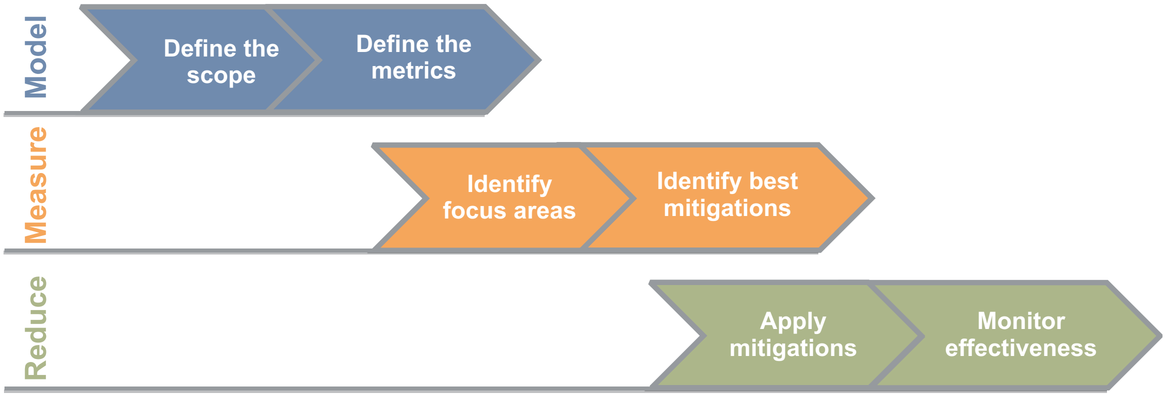


Figure 73. The Access Risk scoring model.

To enable actionable Access Risk scoring, it is necessary to explore the access risk space from the following standpoints:

Data sets
Define the data partition (define the scope and identify the focus area).

Risk Models
Blend access risk contribution types (define the metrics, identify the best mitigation, and apply mitigations).

Time Trend analysis and drilldown snapshot (apply mitigations and monitor effectiveness).

The next figure schematically explains the Access risk space:

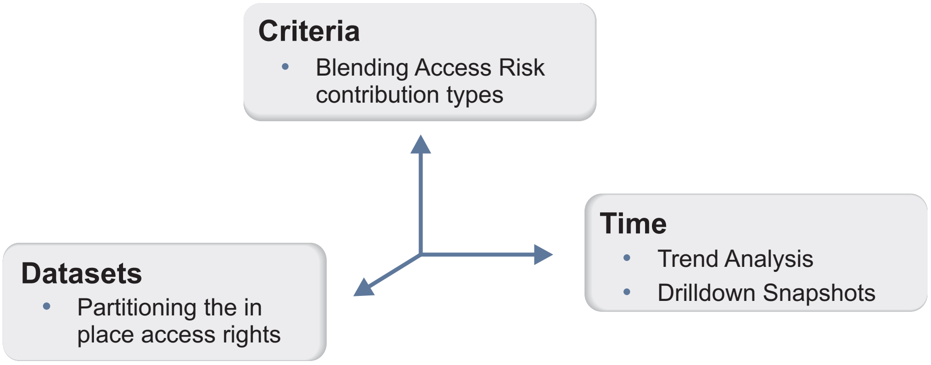

Criteria
Blending Access Risk contribution types
Time
Trend Analysis
Drilldown Snapshots
Datasets
Partitioning the in place access rights

Figure 74. The Access risk space.

The following sections provide a detailed explanation of what it means to explore the access risk space with a viable methodology:

- "Defining an Access data set"
- "Measuring access risk criteria" on page 455
- "Reducing risk distribution" on page 459
- "Monitoring access risk trend over time" on page 459

Defining an Access data set

The first step is to define the relevant perspectives through the data definition.

The next figure shows an example of data definition:

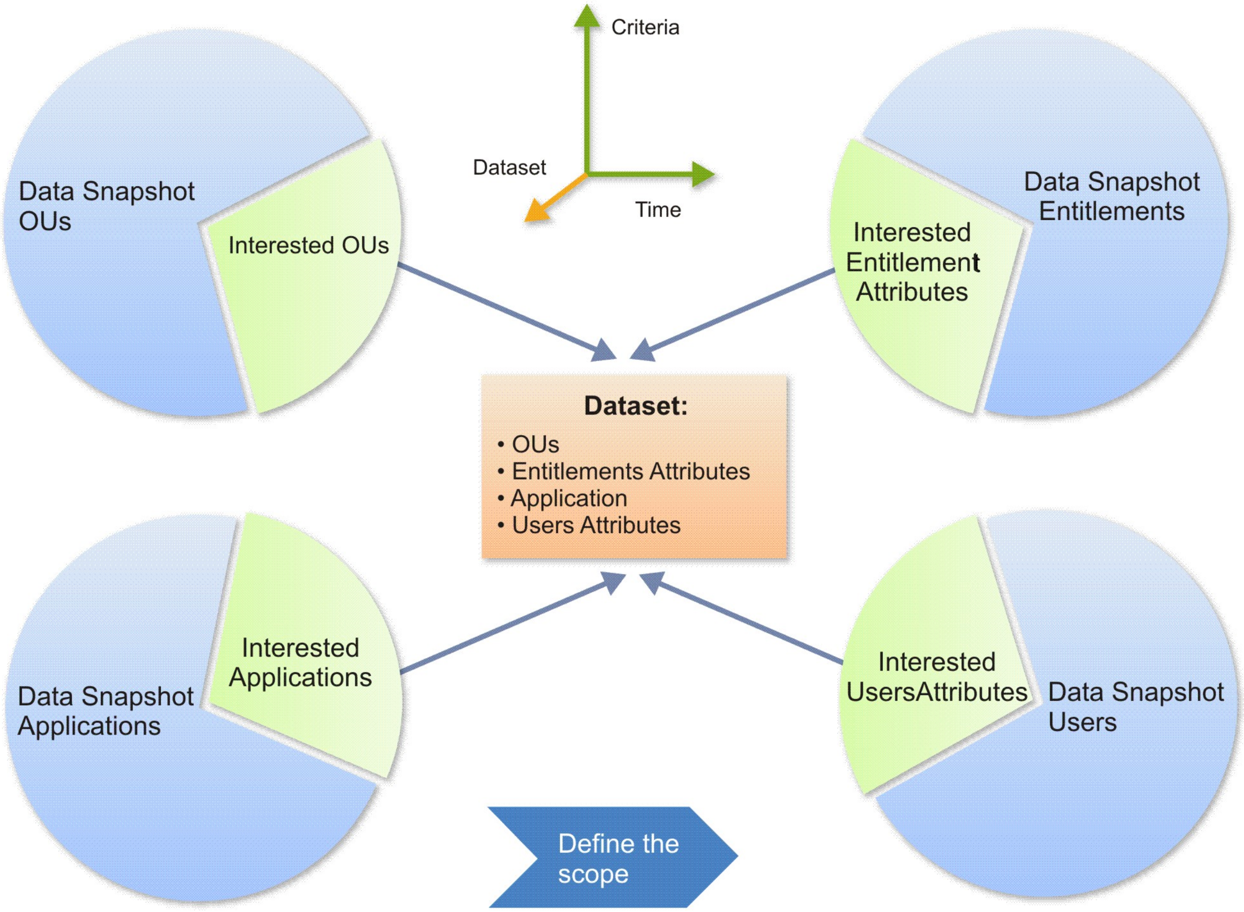
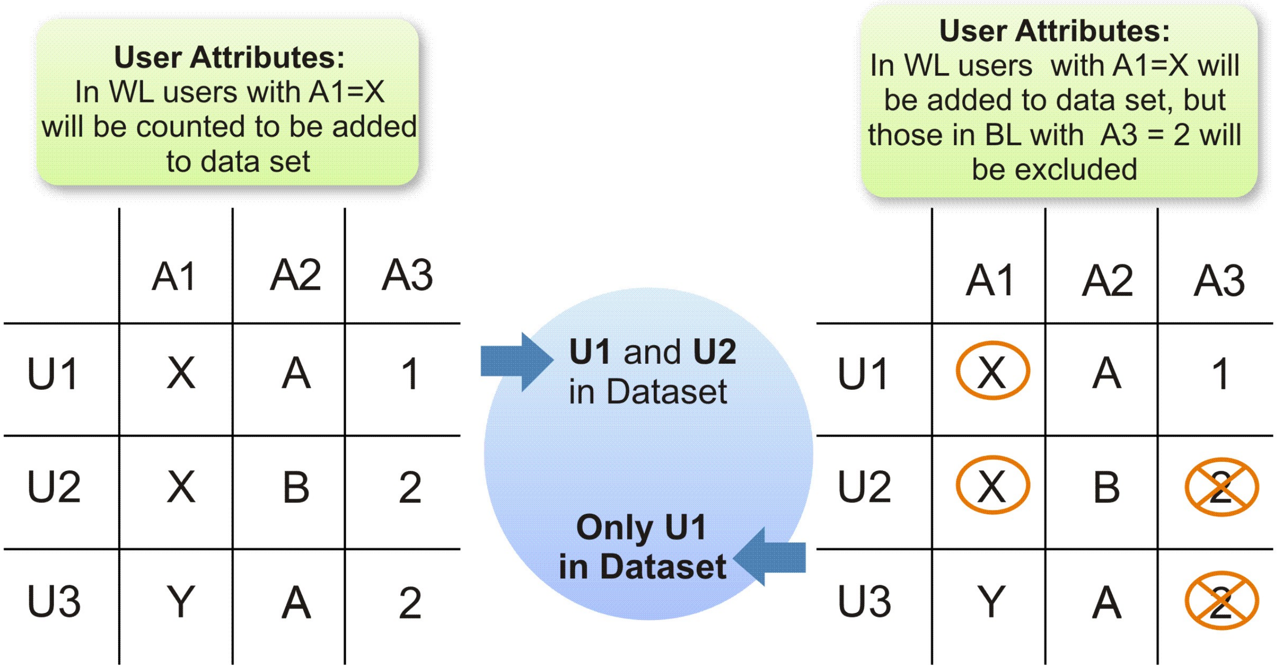


Figure 75. Define a data set.

The figure shows that the relevant OUs, applications, user attributes, and/or entitlement attributes elected for analysis can be grouped in a data set named Access data set. You can define the Access data set by placing the items that you want to inspect in a White List, while placing the elements that you want to exclude from inspection in a Black List. This is shown in the next figure:


User Attributes:
In WL users with A1=X will be counted to be added to data set
U1 and U2 in Dataset
Only U1 in Dataset
User Attributes:
In WL users with A1=X will be added to data set, but those in BL with A3 = 2 will be excluded

	A1	A2	A3
U1	X	A	1
U2	X	B	2
U3	Y	A	2

	A1	A2	A3
U1	X	A	1
U2	X	B	2
U3	Y	A	2

Figure 76. Using black and white lists to define a data set.

The figure shows how to build an Access data set that contains all the users that have the A1=X attribute. To achieve this, in the white list specify all users for whom attribute A1=X. In this way, users U1 and U2 are selected to be included in the data set, as the matrix in the left shows.

Another example is shown by the matrix on the right of the figure, where the Access data set is to include all users with attribute A1=X with the exception of those with attribute A3=2. To achieve this, in the white list specify all users for whom attribute A1=X, and in the black list specify all users for whom attribute A3=2. In this case, user U2 is not added to the data set because, although it has A1=X in the white list, it has A3=2 in the black list. The data set will therefore include only user U1 as it is the only user whose attributes match the desired specifications.

In Access Optimizer you can apply this process to the data (OUs, applications, user attributes, entitlement attributes) on which you want to run a risk analysis. In this way, the risk analysis is performed on an Access data set that includes only the items filtered by the white and black lists.

Note: For any given item (OU, application, user, entitlement) you cannot specify the same filter in both white and black lists. If you do so, the filter is ignored when the data is analyzed.

Measuring access risk criteria

To help the administrator choose the best access risk criteria, Access Optimizer is provided with a predefined catalog.

The predefined catalog is described in the table below:

Table 227. Predefined access risk criteria.

Risk criteria	Description
All Relevances	Global risk score on the assignments to identify critical data sets.
Not Recertified	Higher risk score on assignments not recently certified.
Power Users	Higher risk score on users with critical permissions. (bound to many business activities).
SoD Risk	Higher risk score on users with many SoD conflicts.
The Almighties	Higher risk score on entitlements bound to many business activities, assigned to users with many SoD conflicts but not recently certified.
The Exceptions	Higher risk score on assignments too different from their peers.
The Others	Higher risk score on assignments too different from their peers and not recently certified.

These criteria are a compound of metrics that optimize the risk analysis. Metrics are all configurable and removable. The only exception is the first criteria, All Relevances, which comprises all available risk criteria metric objects.

The compound metric objects are:

- **User Relevance**: relevant information about the user's attributes.
- **Entitlement Relevance**: relevant information about the entitlement's attributes.
- **Assignment Relevance**: relevant information about the assignment's attributes.

You can also customize new risk criteria and relevance depending on your needs. You can use the following filters to search relevant information about these entities:

Table 228. Relevance filters

Filter	Description	ON	OFF
User relevance	Number of assigned permissions	Evaluated in the risk analysis.	Not evaluated in the risk analysis.
	Number of SoD violations		
Entitlement relevance	Number of assigned business activities		
	Number of SoD constraints		
Assignment relevance	Similarity divergence		
	Last certification age		

The access risk models and metrics definitions help the administrator identify the highest access risk place, or focus area, and how the risk spans over different partitions (Access distribution).

The next figure shows an example of what it means to identify the focus area:

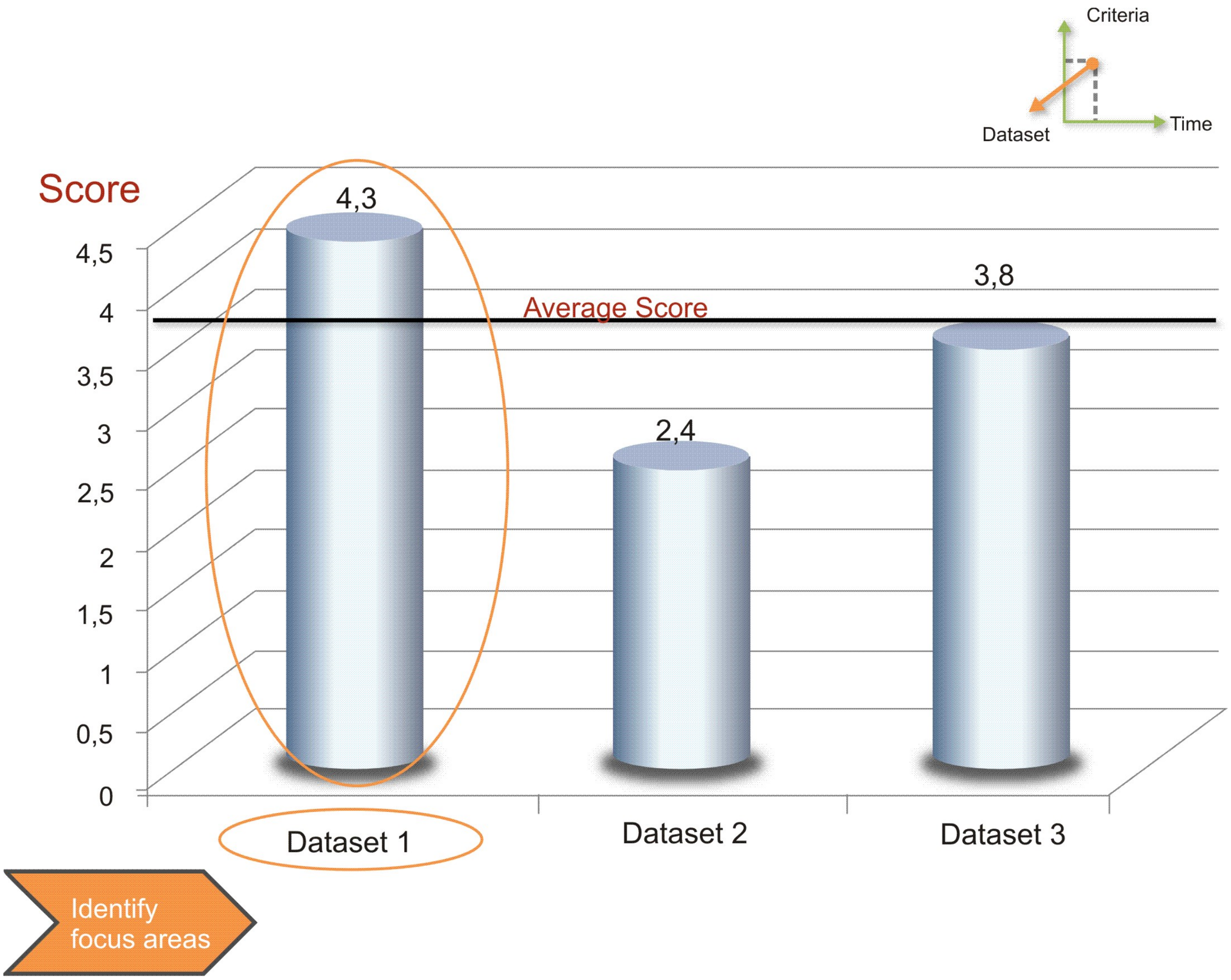


Figure 77. Identify focus area.

In this way, the administrator can immediately visualize the focus Area in data set 1 but, after the focus area is identified, the administrator also needs to investigate the cause of the threat. He or she needs to analyze the interested focus area and compare the different risk criteria.

After the data set is analyzed based on the applied risk criteria, the administrator can see in which of the criteria the highest average risk resides, and identify the best mitigations to apply.

Following the example, the next figure shows that data set 1 has the highest average risk in the SoD risk.

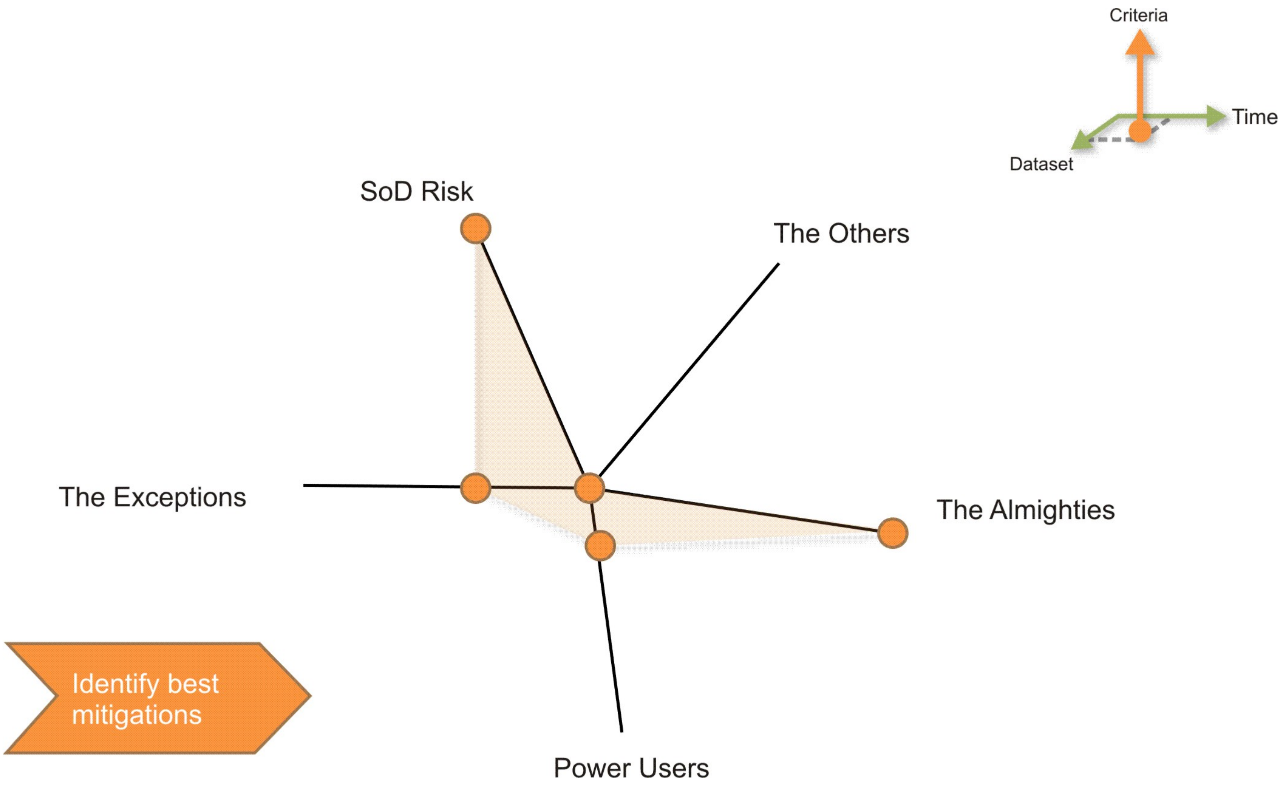


Figure 78. Identifying where the highest risk is.

This means that there are many SoD conflicts in data set 1. Now that the administrator knows where to operate, he or she can choose the best risk mitigating actions.

The most common measures for mitigation are the certification or mitigation campaigns, depending on the risk typology. The access risk criteria configuration suggests the most effective reduction approach. The table below lists a suggested reduction approach for every relevance:

Table 229. The Relevance Reduction Approach.

Name	Description	Suggested reduction approach
User relevance	Number of assigned permissions	Not applicable
	Number of SoD violations	SoD campaign
Entitlement relevance	Number of assigned business activities	Not applicable
	Number of SoD constraints	SoD campaign
Assignments relevance	Similarity divergence	Access certification
	Last certification age	Access certification

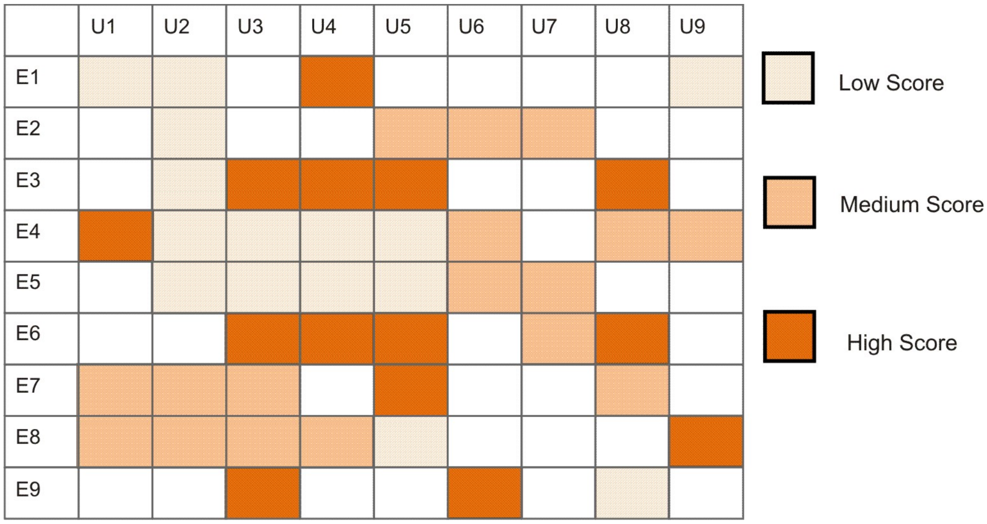
Note: To get meaningful data, you need to compare snapshots or data sets that contain the same data, updated from time to time. When data is first loaded, a trend graphic is not present.

Reducing risk distribution

After identifying the type of risk and determining the best solution to minimize it, the administrator must have the detail of how the risk is distributed amongst users and entitlements.

For this,Access Optimizer can provide Maps, where the rows are entitlements and the columns are users, that show the distribution and the magnitude of risk, which can then be easily identified by the administrator.

The next figure shows an example of a risk distribution map:



	U1	U2	U3	U4	U5	U6	U7	U8	U9
E1	░	░		█					░
E2		░			▒	▒	▒		
E3		░	█	█	█			█	
E4	█	░	░	░	░	▒		▒	▒
E5		░	░	░	░	▒	▒		
E6			█	█	█		▒	█	
E7	▒	▒	▒		█			▒	
E8	▒	▒	▒	▒	░				█
E9			█			█		░	

░ Low Score

▒ Medium Score

█ High Score

Figure 79. Risk degree and distribution.

The administrator can thus ascertain what combinations of users and entitlements bear the highest risk and require action. He/she can run attestation campaigns on the high risk section only, to gain complete control of the situation and easily manage the risks.

Monitoring access risk trend over time

By periodically inspecting the access risk space (or access distribution), the administrator can monitor the levels of risk over time, and ascertain the effectiveness of the risk mitigation actions he/she applied.

The following figure shows an example of how the administrator can monitor the presence of risk over time:

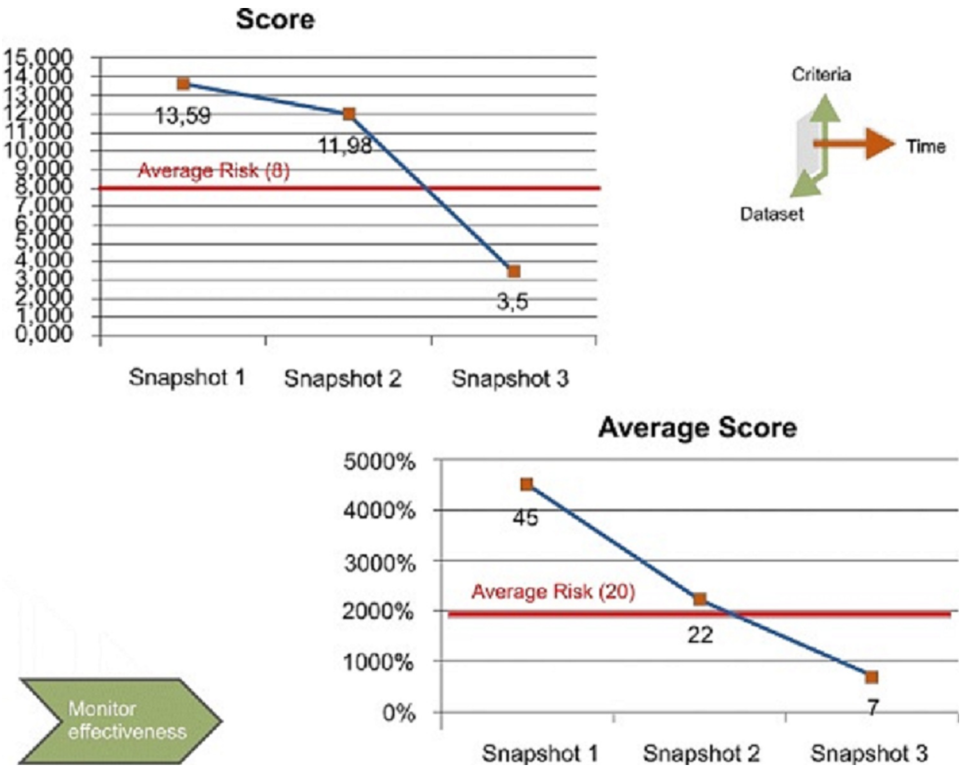


Figure 80. Monitoring effectiveness.

To get this kind of graphic, the administrator must compare more snapshots over time (always updated).

The figure shows that there are three snapshots:

- The first snapshot is taken when the data is first loaded.
- The second one is taken after the data was updated over time with a resulting gradual decrease of risk.
- The third one shows a further reduction of risk.

This means that the administrator mitigated the risk with the appropriate measures and, over time, saw a significant decrease in risk. In this way, the administrator can drive and track the reduction of access risk over time.

Note: To get meaningful data, the administrator needs to compare snapshots or data sets that contain the same data, updated from time to time. When data is first loaded, a trend graphic is not present.

Role mining guidelines

This section describes important role mining modeling concepts, including concerns related to configuration issues that can influence how you interpret the results produced by the role mining algorithms.

The role engineer must have a clear objective for the role mining process to be effective.

Candidate roles can be considered well-formed only when correlated with:

- The characteristics of the input data.

- The role engineer's objective.

In the basic roadmap for Access Optimizer, the role mining step can be exploited with the iterative approach listed below:

1. Run data exploration (**Manage** > **Data Exploration**).
2. Choose one of the result sets produced in step 1.
3. Run the Optimal Role-set algorithm.
4. Analyze the candidate roles proposed by the results of the previous step.
5. Return to step 3 to refine the analysis.

When you follow the basic roadmap, carefully examine the results provided by step 4.

These main aspects are listed below and described later:

- Minability
- Direct/Hierarchical assignments: Entitlement Type
- Spread
- Farness

Optimal Role-Set algorithm

This section explains the default parameter values of the Optimal Role-set algorithm. These default values will appear in every new Request operation (**Monitor** > **Report** > **Request**.

The Optimal Role-set parameters are described in the table below:

Table 230. Optimal Role-Set parameters

Parameter	Description
Minimum Number of Users per Role	Minimum number of users to whom a candidate role can be assigned
Minimum Number of Entitlements per Role	Minimum number of entitlements that can be associated to a profile included in a candidate role
Maximum Number of Roles	Maximum number of candidate roles
Role to User Assignments	Tendency to associate many/few users with a role
Role to Entitlement Assignments	Tendency to construct "large/small" candidate roles, grouping many/few entitlements into a Role
User to Entitlement Assignments	Tendency to associate many/few entitlements with a user (through a subset of candidate roles)
OU Spread	Spread is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization
Application Number	Tendency to associate many/few applications to a user (through a subset of candidate roles)

Table 230. Optimal Role-Set parameters (continued)

Parameter	Description
`Entitlement Type Number`	Tendency to associate many/few entitlement types to a user (through a subset of candidate roles)
`User Attributes`	These are listed only if configured in the User Attributes section.
`Entitlements Attributes`	These are listed only if configured in the Entitlements Attributes section.

The Minability index

This index, ranging from 0 to 100, represents the main output of the data exploration algorithm.

The Minability index measures the ability to create roles easily and efficiently by aggregating several assignments under a single role. This implies that when assignments are densely aggregated, the role can be identified more easily (High minability). If assignments are scattered throughout the map, it becomes more difficult to choose a meaningful set of assignments to create a candidate role (Low minability).

Generally, high minability values correspond to large aggregations of assignments. This is shown by large and unbroken blocks of assignments in the Entitlements map.

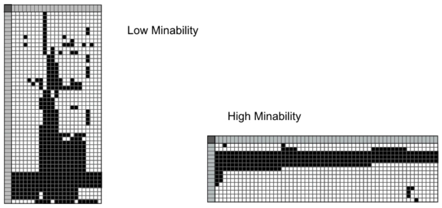


Figure 81. High/Low minability

It is best to avoid examining maps with very high numbers (thousands) of entitlements and users, as you would not obtain very useful information.

Direct or hierarchal assignments: concept of entitlement type

The Identity Governance and Intelligence data model is based on the concept of hierarchical entitlements.

There are several types of entitlements. They are:

Permission
: It is the basic authorization object. It is defined as a permitted action on a protected object (such as reading and writing a local files or creating a connection).

IT Role
: A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Role(s)

- Permission(s)

External Role

A set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Role(s)
- Permission(s)

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined within the same organization unit. It can contain:

- Business Role(s)
- IT Role(s)
- External Role(s)
- Permission(s)

A business role (BRole) can be hierarchically formed by business roles, IT roles, external roles, and permissions. An IT role can be formed by IT roles and permissions. An external role can include other external roles and permissions.

The generic hierarchical structure of an entitlement is shown in the following figure.

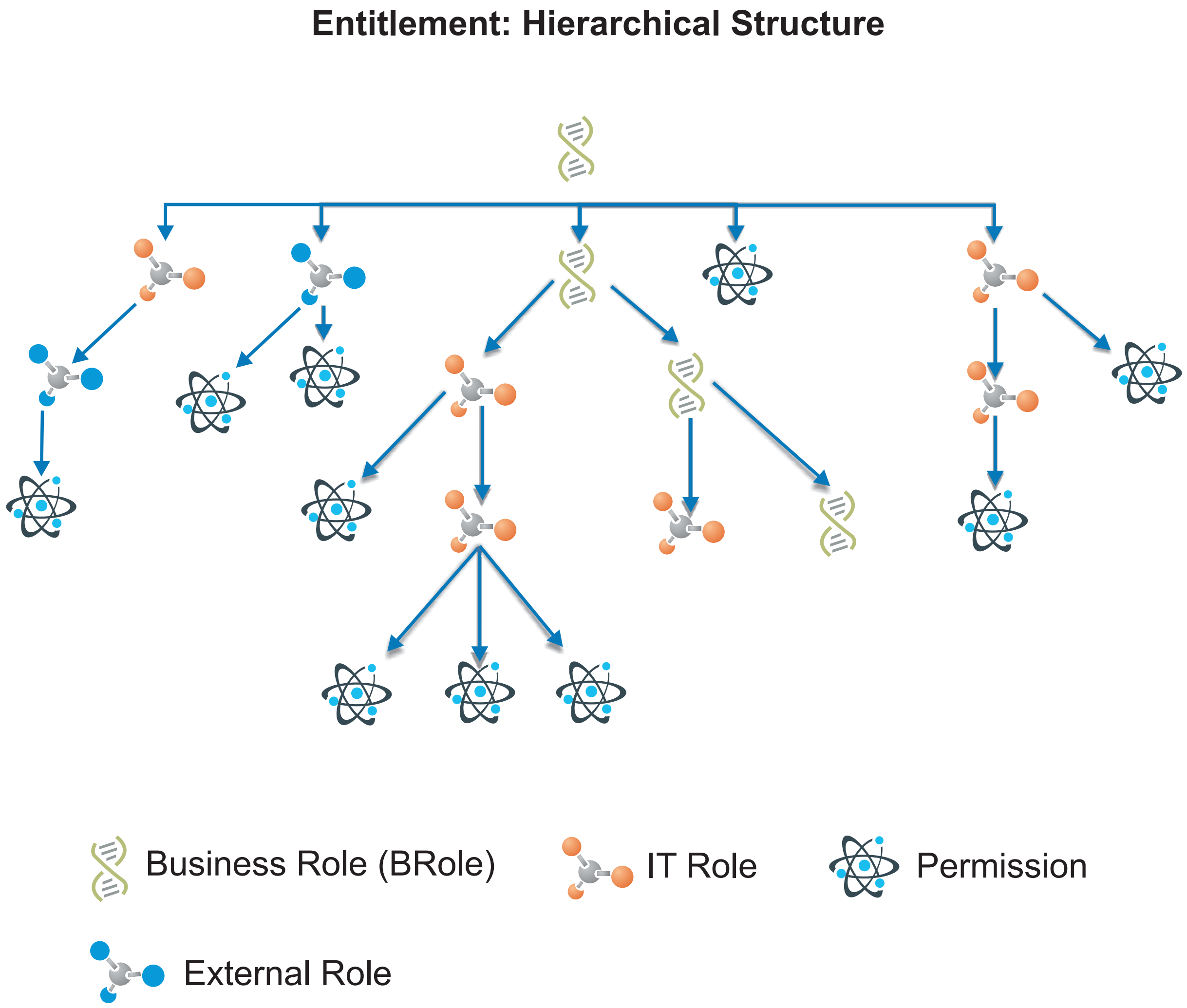


Figure 82. Structure of a generic entitlement

The IBM Security Identity Governance and Intelligence entitlements model does not limit the number of hierarchy levels.

Permissions represent the basic elements on which authorizations are built. The permissions of an application are mapped with target system authorizations that are directly assigned to the users.

In IBM Security Identity Governance and Intelligence you can select *N* permissions that are filtered by an application in several sections. The IT Role object collects a set of permissions that are related to the same application.

You can have two types of scenarios.

- an entitlement that is assigned in a direct mode (direct assignment)
- an entitlement that is in a hierarchical structure (hierarchical assignment) is assigned in a hierarchical mode.

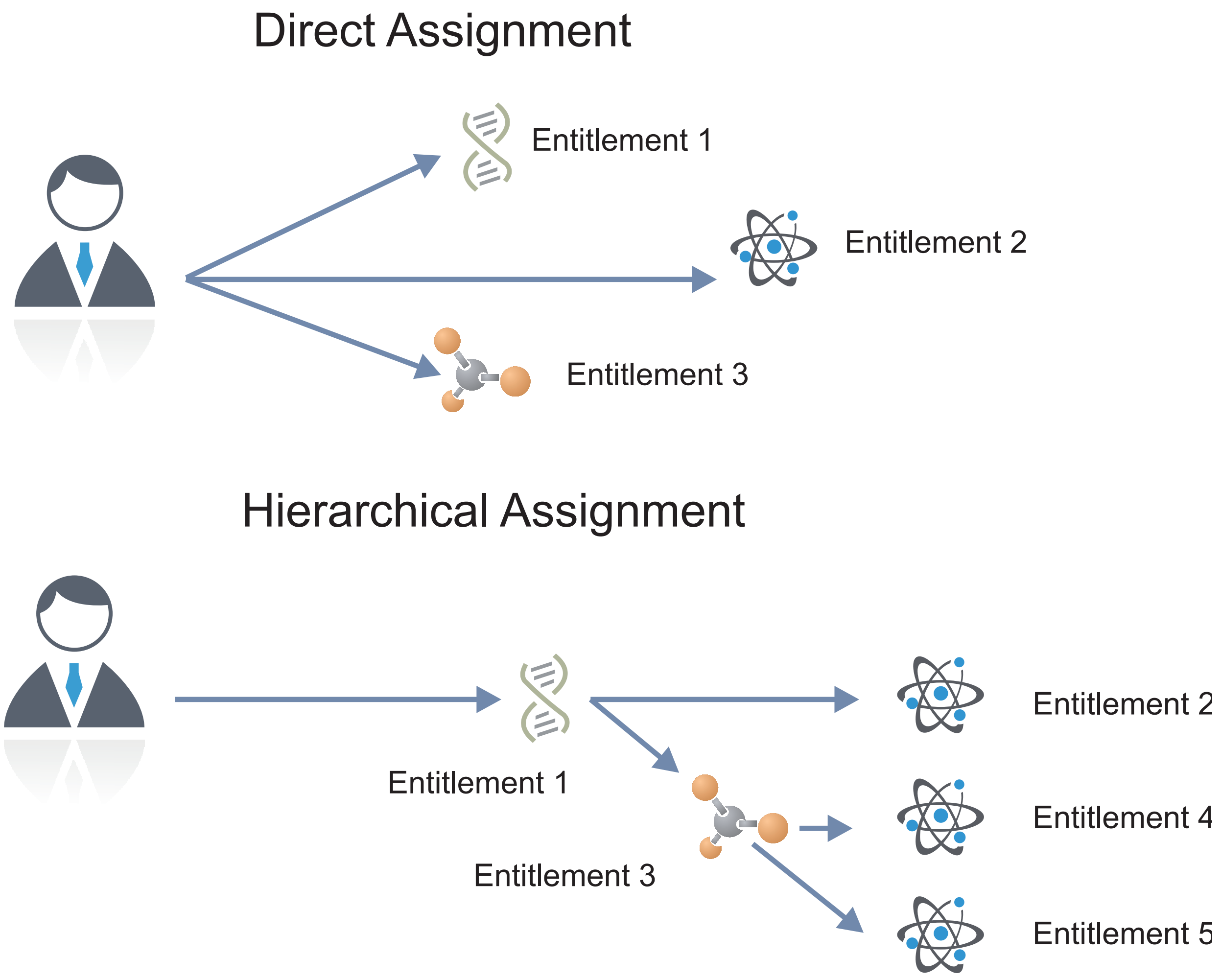


Figure 83. Direct and hierarchical assignment

If you assign the Entitlement 2 (Permission 2) to a user, you directly assign the Entitlement 2 only.

If you assign the Entitlement 1 (Business Role 1) to a user, you directly assign the Entitlement 1. Hierarchically, the user is assigned the Entitlements 2 - 5. This must be taken into consideration during the role engineering activity.

The permissions grouped in an external role are by definition handled by hierarchical assignment, since they cannot be granted individually.

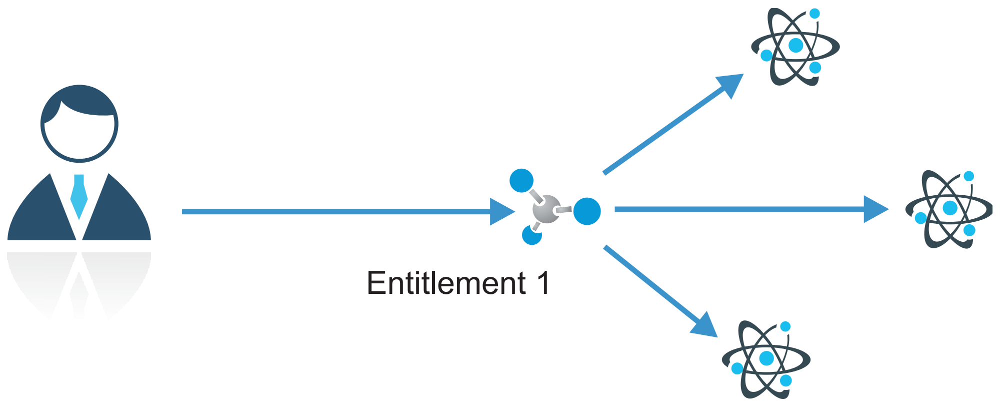


Figure 84. Hierarchical assignment for external roles

During the request construction, the selection of the **Only direct assignments** check box limits the analysis to direct assignments only. If the check box is not selected, inherited entitlements will also be included. This check box is available for all algorithms (data exploration, optimal role set) of the Access Optimizer module.

Hierarchical assignments: a blue spotted map

In the roles map, entitlements hierarchically inherited from another entitlement are highlighted in blue. The involved assignment, instead of being represented by a black box, is outlined in blue.

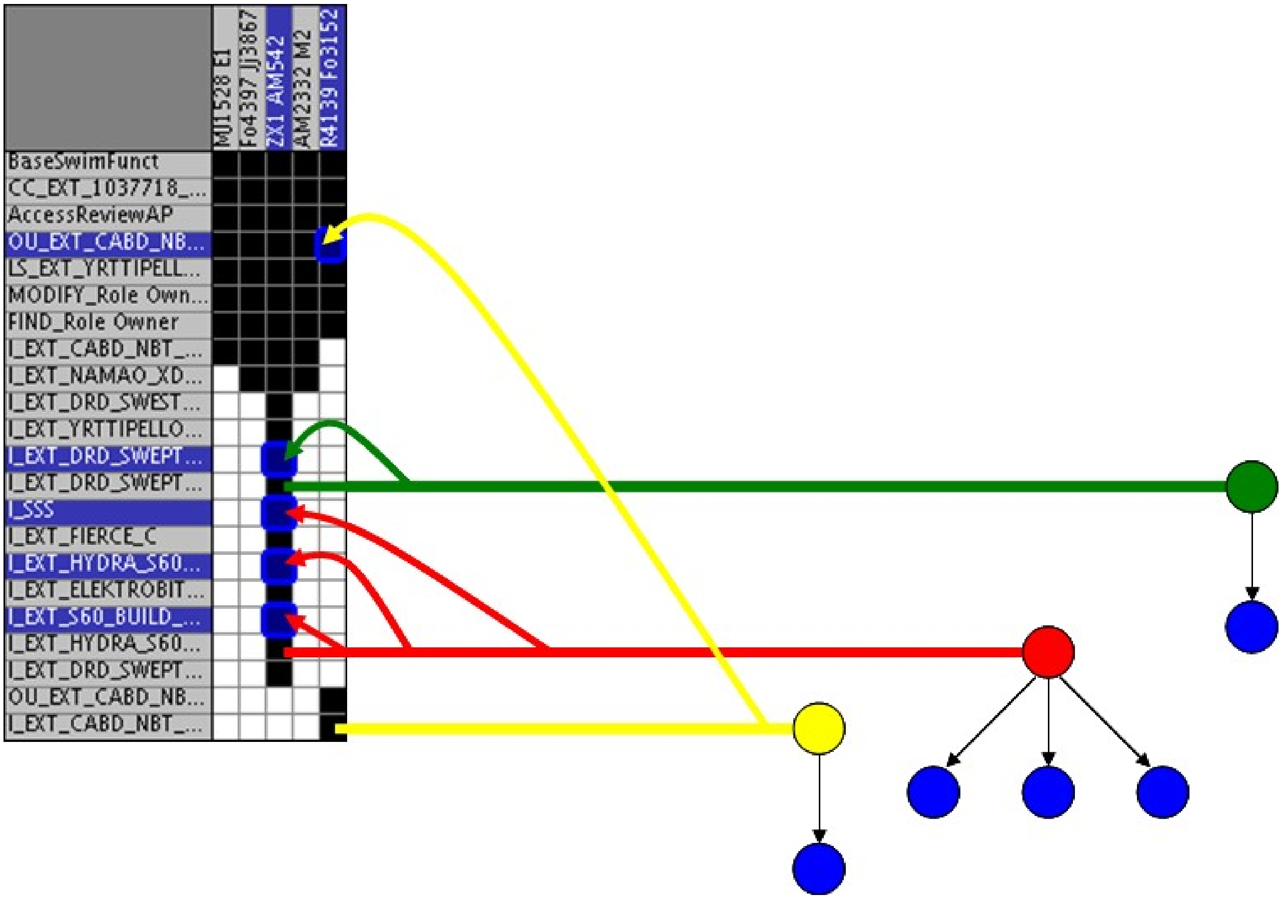


Figure 85. Blue entitlements inherited from others (Yellow, red and green entitlements)

Positioning the mouse pointer on a box outlined in blue triggers a dedicated tooltip which highlights the position coordinates and identifies the parent entitlement, in the form:

User: User name, user surname [User code]

Entitlement: Entitlement name | Entitlement type | Application name

Inherited from: Parent entitlement name | Parent entitlement type | Parent application name

The figure above contains five blue entitlements.

One entitlement has a yellow parent and one a green parent.

The three remaining blue entitlements are all inherited from a red parent.

The creation of the blue spotted map is enabled/disabled by a dedicated check box.

Only direct assignments are available for the following algorithms:

- Data exploration
- Entitlement clusters

If the check box is selected, only direct assignments are investigated and a map without blue spots is generated.

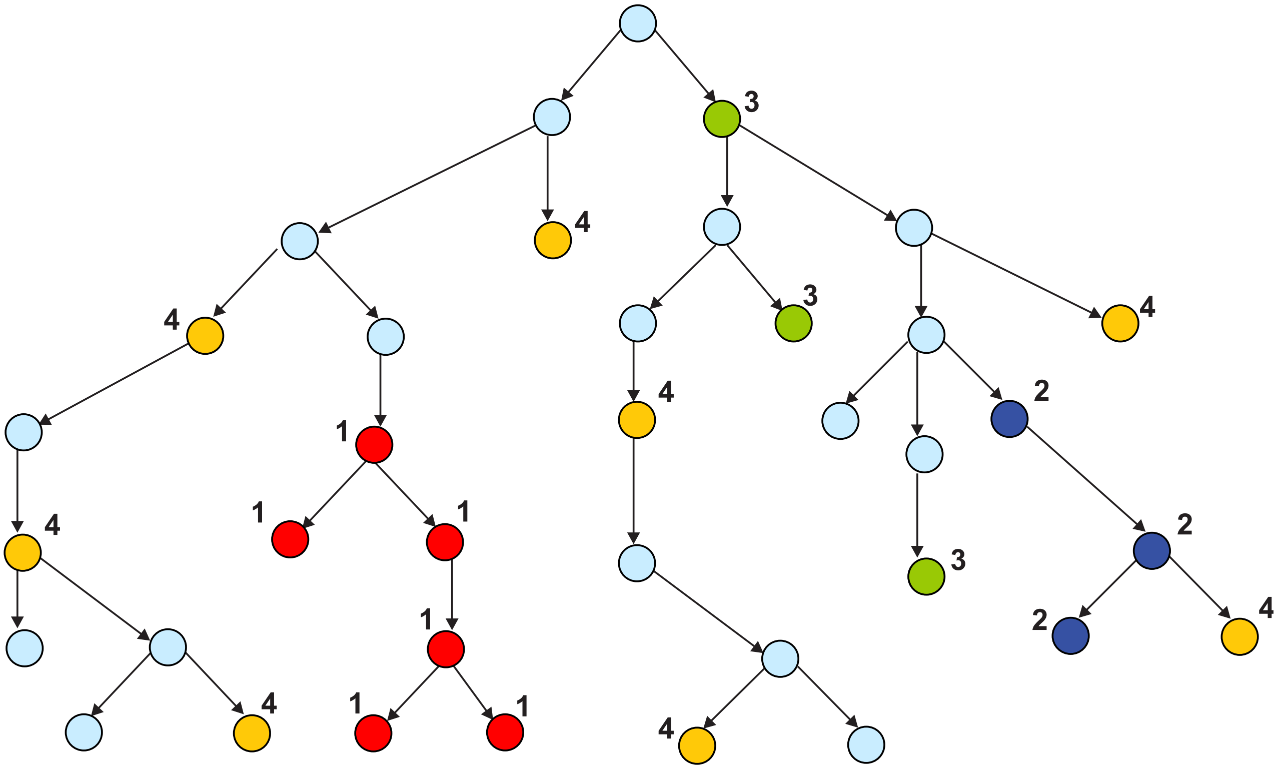
Spread

Spread is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization.

This index has 0 as minimum value and no maximum value. It can be considered as the statistical variance of Farness.

Use this index to find a correlation between a role and its position in the hierarchy of the organization under consideration.

The following example better explains this concept. The next figure shows the subtree of an organizational hierarchy where role `Role 1` is present in the root OU of the subtree and in all its other OUs.



Spread1 = 0 < Spread2 < Spread3 < < Spread4

Figure 86. Organization hierarchy: Spread.

In this scenario, where `Role 1` is limited to a specific subtree, it is very likely that `Role 1` is significant only for the users who belong to that subtree. In this case, `Role 1` is characterized by a spread value equal to 0.

Consider, for example, the `PHOTOSHOP_EXPERT` role. It is reasonable to think that in the `Graphic&WebDesigner` organization unit, this role has 0 spread.

If the spread value of a role is very high, the role is not homogeneously scattered over a large number of OUs. In the figure, the spread of `Role 4` is very high because `Role 4` is associated with users that are not homogeneously scattered throughout the organization tree. This does not provide useful information about the significance of `Role 4`. In other words, if this role was assigned randomly, no interesting conclusions can be drawn about its actual value in relation to the OUs where it is found, nor in relation to the users registered in these OUs.

`Role 2` shows a distribution similar to `Role 1`, but is not present in any of the OUs of the subtree under consideration. Its spread value is likely greater than 0, so that spread 2 > spread 1 = 0

`Role 3` has a fairly heterogeneous distribution within the right subtree. This indicates that spread 3 < spread 4, because `Role 4` has a heterogeneous distribution throughout the entire organization.

Therefore, if a role has a spread index equal to 0 (or almost 0) compared to a subtree of the organization hierarchy, there is a high concentration of users with that role in the subtree. Moreover, the role is probably "quite suitable" for the users of that subtree.

For example, role `INTERNET_ACCESS` is a default role that must be assigned to all users. In this case, the spread is 0 because, since the role is assigned to all users, it is homogeneously distributed over all the OUs of the organization.

Note: The spread index can be calculated for every attribute distributed in a hierarchical organization. It is not limited to candidate roles.

Farness

Farness is a numeric index that provides an estimate of the virtual distance between OUs having the same entitlement/candidate role. It can measure the distance between OUs in which different registered users are assigned the same entitlement/candidate role.

This index has 0 as its minimum value and no maximum value. It is calculated using the centroid of distribution of Organization units having a fixed entitlement/candidate role.

Calculate the Farness index to answer a question such as: Starting from a generic OU, how many moves are needed along the organization tree to reach the centroid of distribution based on the same entitlement/candidate role of the starting OU?

The following diagrams help explain this concept.

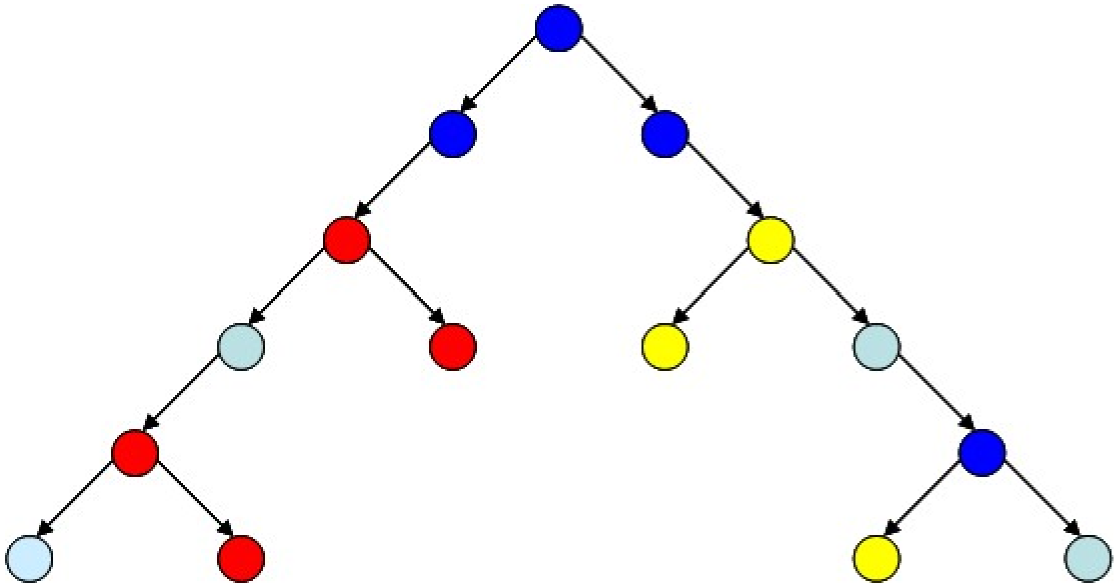


Figure 87. Farness: sample organization tree.

The nodes in this organization tree are colored in correspondence with different entitlements. Take the light-blue entitlement and find where the light-blue centroid of the tree is found.

In this very simple and symmetric tree, the centroid of distribution is easy to locate, as shown below:

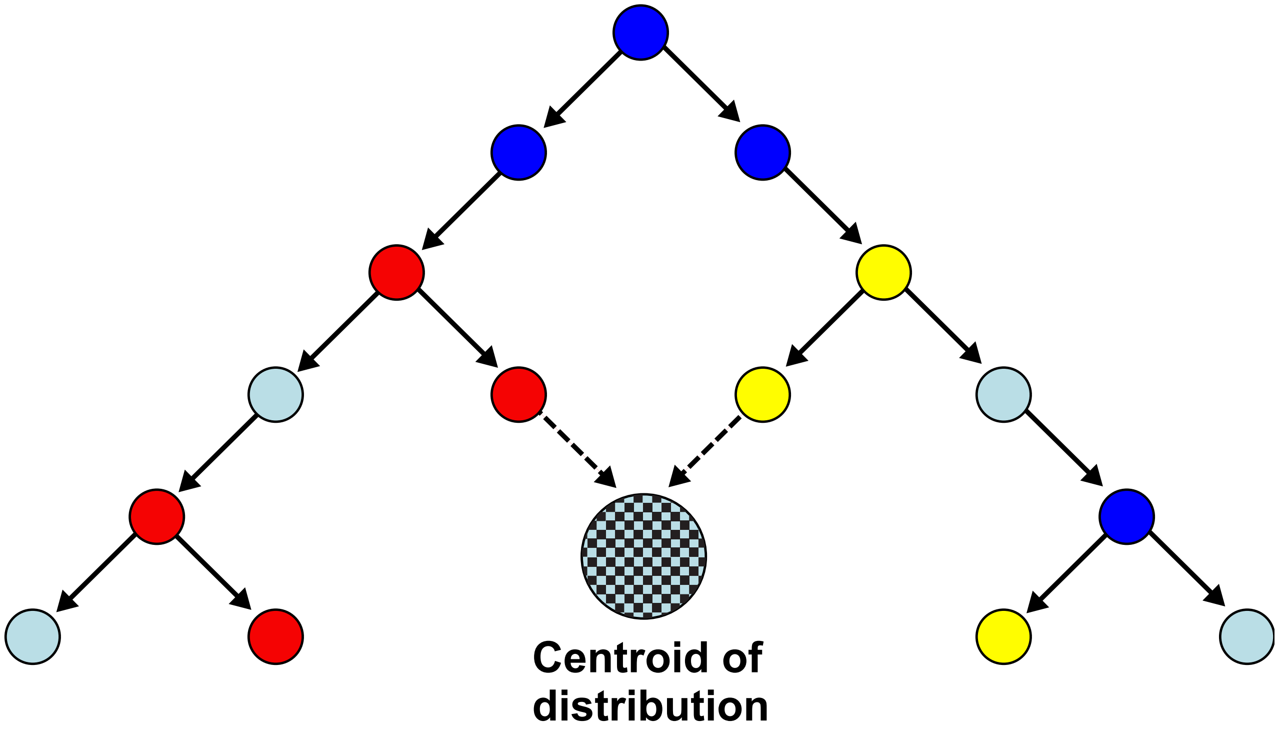


Figure 88. Farness: "virtual" centroid of distribution.

Note: The centroid is a virtual entity that can rarely be matched in a real OU.

After the centroid is located, the minimum farness - the shortest possible path from the generic OU to the centroid of the hierarchy - is easy to find. In the organization tree of the previous figure the minimum farness is equal to 3.

The example just shown is a very simplified scheme that is valid only when all OUs have the same number of users. When you try to locate a centroid of distribution, it is very important to acknowledge that different OUs may include very different amounts of users.

The next figure displays an unbalanced organization tree with many closely grouped and highly populated OUs (colored in blue) on the right side of the tree. This is a more realistic scenario.

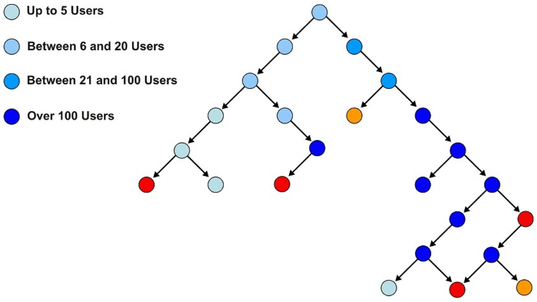


Figure 89. Farness: unbalanced distribution tree

A reasonable position for the virtual centroid of this distribution is:

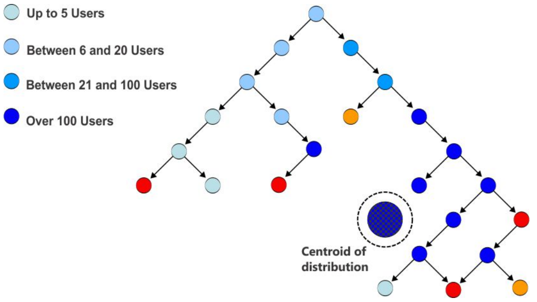


Figure 90. Farness: "virtual" centroid of the unbalanced distribution tree

After locating the centroid, you can calculate the minimum farness by finding the shortest path between the generic OU and the centroid for any blue family OU. The concept of Farness relates to the concept of Spread. Spread is the variance of the farness values calculated for all the involved OUs .

In other words, calculating farness means calculating the distance between an OU and the centroid of the hierarchy, rather than between an OU and a specific attribute such as an entitlement or a candidate role. Spread identifies the diffusion of that attribute throughout the entire hierarchy.

Maps

The visual map of roles and risks is described.

The Identity Governance and Intelligence model uses a "visual map" layout to represent:

- Entitlement-user assignments
- Levels of risk present in entitlement-user assignments

Do become familiar with this visual support before you start working with the Access Optimizer functions, which are all based on the visual map paradigm.

- Role Map
- Map
- Map Management

Role map

A role map represents entitlement-user assignments.

Good familiarity with role maps is required to:

- Investigate the set of results calculated by the role mining engine.
- Be able to best modify the input data to refine the obtained results set.

The following is an example of a Role map:

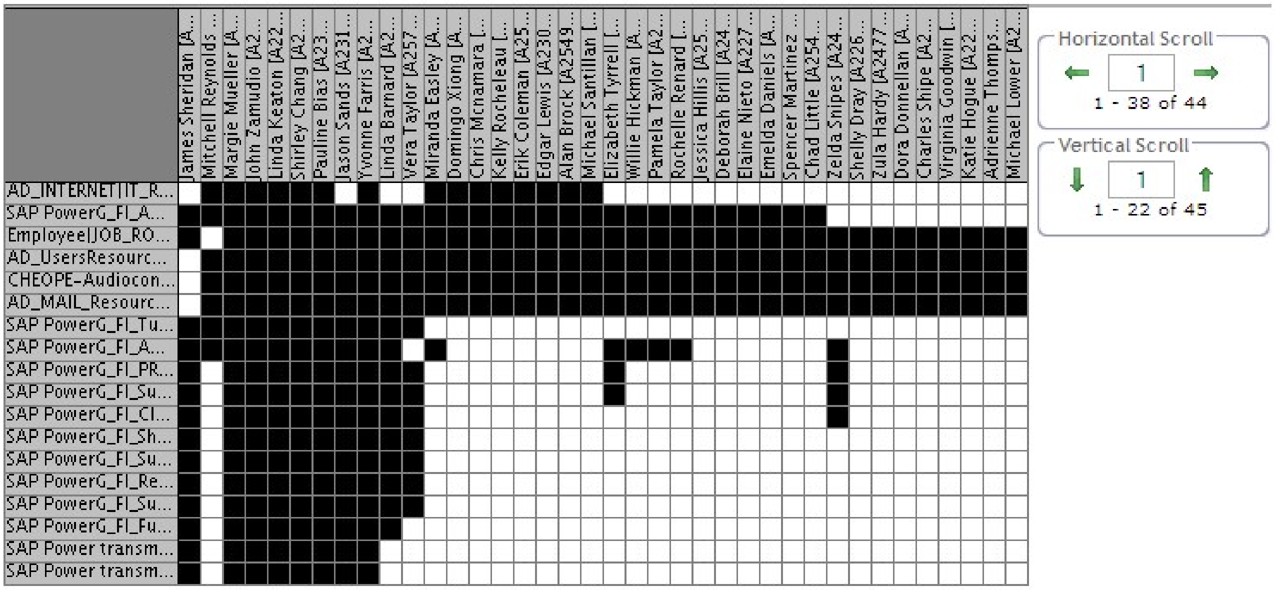


Figure 91. Role map example.

In the map, the vertical axis shows the entitlements whereas the horizontal axis shows the users. The black boxes show when an entitlement is assigned to a user.

If the map is too large to be displayed entirely, use the **Horizontal**/**Vertical** scrolls, on the right side of the map.

To navigate the map, either click the arrows (⬅ /➡ or/and ⬇ / ⬆), or write the desired number directly in the text area and then click the arrows.

Although not all the possible configuration maps can be covered, the more significant role maps are described in the next sections:

- Default Role

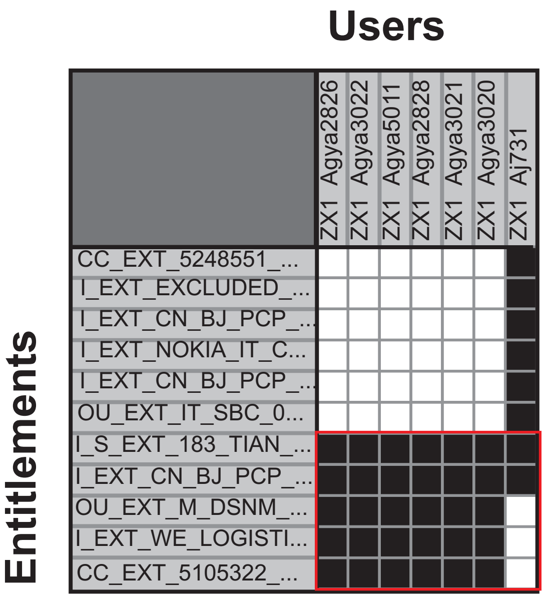
- Candidate Roles
- Select Area on the Map
- Exception/Missing filters
- Searching "Out Roles" in the Map
- Zoom on the Map

Default Role

A `Default Role` is automatically assigned to all the users of a specific OU.

For example, if in an OU characterized by N entitlements and M users a number of K entitlements is assigned to all M Users, these K Entitlements can indicate a Default Role that can be assigned to all the users of that OU.

In the following map, the same five entitlements are assigned to all the users (7) of the Organization unit.

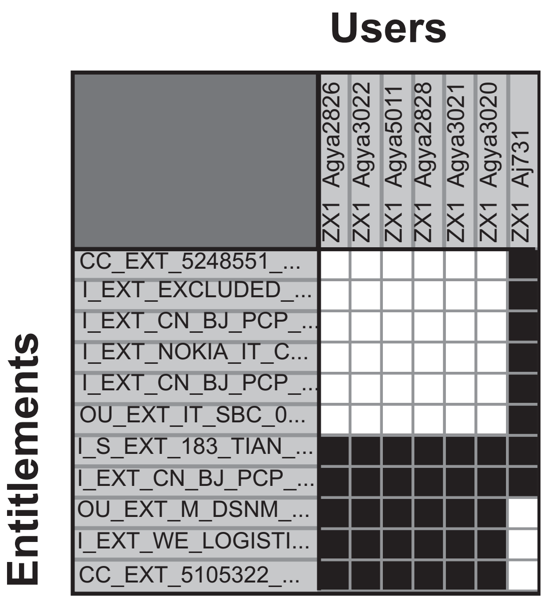


	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 Aj731
CC_EXT_5248551_...	□	□	□	□	□	□	■
I_EXT_EXCLUDED_...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
I_EXT_NOKIA_IT_C...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
OU_EXT_IT_SBC_0...	□	□	□	□	□	□	■
I_S_EXT_183_TIAN_...	■	■	■	■	■	■	■
I_EXT_CN_BJ_PCP_...	■	■	■	■	■	■	■
OU_EXT_M_DSNM_...	■	■	■	■	■	■	□
I_EXT_WE_LOGISTI...	■	■	■	■	■	■	□
CC_EXT_5105322_...	■	■	■	■	■	■	□

Figure 92. A default Role configuration.

The resulting 35 distinct assignments (black boxes) are outlined by the red rectangle. This configuration strongly suggests creating a default role that includes these five entitlements.

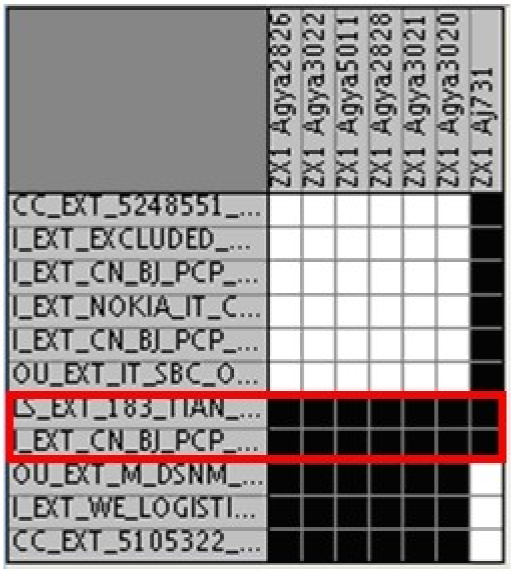
The next map presents a similar situation but the last user is assigned only two of the five entitlements.



	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 Aj731
CC_EXT_5248551_...	□	□	□	□	□	□	■
I_EXT_EXCLUDED_...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
I_EXT_NOKIA_IT_C...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
OU_EXT_IT_SBC_0...	□	□	□	□	□	□	■
I_S_EXT_183_TIAN_...	■	■	■	■	■	■	■
I_EXT_CN_BJ_PCP_...	■	■	■	■	■	■	■
OU_EXT_M_DSNM_...	■	■	■	■	■	■	□
I_EXT_WE_LOGISTI...	■	■	■	■	■	■	□
CC_EXT_5105322_...	■	■	■	■	■	■	□

Figure 93. Missing Entitlements configuration.

This leads to the definition of a different default role that includes only the two entitlements the users have in common.



	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 Aj731
CC_EXT_5248551_...	□	□	□	□	□	□	■
I_EXT_EXCLUDED_...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
I_EXT_NOKIA_IT_C...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
OU_EXT_IT_SBC_O...	□	□	□	□	□	□	■
I_S_EXT_183_TIAN_...	■	■	■	■	■	■	■
I_EXT_CN_BJ_PCP_...	■	■	■	■	■	■	■
OU_EXT_M_DSNM_...	■	■	■	■	■	■	□
I_EXT_WE_LOGISTI...	■	■	■	■	■	■	□
CC_EXT_5105322_...	■	■	■	■	■	■	□

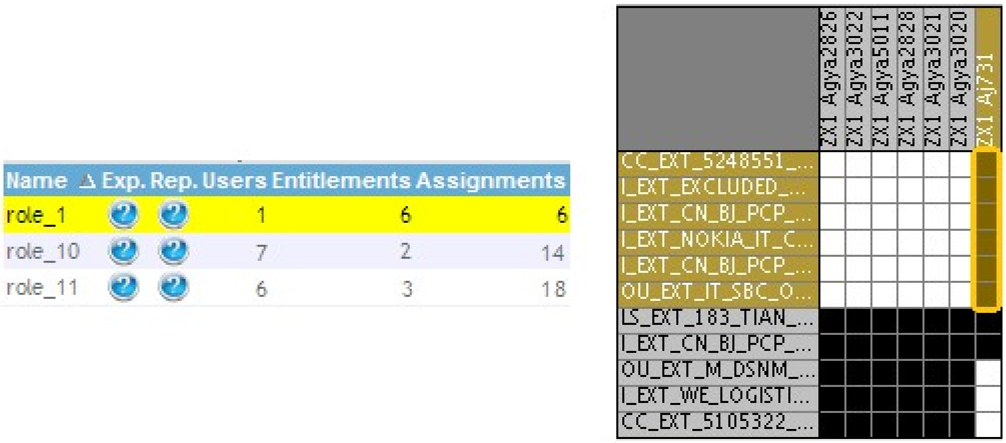
Figure 94. Another Default Role configuration.

Candidate Roles

The Role Mining analysis output is generally built on a set of "Candidate Roles" represented by the black/white box combinations in the map.

The next three figures show examples of output yielded by three Candidate Roles.

The first Candidate Role is shown below:



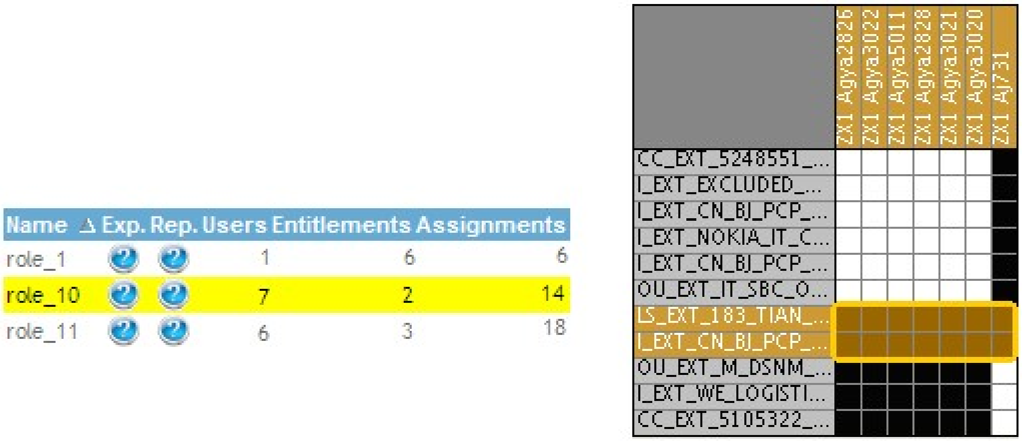
Name ▵	Exp.	Rep.	Users	Entitlements	Assignments
role_1	?	?	1	6	6
role_10	?	?	7	2	14
role_11	?	?	6	3	18

	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 Aj731
CC_EXT_5248551_...	□	□	□	□	□	□	▨
I_EXT_EXCLUDED_...	□	□	□	□	□	□	▨
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	▨
I_EXT_NOKIA_IT_C...	□	□	□	□	□	□	▨
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	▨
OU_EXT_IT_SBC_O...	□	□	□	□	□	□	▨
LS_EXT_183_TIAN_...	■	■	■	■	■	■	■
I_EXT_CN_BJ_PCP_...	■	■	■	■	■	■	■
OU_EXT_M_DSNM_...	■	■	■	■	■	■	□
I_EXT_WE_LOGISTI...	■	■	■	■	■	■	□
CC_EXT_5105322_...	■	■	■	■	■	■	□

Figure 95. Candidate Role n° 1.

In this case, a specific Candidate Role built on 6 Entitlements is shaded in brown and can be assigned to only one User.

The second Candidate Role is shown below:



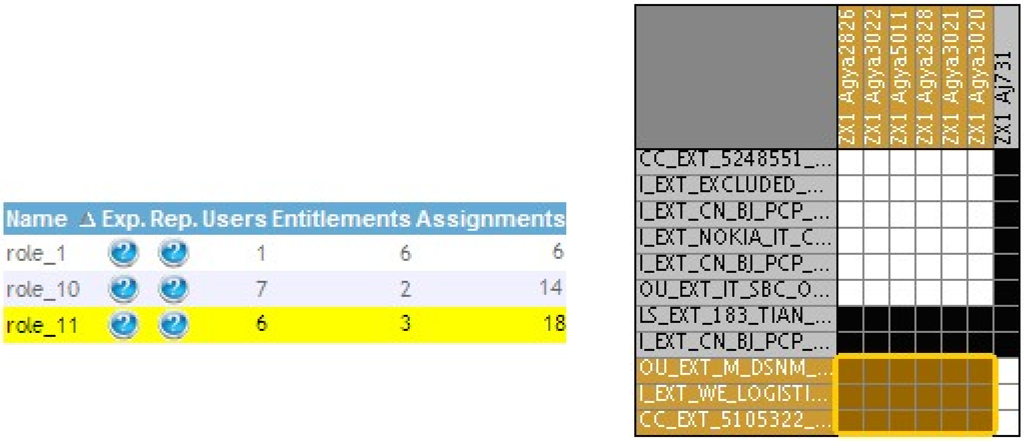
Name ▵	Exp.	Rep.	Users	Entitlements	Assignments
role_1	?	?	1	6	6
role_10	?	?	7	2	14
role_11	?	?	6	3	18

	ZX1 Agya2826	ZX1 Agya3022	ZX1 Agya5011	ZX1 Agya2828	ZX1 Agya3021	ZX1 Agya3020	ZX1 Aj731
CC_EXT_5248551_...	□	□	□	□	□	□	■
I_EXT_EXCLUDED_...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
I_EXT_NOKIA_IT_C...	□	□	□	□	□	□	■
I_EXT_CN_BJ_PCP_...	□	□	□	□	□	□	■
OU_EXT_IT_SBC_O...	□	□	□	□	□	□	■
LS_EXT_183_TIAN_...	▨	▨	▨	▨	▨	▨	▨
I_EXT_CN_BJ_PCP_...	▨	▨	▨	▨	▨	▨	▨
OU_EXT_M_DSNM_...	■	■	■	■	■	■	□
I_EXT_WE_LOGISTI...	■	■	■	■	■	■	□
CC_EXT_5105322_...	■	■	■	■	■	■	□

Figure 96. Candidate Role n° 2.

This case involves 14 assignments, with two Entitlements assigned TO ALL CONSIDERED USERS. This can be a Default Role, even if the Role is only composed of two Entitlements.

The third Candidate Role is shown below:



Name △	Exp.	Rep.	Users	Entitlements	Assignments
role_1	?	?	1	6	6
role_10	?	?	7	2	14
role_11	?	?	6	3	18

Figure 97. Candidate Role n° 3.

This can be considered a very common situation, in which K of N (K<N) Entitlements are assigned to H of M (H<M) Users. In this case, 3 of 11 Entitlements are assigned (brown area) to 6 of 7 Users.

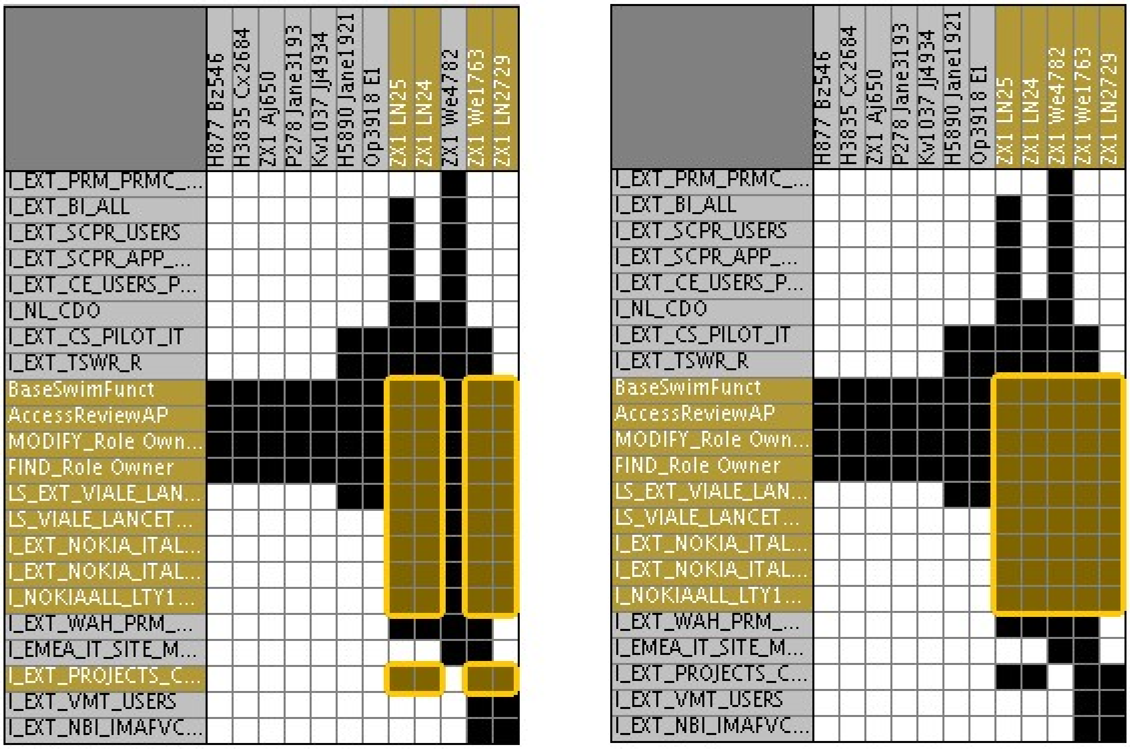


Figure 98. Two more examples of Candidate Roles.

The preceding figure shows an example of two other Candidate Roles.

In the "L" configuration below, 8 Entitlements and 4201 Users are displayed. The first two Entitlements are assigned to ALL 4201 Users, while the other six are assigned only to the first two Users. You can scroll the right side of the Map to view all the other assignments.

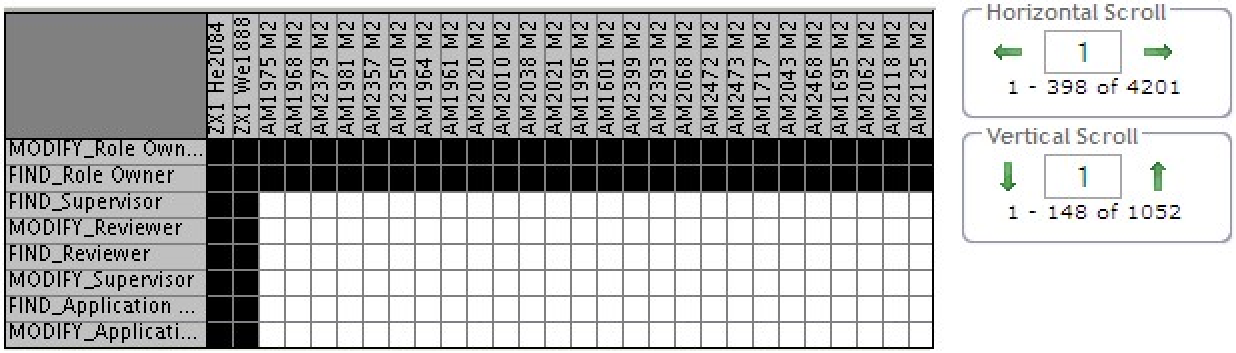


Figure 99. "L" Map.

The Map resolution can always be adjusted using the zoom buttons (**Zoom In**/**Zoom Out**) (see Map management/functionality).

Note: When moving the mouse pointer to a specific position on the Map, a dedicated tooltip appears, highlighting the position's coordinates in the form:

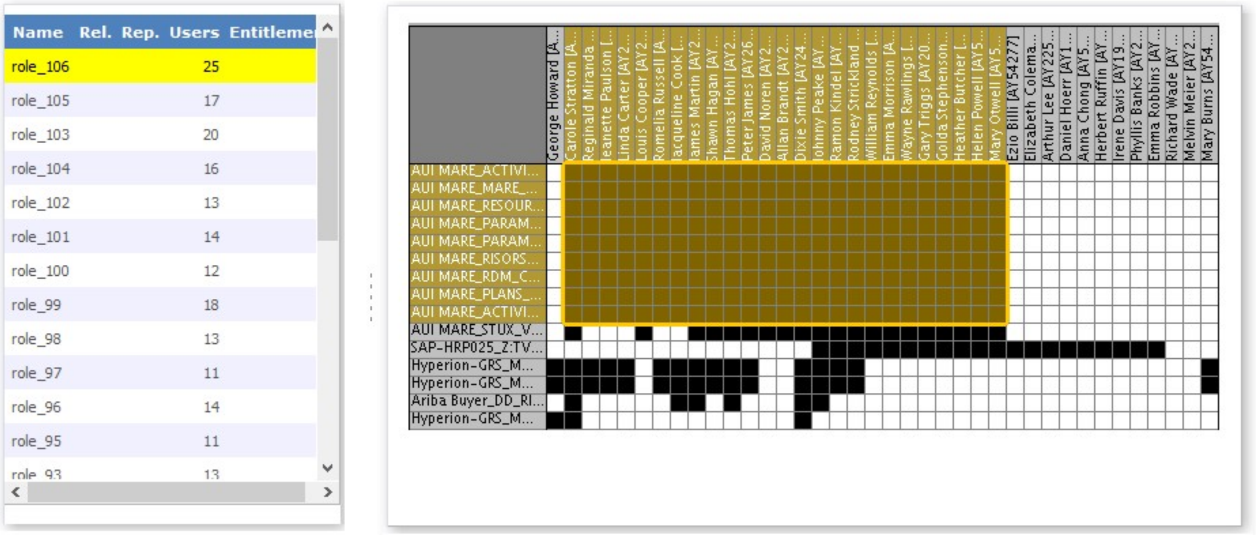
User : User name | User surname [User code]

Entitlement : Entitlement name | Entitlement type | Application name

Select Area on the Map

You can analyze user entitlement assignments

One of the approaches to analyze the User-Entitlement assignment, is the selection of an area on the Map.



Name	Rel.	Rep.	Users	Entitleme
role_106			25	
role_105			17	
role_103			20	
role_104			16	
role_102			13	
role_101			14	
role_100			12	
role_99			18	
role_98			13	
role_97			11	
role_96			14	
role_95			11	
role_93			13	

Figure 100. Selection of an area on the Map.

In the figure above is displayed a generic example of the select area operation; this operation is possible by the **Select Area** button.

When the selected area corresponds to a specific Role, in the **Role Search** frame (left), automatically the Role is highlighted in light orange. This feature, make possible to easily identify the Roles already defined.

Another possibility that offer this feature is the easily reorganization of the black blocks in the Map, as shown in the figure below:

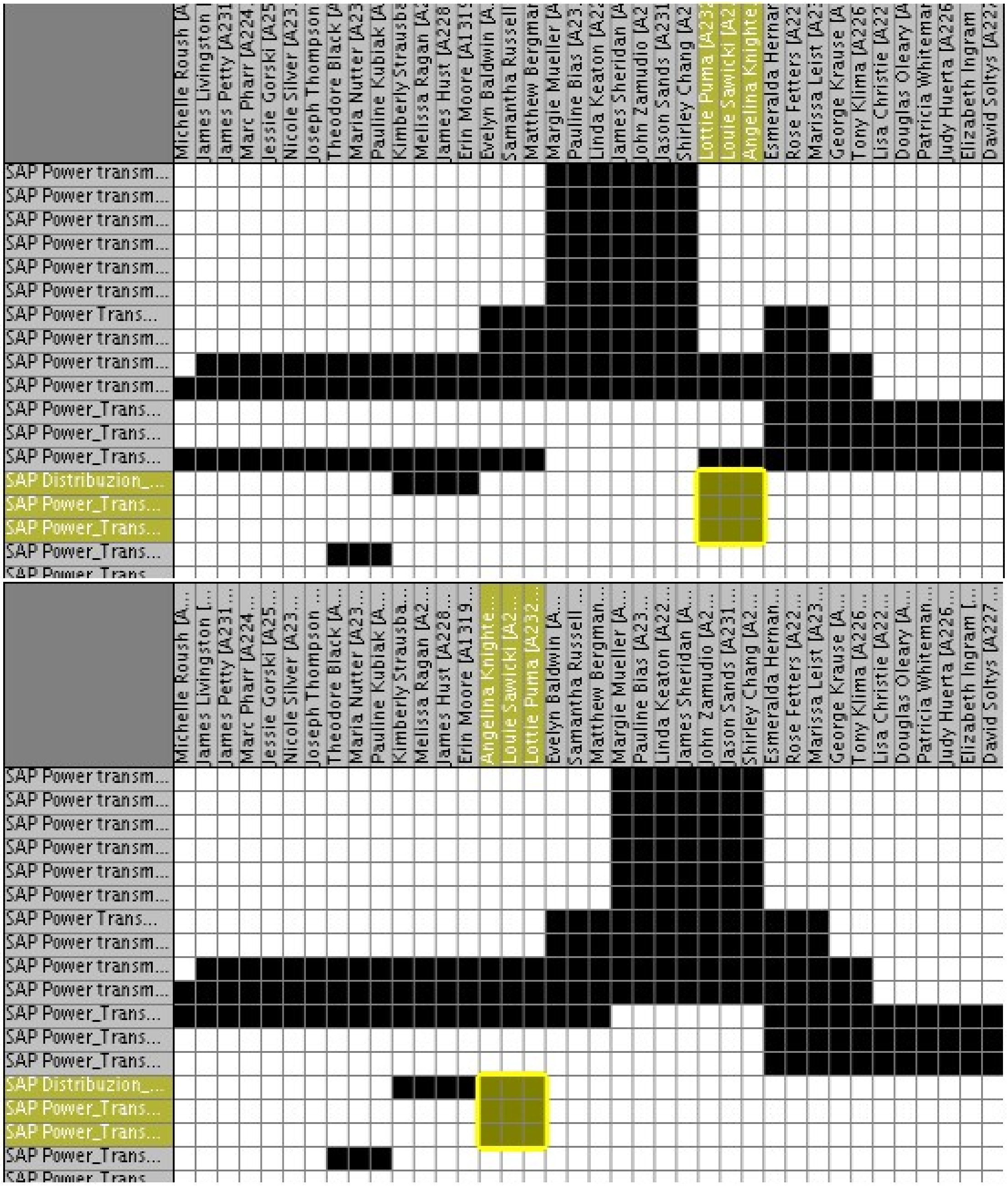


Figure 101. Selection of an area and reorganization of it on the Map.

In the figure above, the map has been reorganized based on the selection of the highlighted blocks (Select Area). In this way, the map is built around the Role highlighted.

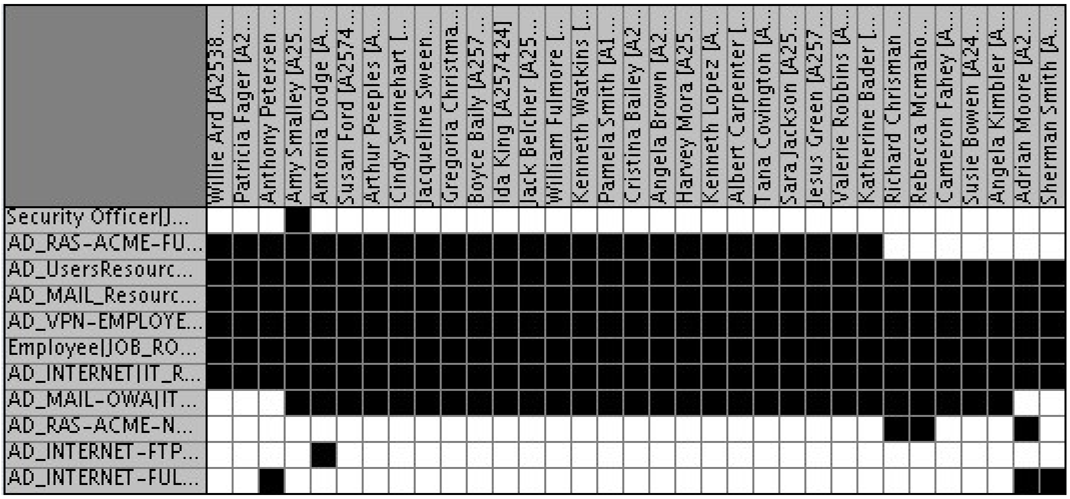
If it is decided to select one other area and then reorganize again, the map will change again and so on. This operation is possible, after selecting the area, by clicking the **Reshuffle** button.

This feature does not compromise the original meaning of the Map, but allows the Administrator to visualize the different organizations of the existing Roles. It is possible to group not only the black blocks in an area, but also the white blocks. This operation permits you to use the **Exceptions**/**Missing** filters.

Exeption and Missing filters

The Exception/Missing assignments analysis is one of the graphic analysis approaches available; they can be considered a "noise analysis" aimed at reaching the "core" assignments by either erasing a subset of "weak assignments" (Exception filter) or adding a subset of "interesting assignments" (Missing filter).

A generic Role Map is shown in the figure below:



	Willie Ard [A2538...	Patricia Fager [A2...	Anthony Petersen ...	Amy Smalley [A25...	Antonia Dodge [A...	Susan Ford [A2574...	Arthur Peeples [A...	Cindy Swinehart [...	Jacqueline Sween...	Gregoria Christma...	Boyce Baily [A257...	Ida King [A257424]	Jack Belcher [A25...	William Fulmore [...	Kenneth Watkins [...	Pamela Smith [A1...	Cristina Bailey [A2...	Angela Brown [A2...	Harvey Mora [A25...	Kenneth Lopez [A...	Albert Carpenter [...	Tana Covington [A...	Sara Jackson [A25...	Jesus Green [A257...	Valerie Robbins [A...	Katherine Bader [...	Richard Chrisman ...	Rebecca Mcmaho...	Cameron Fahey [A...	Susie Bowen [A24...	Angela Kimbler [A...	Adrian Moore [A2...	Sherman Smith [A...
Security Officer|J...				■																													
AD_RAS-ACME-FU...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■							
AD_UsersResourc...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_MAIL_Resourc...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_VPN-EMPLOYE...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Employee|JOB_RO...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_INTERNET|IT_R...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_MAIL-OWA|IT...				■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		
AD_RAS-ACME-N...																											■	■				■	
AD_INTERNET-FTP...					■																												
AD_INTERNET-FUL...			■																													■	■

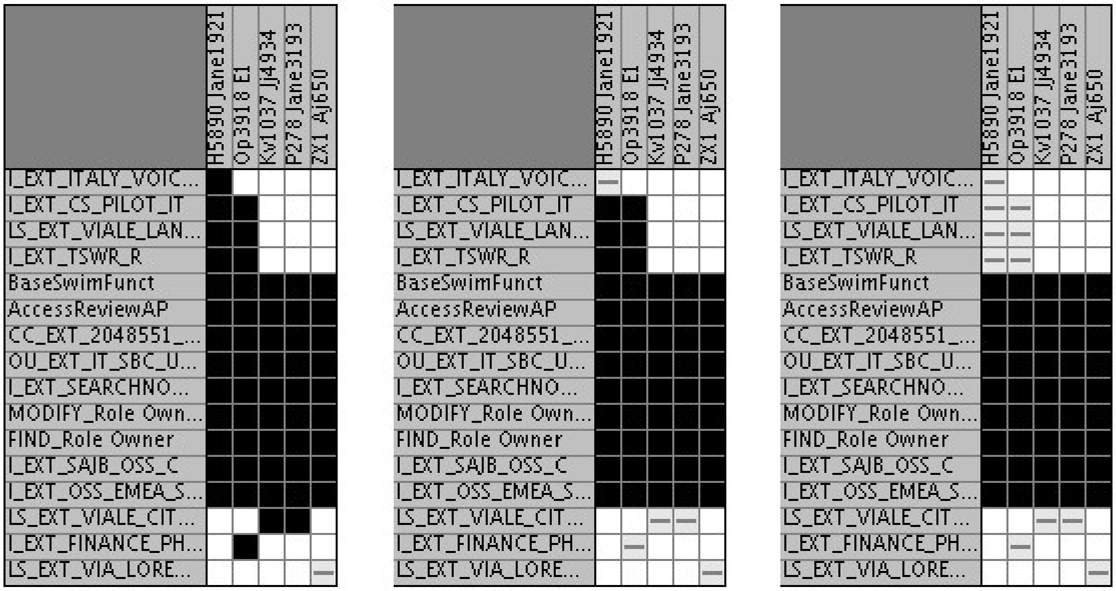
Figure 102. Exceptions Role analysis.

There are two distinct scroll in the upper portion of the **Role Map** frame; the **Exceptions** scroll on the left and the **Missing** scroll on the right.

The **Exceptions** scroll provides a dynamic filter to identify assignments which are more "uneven" and "dissimilar" in relation to the starting Role Map.

Using the ⊟ symbol to change the scroll value (from 0 to 100), or writing in the text area the desired exceptions number and clicking the up/down arrow (automatic Exception), shows the "peripheral" assignments in the Role Map configuration. It could be more efficient to segregate such assignments into a well defined Role rather than in the "core zone" of the Map, where "well aggregated" assignments are concentrated.

Thus, assignments which are possibly more efficient segregate into a well-defined Role rather than into the Map's "core zone" concentrated, "well-aggregated" assignments having low red levels ("weak" red).



	H5890 Jane1921	Op3918 E1	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	■				
I_EXT_CS_PILOT_IT	■	■			
LS_EXT_VIALE_LAN...	■	■			
I_EXT_TSWR_R	■	■			
BaseSwimFunct	■	■	■	■	■
AccessReviewAP	■	■	■	■	■
CC_EXT_2048551_...	■	■	■	■	■
OU_EXT_IT_SBC_U...	■	■	■	■	■
I_EXT_SEARCHNO...	■	■	■	■	■
MODIFY_Role Own...	■	■	■	■	■
FIND_Role Owner	■	■	■	■	■
I_EXT_SAJB_OSS_C	■	■	■	■	■
I_EXT_OSS_EMEA_S...	■	■	■	■	■
LS_EXT_VIALE_CIT...			■	■	
I_EXT_FINANCE_PH...		■			
LS_EXT_VIA_LORE...					—

	H5890 Jane1921	Op3918 E1	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	—				
I_EXT_CS_PILOT_IT	■	■			
LS_EXT_VIALE_LAN...	■	■			
I_EXT_TSWR_R	■	■			
BaseSwimFunct	■	■	■	■	■
AccessReviewAP	■	■	■	■	■
CC_EXT_2048551_...	■	■	■	■	■
OU_EXT_IT_SBC_U...	■	■	■	■	■
I_EXT_SEARCHNO...	■	■	■	■	■
MODIFY_Role Own...	■	■	■	■	■
FIND_Role Owner	■	■	■	■	■
I_EXT_SAJB_OSS_C	■	■	■	■	■
I_EXT_OSS_EMEA_S...	■	■	■	■	■
LS_EXT_VIALE_CIT...			—	—	
I_EXT_FINANCE_PH...		—			
LS_EXT_VIA_LORE...					—

	H5890 Jane1921	Op3918 E1	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	—				
I_EXT_CS_PILOT_IT	—	—			
LS_EXT_VIALE_LAN...	—	—			
I_EXT_TSWR_R	—	—			
BaseSwimFunct	■	■	■	■	■
AccessReviewAP	■	■	■	■	■
CC_EXT_2048551_...	■	■	■	■	■
OU_EXT_IT_SBC_U...	■	■	■	■	■
I_EXT_SEARCHNO...	■	■	■	■	■
MODIFY_Role Own...	■	■	■	■	■
FIND_Role Owner	■	■	■	■	■
I_EXT_SAJB_OSS_C	■	■	■	■	■
I_EXT_OSS_EMEA_S...	■	■	■	■	■
LS_EXT_VIALE_CIT...			—	—	
I_EXT_FINANCE_PH...		—			
LS_EXT_VIA_LORE...					—

Figure 103. Exception Role analysis: three distinct values.

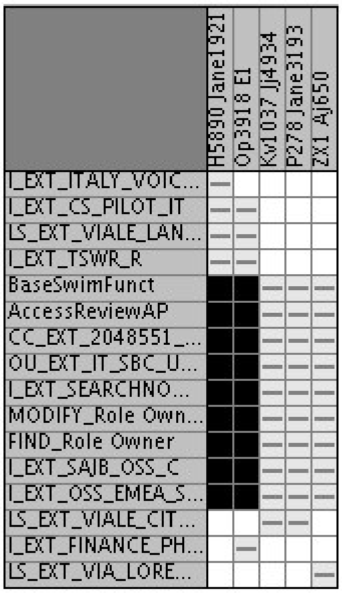
In the above figure, three distinct values of the **Exceptions** scroll are shown from left to right.

In the left column of the above figure (Exception =10) only one assignment is highlighted in the bottom-right corner of the Map. Those isolated assignments are clearly suitable to be collapsed into a single Entitlement Role.

More assignments are shown by Exception =20.

Exception =50 shows assignments outside the main black-box rectangle -- separate from the ideal "Default Role".

What happens if Exception =100? The result is shown in the next figure:



	H5890 Jane1921	Op3918 El	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	—				
I_EXT_CS_PILOT_IT	—	—			
LS_EXT_VIALE_LAN...	—	—			
I_EXT_TSWR_R	—	—			
BaseSwimFunct	■	■	—	—	—
AccessReviewAP	■	■	—	—	—
CC_EXT_2048551_...	■	■	—	—	—
OU_EXT_IT_SBC_U...	■	■	—	—	—
I_EXT_SEARCHNO...	■	■	—	—	—
MODIFY_Role Own...	■	■	—	—	—
FIND_Role Owner	■	■	—	—	—
I_EXT_SAJB_OSS_C	■	■	—	—	—
I_EXT_OSS_EMEA_S...	■	■	—	—	—
LS_EXT_VIALE_CIT...			—	—	
I_EXT_FINANCE_PH...		—			
LS_EXT_VIA_LORE...					—

Figure 104. Exception Role analysis: the "black core" of the Candidate Role.

How must this Map be interpreted?

This is the "core" of the Map where the most meaningful assignments are concentrated.

The RC engine seems to suggest this particular Role, which includes the same Entitlements as the Default Role, but differs in the fact that it is assigned only to two Users. It is quite evident that Exception =100 results in a Candidate Role covering fewer Users than the Exception =50 option.

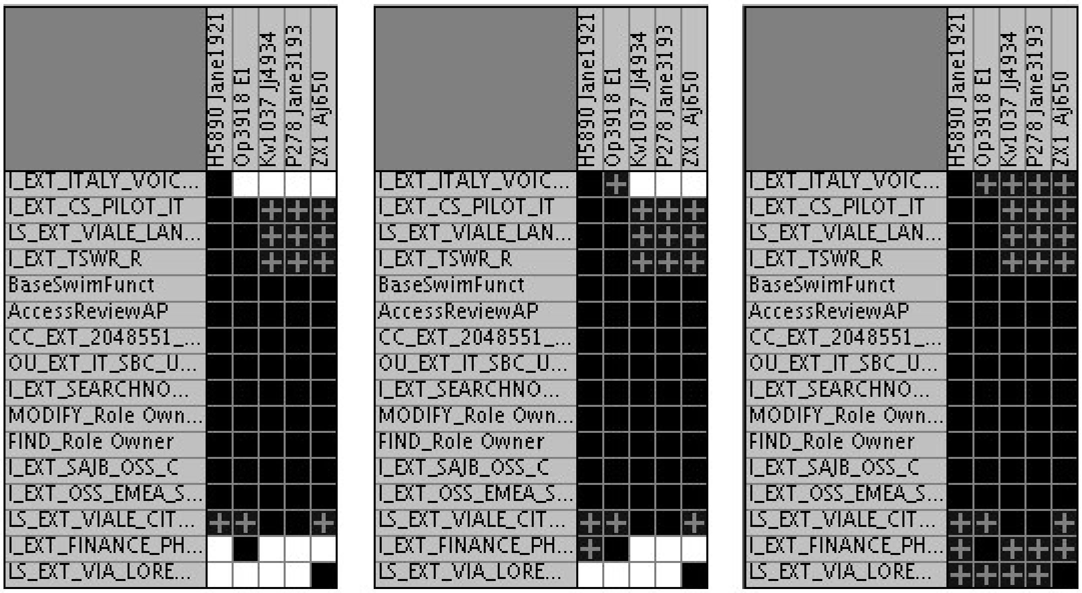
The same effect will be obtained by directly selecting a black assignment (clicking on it with the left mouse button) and clicking on the — **Remove Assignments** button.

Considering the "noise" concept mentioned earlier, erasing too much noise (high Exception index value), poses the risk of also erasing a lot of good signal!

The figure on the next page provides a qualitative description of this mechanism using the **Exception** index values.

The **Missing** scroll provides a dynamic filter to identify assignments that are "closer" and more "alike" in relation to the starting Role Map.

Using the ⊞ symbol to change the scroll value (from 0 to 100) or writing in the text area the desired exceptions number and clicking the up/down arrow (automatic Missing), shows assignments that are "closer" to the Role Map configuration. It would probably be useful to add such assignments to the "core zone" of the Map where there is a "well aggregated" concentration of assignments.



	H5890 Jane1921	Op3918 E1	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	■	□	□	□	□
I_EXT_CS_PILOT_IT	■	■	+	+	+
LS_EXT_VIALE_LAN...	■	■	+	+	+
I_EXT_TSWR_R	■	■	+	+	+
BaseSwimFunct	■	■	■	■	■
AccessReviewAP	■	■	■	■	■
CC_EXT_2048551_...	■	■	■	■	■
OU_EXT_IT_SBC_U...	■	■	■	■	■
I_EXT_SEARCHNO...	■	■	■	■	■
MODIFY_Role Own...	■	■	■	■	■
FIND_Role Owner	■	■	■	■	■
I_EXT_SAJB_OSS_C	■	■	■	■	■
I_EXT_OSS_EMEA_S...	■	■	■	■	■
LS_EXT_VIALE_CIT...	+	+	■	■	+
I_EXT_FINANCE_PH...	□	■	□	□	□
LS_EXT_VIA_LORE...	□	□	□	□	■

	H5890 Jane1921	Op3918 E1	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	■	+	□	□	□
I_EXT_CS_PILOT_IT	■	■	+	+	+
LS_EXT_VIALE_LAN...	■	■	+	+	+
I_EXT_TSWR_R	■	■	+	+	+
BaseSwimFunct	■	■	■	■	■
AccessReviewAP	■	■	■	■	■
CC_EXT_2048551_...	■	■	■	■	■
OU_EXT_IT_SBC_U...	■	■	■	■	■
I_EXT_SEARCHNO...	■	■	■	■	■
MODIFY_Role Own...	■	■	■	■	■
FIND_Role Owner	■	■	■	■	■
I_EXT_SAJB_OSS_C	■	■	■	■	■
I_EXT_OSS_EMEA_S...	■	■	■	■	■
LS_EXT_VIALE_CIT...	+	+	■	■	+
I_EXT_FINANCE_PH...	+	■	□	□	□
LS_EXT_VIA_LORE...	□	□	□	□	■

	H5890 Jane1921	Op3918 E1	Kv1037 Jj4934	P278 Jane3193	ZX1 Aj650
I_EXT_ITALY_VOIC...	■	+	+	+	+
I_EXT_CS_PILOT_IT	■	■	+	+	+
LS_EXT_VIALE_LAN...	■	■	+	+	+
I_EXT_TSWR_R	■	■	+	+	+
BaseSwimFunct	■	■	■	■	■
AccessReviewAP	■	■	■	■	■
CC_EXT_2048551_...	■	■	■	■	■
OU_EXT_IT_SBC_U...	■	■	■	■	■
I_EXT_SEARCHNO...	■	■	■	■	■
MODIFY_Role Own...	■	■	■	■	■
FIND_Role Owner	■	■	■	■	■
I_EXT_SAJB_OSS_C	■	■	■	■	■
I_EXT_OSS_EMEA_S...	■	■	■	■	■
LS_EXT_VIALE_CIT...	+	+	■	■	+
I_EXT_FINANCE_PH...	+	■	+	+	+
LS_EXT_VIA_LORE...	+	+	+	+	■

Figure 105. Missing Role analysis: three distinct values.

Note: If the Map produced is too large, the automatic Exceptions/Missing modulation is not available.

In the above figure, three distinct values of the **Missing** scroll are shown from left to right.

In the left column of the above figure (Missing =55) nine assignments are highlighted in the upper portion of the Map and another three at the bottom of the Map.

With Missing =75, another two assignments are added without any significant changes in the quality of the solution when compared with the previous configuration.

With Missing =95, the entire Map goes black!

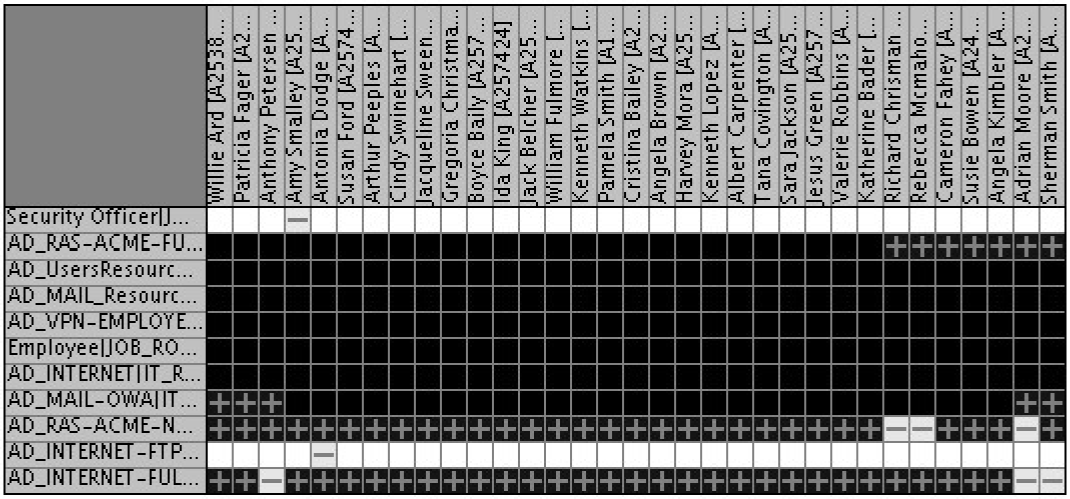
How must this Map set be interpreted?

To obtain an appreciable improvement over the starting configuration, the not so "near" assignments must be selected (Missing =>55).

Thus the advantage represented by a "heavier" Default Role (built with more Entitlements) has to be balanced by the need to consider assignments that probably are not very suitable for the Users considered.

The same effect will be obtained by directly selecting a white box (clicking on it with the left mouse button) and clicking on the **Fill up** button.

Using these two dynamic filters together, different values can be combined to obtain the mixed result shown in previous figures:



	Willie Ard [A2538...	Patricia Fager [A2...	Anthony Petersen ...	Amy Smalley [A25...	Antonia Dodge [A...	Susan Ford [A2574...	Arthur Peeples [A...	Cindy Swinehart [...	Jacqueline Sween...	Gregoria Christma...	Boyce Baily [A257 ...	Ida King [A257424]	Jack Belcher [A25...	William Fulmore [...	Kenneth Watkins [...	Pamela Smith [A1...	Cristina Bailey [A2...	Angela Brown [A2...	Harvey Mora [A25...	Kenneth Lopez [A...	Albert Carpenter [...	Tana Covington [A...	Sara Jackson [A25...	Jesus Green [A257...	Valerie Robbins [A...	Katherine Bader [...	Richard Chrisman ...	Rebecca Mcmaho...	Cameron Fahey [A...	Susie Bowen [A24...	Angela Kimbler [A...	Adrian Moore [A2...	Sherman Smith [A...
Security Officer|J...				−																													
AD_RAS-ACME-FU...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	+	+	+	+	+	+	+
AD_UsersResourc...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_MAIL_Resourc...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_VPN-EMPLOYE...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Employee|JOB_RO...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_INTERNET|IT_R...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_MAIL-OWA|IT...	+	+	+	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	+	+
AD_RAS-ACME-N...	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	−	−	+	+	+	−	+
AD_INTERNET-FTP...					−																												
AD_INTERNET-FUL...	+	+	−	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	−	−

Figure 106. Exception-Missing combined analysis.

The above figure illustrates the combination of Exception =55 and Missing =95.

It is impossible to apply a general rule for every situation. The best suggested practice is to use the **Exception/Missing** scrolls for small variations around the Map's "black core" and then recalculate the Request using the **New Request** button.

Note: To delete assignments (− symbol), means identifying Candidate Roles with fewer authorizations than the actual Roles in use, thus "less powerful Roles".

On the other hand, to add assignments (+ symbol) means identifying Candidate Roles with more authorizations than the actual Roles in use, thus "more powerful Roles".

In this last option, creating a more powerful Candidate Role implies the need for a new authorization workflow process once the Candidate Role is exported to the system.

Note: These functionalities must be used very carefully!

If too many assignments are deleted (− symbol) near the "core" of the map (see Figure 3.21) and too many assignments are added (+ symbol) to the same area of the map, a "conceptual mismatch" can occur, tending to overturn the result of the analysis!

The **Exception/Missing** scrolls MUST BE USED VERY CAREFULLY!

By deleting some assignments (− symbol in Figure 3.23) and invoking a New Request operation, the RC Engine generates a new Map. In this instance, using the same Missing index value as the original Map does not result in the same + distribution.

This means there is a dynamic and mutual relationship between both the presence and absence of ⊟ / ⊞ symbols.

CAUTION:
IF Exception = Missing = 1

... the result is the "negative" of the original Map (Exception = Missing = 0).

This is a situation of ALL "noise" and NO "signal"!

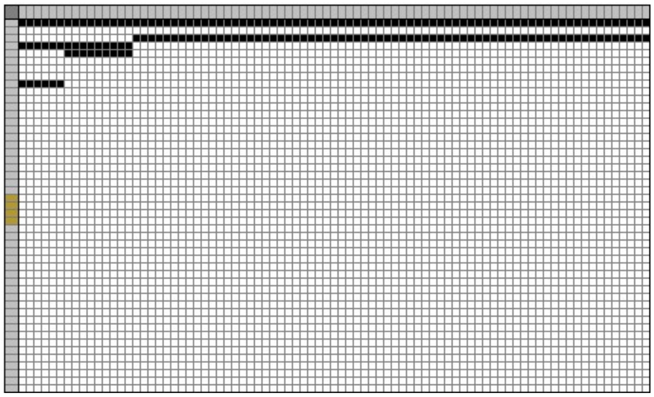
This is the worst case of all!

Searching "out Roles" in the Map

When the Role Map is built with a lot of Users and Entitlements it can be difficult to detect the graphic structure of a Role. For a very large Map, it is not always easy to recognize a Role by selecting it from the list in the left-hand frame. For example, in a map that has 375 Roles built on 1060 Entitlements and distributed on a set of 4204 Users.

Selecting a Role in the **Role Search** frame returns this fragment of the Map:

Table 231. Candidate Role

15 Users 4 Entitlements	

In this Map the position of the 4 Entitlements can be identified in the left-hand, vertical, gray column.

BUT WHERE ARE THE USERS?

Finding them requires some work with the horizontal scroll or, more easily, clicking on the Role Search button positioned on the upper-right toolbar of the GUI:

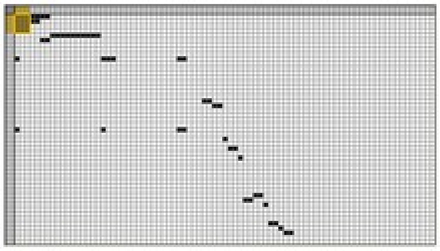


Figure 107. Recognized role.

The four Entitlements and the first three Users are Located in the top-left corner of the Map. The other 12 Users are now more easily found by scrolling horizontally through the first 4 rows at the top of the Map.

Zoom on the Map

Maps in the AA Module can be viewed at three distinct zoom levels.

By default, the base Map is always shown.

In the panel below, the upper figure displays the Map at the base resolution:

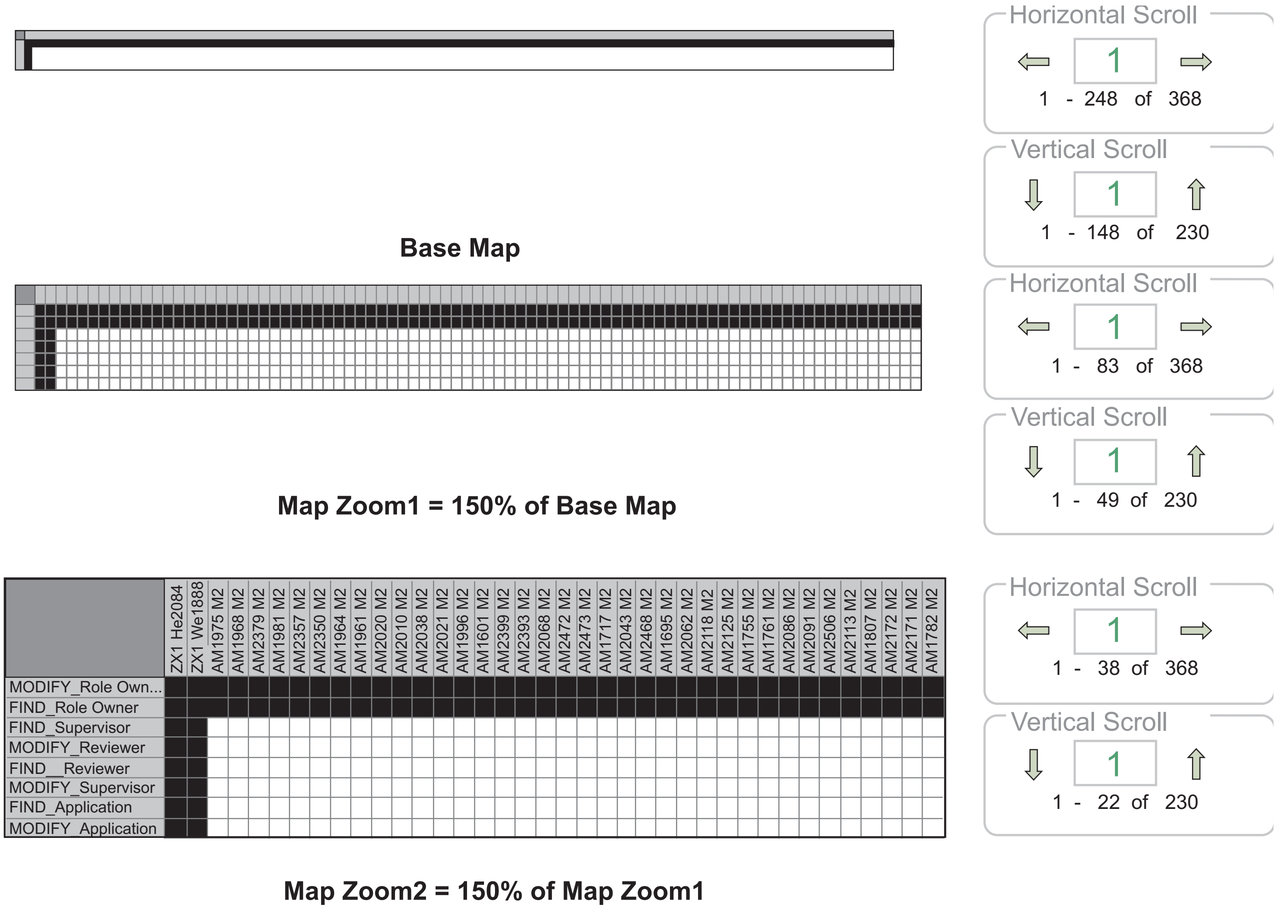


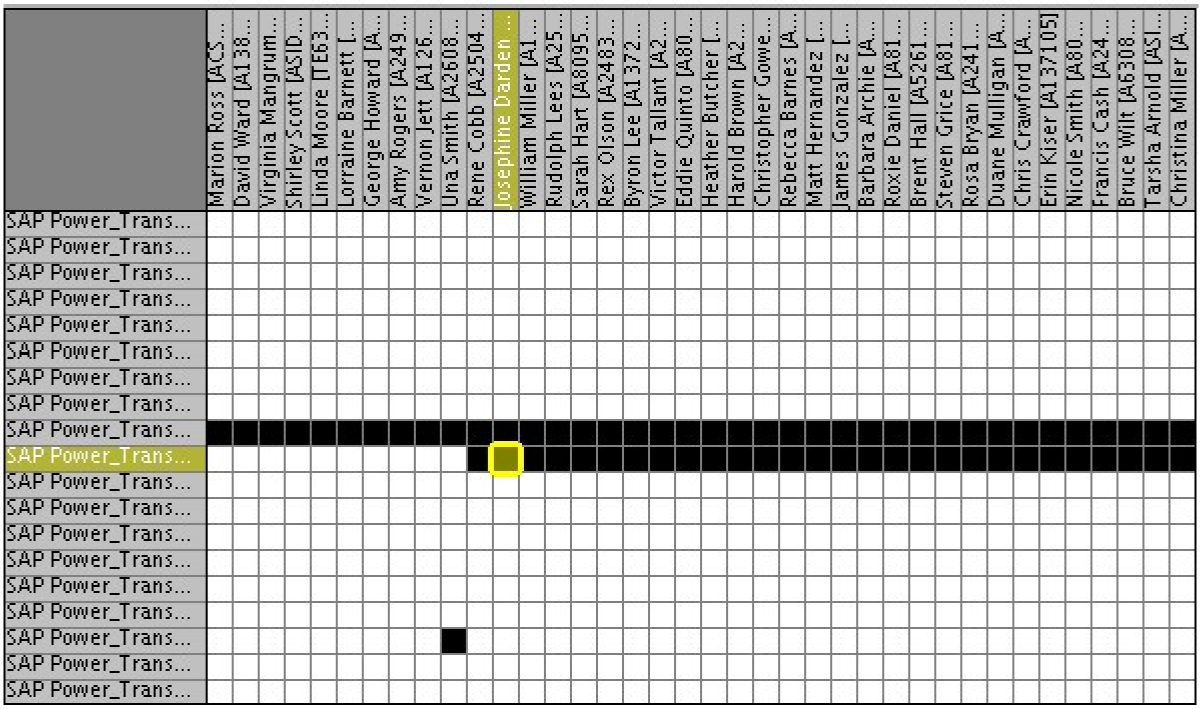
Figure 108. Examples of three Map zoom levels

The 2nd and 3rd figures are obtained by clicking on the **Zoom In** button (the converse is performed by clicking on the **Zoom Out** button).

Every zoom action modifies the resolution of the Map at 150% (reducing/enlarging according to **Zoom Out**/**Zoom In** buttons). By using the horizontal/vertical scrolls and zoom buttons together, you can easily browse the Map and analyze the entire result-set.

In the first sample you can only visualize the map, in the second you can click one black block to visualize a tooltip that explains the basic information about User and Entitlement.

In the third sample you can click a block to highlight in the map the basic information about User and Entitlement, as shown in the figure below:



	Marion Ross [ACS...	David Ward [A138...	Virginia Mangrum...	Shirley Scott [ASID...	Linda Moore [TE63...	Lorraine Barnett [...	George Howard [A...	Amy Rogers [A249...	Vernon Jett [A126...	Una Smith [A2608...	Rene Cobb [A2504...	Josephine Darden ...	William Miller [A1...	Rudolph Lees [A25...	Sarah Hart [A8095...	Rex Olson [A2483...	Byron Lee [A1372...	Victor Tallant [A2...	Eddie Quinto [A80...	Heather Butcher [...	Harold Brown [A2...	Christopher Gowe...	Rebecca Barnes [A...	Matt Hernandez [...	James Gonzalez [...	Barbara Archie [A...	Roxie Daniel [A81...	Brent Hall [A5261...	Steven Grice [A81...	Rosa Bryan [A241...	Duane Mulligan [A...	Chris Crawford [A...	Erin Kiser [A137105]	Nicole Smith [A80...	Francis Cash [A24...	Bruce Wilt [A6308...	Tarsha Arnold [ASI...	Christina Miller [A...
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
SAP Power_Trans...											■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...																																						
SAP Power_Trans...										■																												
SAP Power_Trans...																																						
SAP Power_Trans...																																						

Figure 109. Examples of three Map zoom levels

A more complex example is shown below:

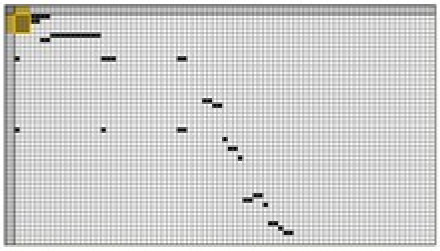


Figure 110. “Scattered” Map

Looking at this scattered Map (13357 Entitlements for 8741 Users) it becomes evident why zoom functions are so useful, as demonstrated by the “zoomed” Map below:

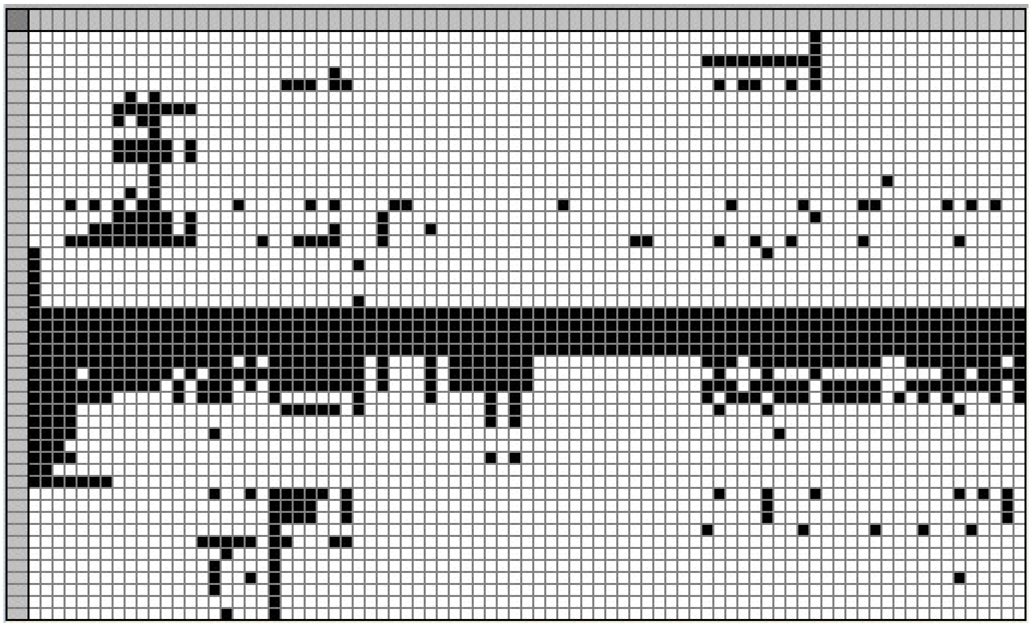


Figure 111. “Scattered” Map: Zoomed In (150% enlargement)

Risk Map

The Map represents the score in the entitlements-users assignments.

A high level of familiarity with the Map is a must in order to:

- Investigate the result set produced by the analysis process.
- Make decisions about Attestation Campaign on input data to refine the obtained result set.

A set of entitlements is listed on one axis of the map and a set of users on the other. The red dot represents the risk on the assignment of the entitlements to a user.

Map is colored with 256 different levels of red, depending on the risk level present in that assignment.

From the same Map window, you can launch the Review Campaign. It is possible to exclude from campaigns the assignments with low risk level and consider only the high risk assignments.

The attestation campaigns made by the AO module will go into the AG Core database, where they will be processed and made available.

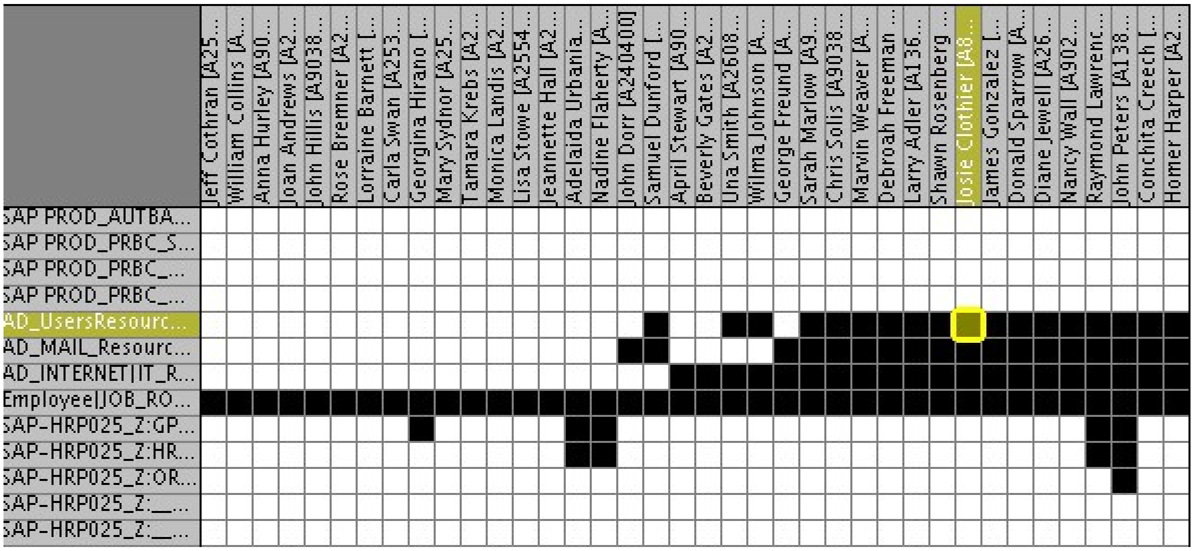
For viewing the campaign status on the AG Core administration module, from the tabs bar, click:

Configure > **Certification** > **Campaigns**.

Map management

In this section are listed all common buttons available for any map of the AA module, role and risk maps.

The following figure provides an example of map section:



	Jeff Cothran [A25…	William Collins [A…	Anna Hurley [A90…	Joan Andrews [A2…	John Hillis [A9038…	Rose Bremner [A2…	Lorraine Barnett […	Carla Swan [A253…	Georgina Hirano […	Mary Sydnor [A25…	Tamara Krebs [A2…	Monica Landis [A2…	Lisa Stowe [A2554…	Jeannette Hall [A2…	Adelaida Urbania…	Nadine Flaherty [A…	John Dorr [A240400]	Samuel Dunford […	April Stewart [A90…	Beverly Gates [A2…	Una Smith [A2608…	Wilma Johnson [A…	George Freund [A…	Sarah Marlow [A9…	Chris Solis [A9038…	Marvin Weaver [A…	Debroah Freeman …	Larry Adler [A136…	Shawn Rosenberg …	Josie Clothier [A8…	James Gonzalez […	Donald Sparrow [A…	Diane Jewell [A26…	Nancy Wall [A902…	Raymond Lawrenc…	John Peters [A138…	Conchita Creech […	Homer Harper [A2…
SAP PROD_AUTBA…																																						
SAP PROD_PRBC_S…																																						
SAP PROD_PRBC_…																																						
SAP PROD_PRBC_…																																						
AD_UsersResourc…																		■			■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_MAIL_Resourc…																	■	■					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
AD_INTERNET|IT_R…																			■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Employee|JOB_RO…	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
SAP-HRP025_Z:GP…									■						■	■																			■	■		
SAP-HRP025_Z:HR…															■	■																			■	■		
SAP-HRP025_Z:OR…																																				■		
SAP-HRP025_Z:__…																																						
SAP-HRP025_Z:__…																																						

Figure 112. Example of map.

If the map is too large to be displayed entirely, use the **Horizontal**/**Vertical** scrolls, on the right side of the map.

To navigate the map, either click the arrows (⬅ /➡ or/and ⬇ / ⬆), or write the desired number directly in the text area and then click the arrows.

In the **Map** tabs, buttons and functions allow you to perform several role/risk map analysis operations:

- **Exception modulation**: using the **Exception** combo box change the value from 0 to 100. According to the value set in the combo box and clicking **Remove**, a subset of assignments in the map will change from black squares into the ⊟ symbol. For more details, see Select Area in the Map.
- **Missing modulation**: using the **Missing** combo box change the value from 0 to 100. According to the value set in the combo box and clicking **Fill-up**, a subset of assignments in the map will change from white boxes into the ⊞ symbol. For more details, see Select Area on the Map.
- **Remove**/**Fill-up**: directly selecting a white/black box (clicking it with the left mouse button) and clicking **Remove**/**Fill-up**, the assignments will be removed or added in the selected area.
- **New Request**: by clicking **New Request** you can perform a request after a map change. In the New Request window, set the parameters for the new request.
- **Reshuffle**: by clicking **Reshuffle** the map will change. This operation is possible, after selecting the area.For more details, see Select Area on the Map.
- **Select area**: click **Select Area** to highlight an interested area. With the left mouse button click a block on the map to define the start position of the area. The area selected between the start/end positions will be covered with a yellow mask.
- **Single select**: allows you to return to single select mode. The single selection is possible only when the action is performed on the selected area, after the area involved is highlighted in yellow. The single block that is highlighted is the end position block of the **Select Area** action. For more details, see the Select Area on the Map.

- **Zoom in/Zoom out**: the zoom action modifies the resolution of the map.**Zoom in/Zoom out**: the zoom action modifies the resolution of the map. For more details, see Zoom on the Map.
- **Exclude Campaigns**: the **Risk Threshold** combo box allows you to change the value from 5% to 100%. According to the value of the combo box, clicking**Exclude**, a subset of risky assignments in the Risk Map will change from red squares into the ⊟ symbol.
- **Exclude**: by directly selecting a red assignment (clicking it with the left mouse button) and clicking **Exclude**, the assignments will be removed from the selected area.
- **Review Campaigns**: allows you to open the Attestation Campaign window. For more details about this topic, see Risk Map.

Remember:

- When you move the mouse pointer to a specific position on the map, a dedicated tooltip displays, highlighting the position coordinates in the form:

  ```
  User: user name | user surname [user code]
  Entitlement: entitlement name | entitlement type | application name
  ```
- You can manually add/remove missing/exception assignments after an exception/missing modulation which is an automatic operation.

  By inverting the order of the operation typology and performing the manual operation before the automatic operation, the fixed settings of the manual operation are lost.

Access Optimizer: Guide to modeling

Access Optimizer is a role engineering tool that combines the concept of risk analysis with the process of role mining.

The goal is to

- Automate the cumbersome and inefficient process of manual role creation
- Contribute to the ongoing lifecycle management process with operations aimed at controlling the amount of risk

In this manner, roles can be implemented to obtain the best results in governance, risk management, and compliance.

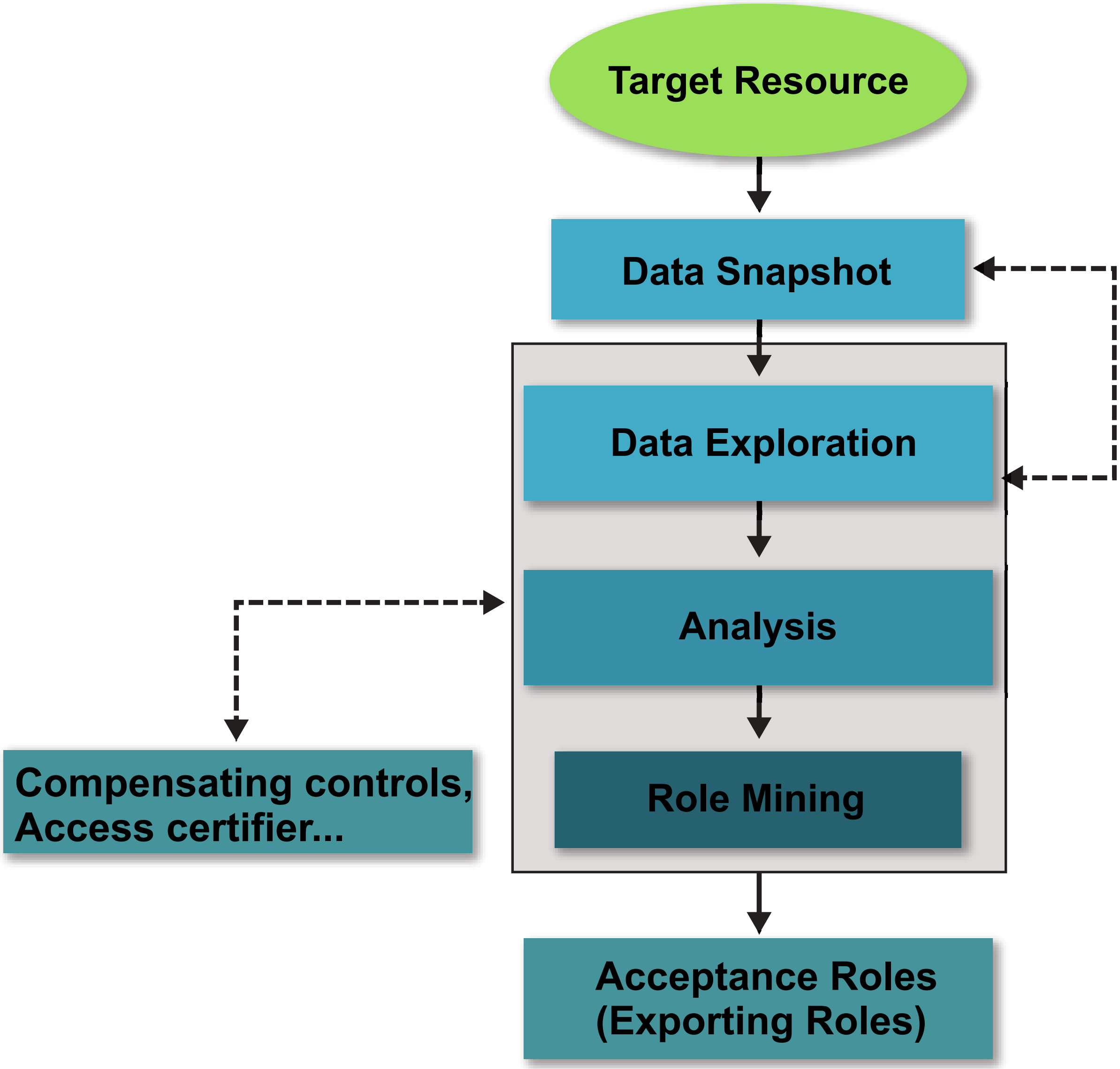

Target Resource
Data Snapshot
Data Exploration
Analysis
Role Mining
Compensating controls, Access certifier...
Acceptance Roles (Exporting Roles)

Figure 113. Main workflow.

Access Optimizer uses a set of advanced algorithms to create a map of users and permissions (entitlements). With a full set of visual tools, role recognition becomes much easier. All key aspects of the role engineering process are described in the following sections.

- “Phase 1: Data snapshot”
- “Phase 2: Data exploration algorithm” on page 491
- “Phase 3: Risk analysis process” on page 492
- “Phase 4: Role mining algorithm” on page 493
- “Phase 5: Role acceptance” on page 493

Phase 1: Data snapshot

In this phase, select the set of access permissions that best represents all the examined IT subsystems to identify the right set of candidate roles.

The selection criteria can be based on target systems and user attributes (for example, all the users who belong to a certain OU).

After identification, the data must be collected from all the sources.

The following entities and relations are loaded:

Organization Units
The units that make up the organization being examined.

Users The users who belong to the organization.

Applications
The applications that are run in the organization.

Entitlements
The entitlements (permissions) registered in the organization.

Entitlement Hierarchy
The hierarchy among the entitlements registered in the organization.

Assignments
All user-entitlement assignments.

These operations are available from Bulk Data Load>Data Snapshot.

The data is loaded from either of two sources:

- A flat file.
- The IAG-DB (AGCore database), a centralized warehouse of the IBM Security Identity Governance platform.

Phase 2: Data exploration algorithm

The goal of role mining is to create/design roles, which means identify a set of entitlements that must be assigned to a set of users.

Even for a medium scale company, it is impossible to find all the interesting roles by analyzing the whole set of user-entitlement assignments.

For a better data subset detection, the access analytics offers a pre-mining phase based on business information such as:

- Users (OUs + 10 user attributes independently selectable)
- Entitlements (Applications + entitlement type + 10 entitlement attributes independently selectable)

After uploading the data performing the data snapshot operation, the data exploration algorithm must be run for all user-entitlement assignments registered in the organization information system. This phase allows you to understand the quality of the expected role patterns by defining a set of filters to identify the best problem partition.

The algorithm allows for data filtering based on a large set of criteria.

For example, the data exploration procedure can be run:

- on all data
- on a specific OU or on a specific subtree of the organization's hierarchy
- on a specific attribute within the set of available attributes

- other data

Generally, it is recommended to run the first instance of this phase on all data.

The pre-analysis computes one special index, the Minability, which guides the analyst in selecting the filters for the subsequent analysis. This index allows for further, more precise risk analysis and role mining processes based on other algorithms and well-shaped areas to best create roles. This activity of "pre-mining" is aimed at reducing subsequent role engineering effort.

For every result set, an advanced graphical role map is provided along with a set of specific statistical data.

Phase 3: Risk analysis process

The risk analysis process is described.

The process consists of two phases:

- Step 1: Analysis
- Steps after Step 1 (2, 3, and so on)

The next figure below the recommended roadmap to follow for the first and for all following analysis:

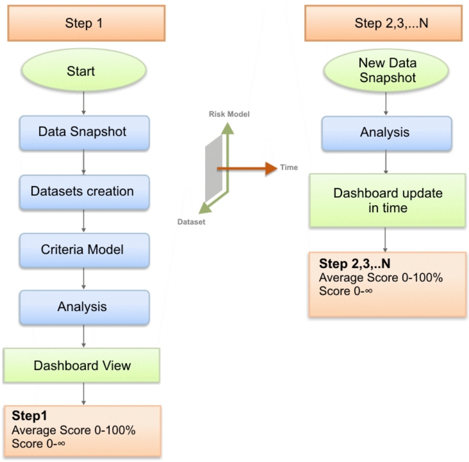


Figure 114. The Risk Analysis process.

After uploading the data from the database or from a file using the data snapshot operation and the data exploration operation, and before you start the risk analysis process, you should create a data subset via a Dataset, by applying specific Risk Criteria.

After detecting an interesting result set, the algorithm provides two indexes for determining its risk: Average risk and risk quantity.

This index helps you keep under control the amount of risk and the relative increase or decrease in time. For every result set, an advanced graphical dashboard is provided along with a set of specific statistical data.

Phase 4: Role mining algorithm

The role mining process have to be preceded by a pre-mining phase of Data Exploration.

The Data Exploration phase is based on the data snapshot previously set.

You have to run a new Data Exploration after every change of the data snapshot.

Optimal role set

This algorithm analyzes the data to find the best (optimal) roles based on the assigned criteria such as input data.

The optimal role set determines the best roles from the analyzed data, maximizing or minimizing the criteria of the chosen aggregation (for example, contextually maximize the number of users with a certain assigned entitlement, minimize the number of roles per user, and so on) .

It can generate a very big number of candidate roles.

Therefore, it is always useful to consult the data exploration output, choosing carefully the initial data set to analyze.

Phase 5: Role acceptance

Before deployment into the production system, correctness and relevance of the identified roles should be checked.

In many organizations, this activity involves both the business and IT departments. After the approval phase, roles can be imported into the IBM Security Identity Governance AG Core main repository.

Manage

The following functions for managing the main entities of this module are available:

- Data Exploration
- Role Mining

Data Exploration analysis and details

This section helps you run the main operations involved with creating and managing an analysis.

An *analysis* is the object that contains all the data required for a data analysis. Analyses are listed under the **Analysis** tab.

An analysis is identified by a set of fields arranged in a row.

Click **Filter** to filter rows of analyses using the items described in the following table:

Table 232. Analysis filters.

Filter	Description
Analysis Description	A descriptive text of the analysis.

Table 232. Analysis filters. (continued)

Filter	Description
Organization Unit	Click ⋯ **Browse** to choose the OU in the analysis.
Application	Click ⋯ **Browse** to choose the Application in the analysis.
Entitlement Type	Indicates the entitlement types. • Permission • IT Role • Business Role • External Role
Status	Indicates the status of the analysis. • ✓ Indicates in progress. • ✓ Indicates complete. • ✗ Indicates an error. • ! Indicates invalidated due to a new bulk load.
User/Entitlement Attributes	If present, according to the current configuration.

The details included in an Analysis row are the same as those described in the preceding table, with the addition of more items.

Click ⓘ **Info** to display all the information of an analysis. The details that characterize an analysis are described next.

Table 233. Analysis details.

Attribute	Description
Analysis	• **Code** is a number that is automatically attached to the request. • **Analysis Description** describes the request. • **Start Time** is expressed in configurable format. • **End Time** is expressed in configurable format. • **Processing Time** is the time that is required to process the request.

Table 233. Analysis details. (continued)

Attribute	Description
Data Filters	• **Only direct assignment** specifies whether the analysis is based only on entitlements that are directly assigned to users. • **OU** is the OU name. • **Hierarchy** specifies that the analysis involves all the OUs starting from the root **OU**. • **Application** is the application name. • **Entitlements Type** can be any of the following types: – Permission – IT Role – Business Role – External Role • **User Attributes** or **Entitlement Attributes**, if present, according to "User – Entitlement Attributes" on page 528.
Analysis Type	• **Type** is the label name. • **Depth** is the position of the OU in the hierarchy. (All or 0...6 depth level)

The **Actions** menu lists the following items:

Add Select to define an analysis.

Remove
Select to delete an analysis row.

Click 🔍 **Details** to display a panel that includes 3 frames.

In the top part of the panel, the **Back** button enables you to return to the Analysis view.

In the left frame, the **Partitions** tab hosts all the partitions generated during the analysis, according to the attributes summarized below:

Table 234. Partition attributes.

Attribute	Description
Name	The name of the partition.
Minability	Minability values.
Subset	Entities of the partition.
Status	The status of the request. It can be: • ✓ : Complete • ✗ : Error • ! : Warning

When you select a partition, the center pane is populated with the subsets of the selected partition. From the center pane you can search (click **Filter**/**Hide Filter**) partition subsets using their `Name` as a filter.

From this pane, you can click **Actions** > **Massive Role Minig** to run a new operation on the entire data exploration partition.

From the tabs on the right pane, you can view the subset data in detail:

- Map (open by default)
- Entitlements/Users
- Entitlements/Users Statistics

Entitlements/Users

Select the **Entitlements**/**Users** tab to display the entitlements/users aggregated to the partition selected in the central pane.

The columns displayed for an entitlement/user are configured in the **Settings** > **Attributes** tab.

Entitlements/Users Statistics

Select the **Entitlements**/**Users Statistics** tab to display a histogram-based graphic that shows statistics about the entitlement/users of the selected partition.

In these tabs, you can search Entitlements/Users Statistics (click **Filter**/**Hide Filter**) using the filters summarized in the next table:

Table 235. Entitlements/Users Statistics filters.

Attribute	Description
Order by	This combo box helps you choose the visualization order of the column attributes
Descendant/**Ascendat**	This combo box helps you choose the sorting order of the data attributes
Attribute 0... Attribute 9 (for Users)	Attributes configured in the "User – Entitlement Attributes" on page 528 section
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the Entitlement attributes section

Role mining

The output of this phase is mainly represented by a set of candidate roles.

During this analysis, the following algorithms can be applied:

- "Optimal Role-Set algorithm" on page 461

The **Analysis** tab displays already made role mining analysis. This pane includes the following buttons:

- **Filter/Hide Filter**: shows/hides the Filters option
- **Search**: finds the results of role mining analyses
- **Add**: makes a new request

- **Remove**: deletes requests

You can use the following filters to search for the results of a role mining request:

Table 236. Role mining search filters.

Filter	Description
Request Description	A description of the request.
Type	The type of request can be one of the following: • **Optimal Role-set**
Organization Unit	The name of the root OU in the hierarchy.. Select **Hier** to include all the Organization Unit starting from the root **OU**.
Application	Name of the application.
Entitlement Type	The entitlement can be one of the following: • : **Permission** • : **IT role** • : **Business role** • : **External role**
Status	The status of the request.
Attribute 0... Attribute 9 (for Users)	Attributes configured in the User attributes section.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the Entitlements attributes section.

A request for a role mining analysis has the following attributes:

Table 237. Role mining analysis attributes.

Attribute	Description
Code	A progressive code number that is automatically attached to the request.
Request Description	A description of the request.
Status	The status of the request can be: • ✓ : **Complete** • ✓ : **In progress** • ✗ : **Error** • ! : **Warning** • ! : **Deleting**
Type	The request type can be: • **Data Exploration** • **Optimal Role-set**
Direct	Indicates that the `only direct assignments` option was specified for the request.

Table 237. Role mining analysis attributes. (continued)

Attribute	Description
Organization Unit	The name of the root OU in the hierarchy.. Select **Hier** to include all the Organization Unit starting from the root **OU**.
Application	Name of the application.
Entitlement Type	The entitlement can be one of the following: • : **Permission** • : **IT role** • : **Business role** • : **External role**
Attribute 0... **Attribute 9** (for Users)	Attributes configured in the User attributes section.
Attribute 0... **Attribute 9** (for Entitlements)	Attributes configured in the Entitlements attributes section.

You can set a specific algorithm type for every new role mining request, based on the following parameters:

Table 238. Optimal role-set parameters.

Attribute	Description
Minimum Number of Users per Role	The minimum number of users that can be aggregated for a candidate role
Minimum Number of Entitlements per Role	The minimum number of profiles that can be aggregated to a profile included in a candidate role
Maximum Number of Roles	The maximum number of candidate roles
Role to User Assignments	The tendency to associate many or few users to a role
Role to Entitlement Assignments	The tendency to create large or small candidate roles, by grouping many or few entitlements in a role
User to Entitlement Assignments	The tendency to associate many or few entitlements to a user (using a subset of candidate roles)
OU Spread	Spread is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization.OU Spread indicates the inclination towards obtaining a very scattered or localized role distribution in the OU hierarchy. See Spread.
Application Number	The tendency to associate many or few applications to a user (using a subset of candidate roles)
Entitlement Type Number	The tendency to associate many or few types of entitlements to a user (using a subset of candidate roles)

Table 238. Optimal role-set parameters. (continued)

Attribute	Description

Click **Details** to display the following tabs:

- **Details** (opened by default)
- Statistics
- Map
- Roles
- Entitlements

The **Details** tab shows the details of a selected data exploration operation according to the attributes described in the next table:

Table 239. Data exploration details.

Attribute	Description
Request	Includes the following: • **Code**: The code number attached to the request • **Request Description**: A description of the request • **Start Time**: The time when execution of the request was started in the *dd/mm/yyyy* and *hh/mm/ss* format • **End Time**: The time when execution of the request was finished in the *dd/mm/yyyy* and *hh/mm/ss* format • **Processing Time**: The time required to process the request
Data Filters	Includes the following: • **Only direct assignment** • **OU name** • **Hierarchy** • **Application name** • **Entitlements Type**: Permission/ IT role/Business role • **Users/ Entitlements Attributes**
Request Type	Includes the following: • **Algorithm type**: Data exploration, Optimal role set • **Type**: Label name • **Depth**: Hierarchy OU position (All or 0...6 depth level)

Statistics

The Statistics tab provides a set of graphical dashboards for the selected analysis.

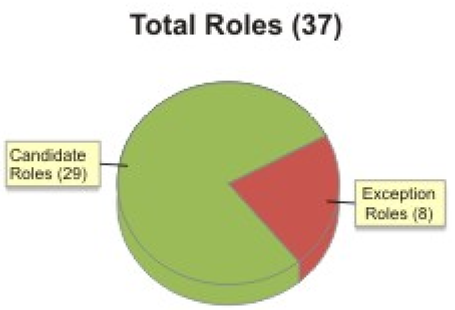
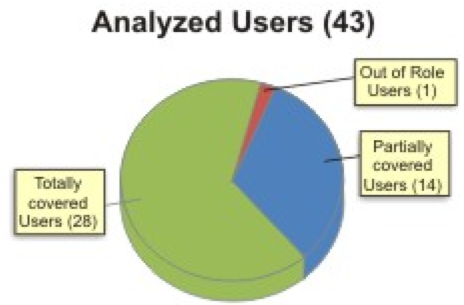
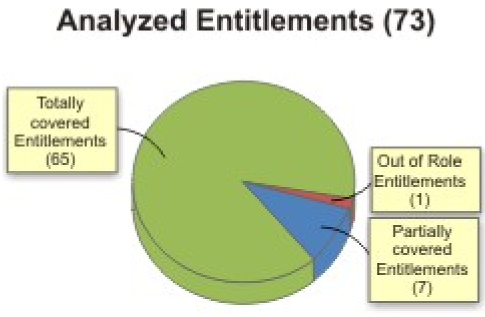
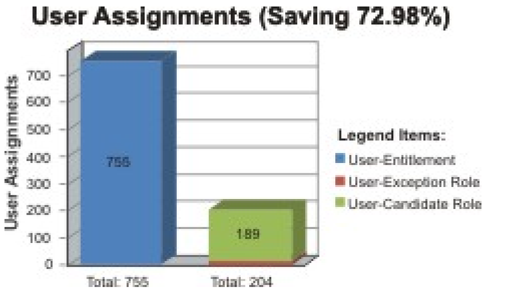
The available dashboards are structured into two tabs:

- Analysis Statistics

- Role Statistics

Analysis Statistics

Table 240. Dashboard set.

Dashboard	Description
	• The green zone represents the collection of candidate roles, for example roles whose adoption into the organization can be considered useful. • The red zone represents exception roles, for example those built with entitlements that are not aggregated to the set of candidate roles. Every exception role is composed of a single entitlement.
	• Users in the green zone: each of their assigned entitlements is involved in at least one candidate role. • Users in the blue zone: some of their assigned entitlements are not involved in any candidate role. • Users in the red zone: none of their assigned entitlements belong to any candidate role.
	• Entitlements in the green zone: each user assigned to these entitlements is involved in at least one candidate role. • Entitlements in the blue zone: some users assigned to these entitlements are not involved in any candidate role. • Entitlements in the red zone: none of the users assigned to these entitlements are involved in any candidate role.
	• The blue histogram shows all entitlements assigned to the considered users. • The green histogram shows all candidate roles assigned to the considered users. • The red histogram shows all exception roles assigned to the considered users.

Role statistics

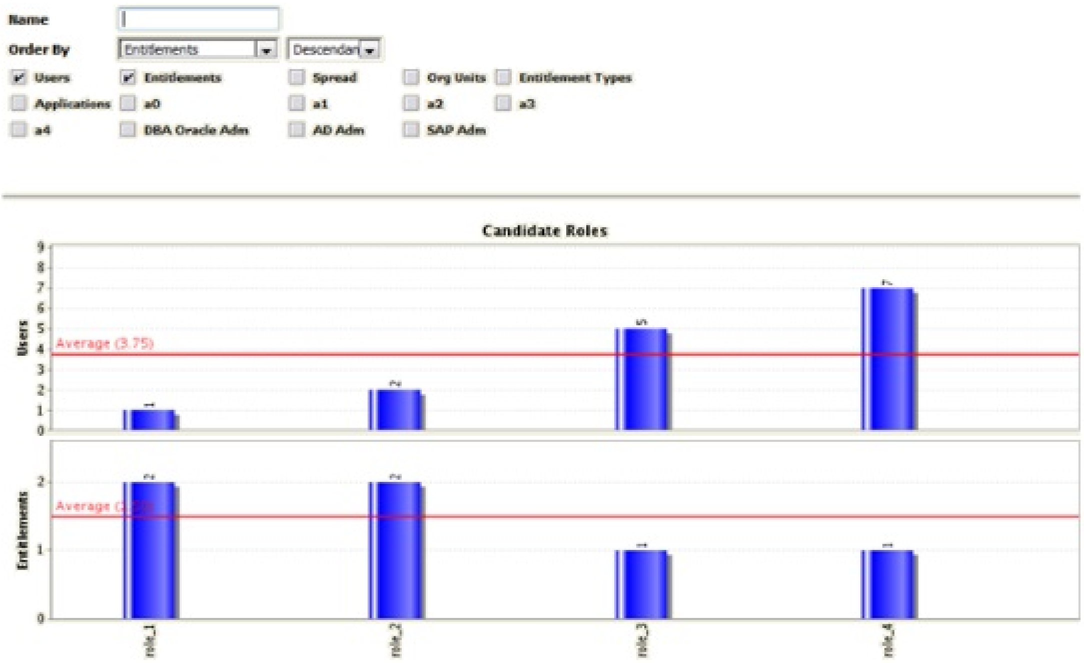
The **Role Statistics** tab provides a set of histograms for a selected request.

Different filters can be chosen as described in the table below:

Table 241. Role statistics filters.

Filter	Description
Name	Name(s) of role(s) involved in the request.
Order By	You can sort the displayed data in ascending or descending order, based on the data elements provided. You can start with **Users**.
Listed in the rows below are all the algorithm parameters involved in the request, selectable by selecting the appropriate check box. The related histogram will be displayed only if the check box is selected.	
Users	Users involved in the request
Entitlements	Entitlements involved in the request
Spread	OU spread
Org Units	OUs involved in the request
Entitlement Types	The entitlement can be one of the following: • : **Permission** • : **IT role** • : **Business role** • : **External role**
Applications	Applications involved in the request
User Attribute 0 ... Attribute 9	Only user attributes specified in the request are available
Entitlement Attribute 0 ... Attribute 9	Only entitlement attributes specified in the request are available
Role Attribute 0 ... Attribute 9	Only role attributes specified in the request are available

The next figure shows an example with the **User** and **Entitlements** check boxes selected, where statistics are listed by entitlement in descending order.



Name

Order By Entitlements Descendan

☑ Users ☑ Entitlements □ Spread □ Org Units □ Entitlement Types

□ Applications □ a0 □ a1 □ a2 □ a3

□ a4 □ DBA Oracle Adm □ AD Adm □ SAP Adm

Figure 115. Example of Statistics with User and Entitlements check boxes selected.

Role analysis

The Role Mining tab contains many features for investigating the structure of the candidate roles indicated by the analysis.

The left frame contains four tabs:

- Roles (default active tab)
- Entitlements
- Users
- Statistics

In the **Roles** tab, the candidate roles are characterized by a set of statuses, according to the role position in the operational flow managed by the role engineer.

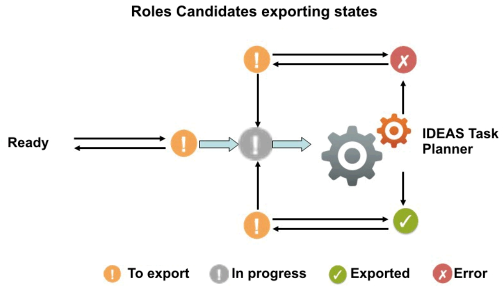


Figure 116. Possible states of candidate roles.

The main goal of Role Mining activity is to identify and import candidate roles, into "Enterprise" roles set (AG Core database).

Click **Filter** to filter candidate roles according to their names.

Each candidate role row presents the attributes shown below:

For any candidate role selected in the **Roles** tab, in the right pane you can select several tabs.

In particular, in **Roles Details** tab are shown all the characteristics of the candidate role, grouped for entity:

Table 242. Entitlement details.

Detail	Description
Role Name	Name of role
Rep. Status	Status of the role
Application	Name of the application.
Application Support (%)	Percentage of application to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
Entitlements	Name of the entitlement.
Entitlements Support (%)	Percentage of entitlements to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
Users	Number of users assigned to the selected role.
User Support (%)	Percentage of users to be assigned to the role, from the entire set of users involved in the analysis.
Org Units	Number of organization units involved in the selected role.
Org Unit Support (%)	Percentage of organization units to be assigned to the role, from the entire set of organization units involved in the analysis.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Minimum Farness	Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness.
Average Farness	Average distance of all OUs from the centroid of distribution. See Farness.
Average Coverage (%)	Average percentage of OUs assigned with the entitlement.
Maximum Coverage (%)	Maximum percentage of OUs assigned with the entitlement.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the section Entitlement attributes.

In the“Role map” on page 472, is shown the map of the candidate role.

Four other tabs (**Entitlements**, **Applications**, **Users**, **Organization Units**) can be selected for showing the related entities involved with the candidate role selected.

Finally, the **Impact Analysis** tab allows you to evaluate the changes involved in the organization if you are going to import the candidate role into "Enterprise" roles set (AG Core database).

Entitlements analysis

This section contains many useful features for investigating the structure of the Candidate Roles from an Entitlement approach.

Entitlements are characterized by the following icons (✅ , ☑ , ○) related to the concept of "User coverage". Entitlements can be filtered (clicking **Filter**) using the filters described in the table below:

Table 243. Entitlement filters

Attribute	Description
Name	Indicates the name of the entitlement.
Entitlement Type	The entitlement can be one of the following: • : **Permission** • : **IT role** • : **Business role** • : **External role**
Application	Name of the application.
User Coverage	This filter can assume three different values: • ○ Out of Role: the entitlement cannot be assigned to any qualified user using the candidate roles. • ☑ Partially covered: the entitlement can be assigned only to a subset of qualified users using the candidate roles. • ✅ Covered: the entitlement can be assigned to all qualified users using the candidate roles.

Upon selecting an entitlement in the **Entitlements** tab on the left, the **Entitlements Details** tab is by default shown on the right with the relevant information. The information is organized in the following groups: **Entitlements - Users - Organization Units**.

Table 244. Entitlement details

Attribute	Description
Application	Name of the application.
Entitlement Name	Name of the entitlement.
Users	Number of users assigned to the selected entitlement.

Table 244. Entitlement details (continued)

Attribute	Description
User Support (%)	Percentage of users that have the entitlement from the entire set of users that must have the entitlement.
Covered Users	Number of users covered with the entitlement.
User Coverage (%)	Percentage of users in the OU who are assigned to the entitlement.
Org Units	Number of organization units involved in the selected entitlement.
Org Unit Support (%)	Percentage of organization units to be assigned to the entitlement, from the entire set of organization units involved in the analysis.
Covered Org Units	Number of organization units covered with the Role entitlement.
Org Unit Coverage(%)	Percentage of organization units that are assigned with the entitlement, from the entire set of organization units that must be assigned with the entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.
Minimum Farness	Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness.
Average Farness	Average distance of all OUs from the centroid of distribution. See Farness.
Average Coverage (%)	Average percentage of OUs assigned with the entitlement.
Maximum Coverage (%)	Maximum percentage of OUs assigned with the entitlement.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the Entitlement attributes section.

The other operations for Entitlements analysis are:

- Users aggregated with the selected Entitlement
- OUs aggregated with the selected Entitlement

Users aggregated with the selected entitlement

The **Users** tab lists all candidate roles containing the entitlement previously selected in the **Entitlements**tab.

For each candidate role, the data set in the table below is displayed:

Table 245. Candidate Role attributes

Attribute	Description
Role Name	Indicates the name of the role.
Exportation (Report/Release)	The role can have one of the following statuses: • ! **Scheduled to be exported** • ! **Exportation in progress** • ✓ **Successfully exported** • ✗ **Error**
Users	Indicates the number of users for the selected candidate role.
Entitlements	Indicates the number of entitlements for the selected candidate role.
Assignments	Indicates the number of user-entitlement assignments for the selected candidate role.
OU Spread	"Spread" on page 468 is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization. OU spread indicates the tendency towards a scattered/localized role distribution in the OU hierarchy.
Org Units	Indicates the number of OUs for the selected candidate role.
Applications	Indicates the number of applications for the selected candidate role.
Entitlement Type	Entitlement types include the following ones: • **Permission** • **IT role** • **Business role** • **External role**
Attribute 0... Attribute 9 (for Users)	Attributes that are configured in the User Attributes section.
Attribute 0... Attribute 9 (for Entitlements)	Attributes that are configured in the Entitlements Attributes section.

When you select a candidate role from the central pane, the users joined to the candidate role are automatically highlighted in the **Users** tab in the far right.

Listed Users are characterized by the attributes shown in the table below:

Table 246. User attributes

Attribute	Description
In/Out	The user status can be one of the following: - ✓ In Role (Role aggregated to the User) - ✗ Out of Role (Role not aggregated to the User)
Last Name	Surname of the user.
Name	Name of the user.
User ID	Unique ID assigned to the user.
Organization Units	Name of the OU, in which the user is registered.
Attribute 0... Attribute 9 (for Users)	Attributes configured in the User attributes section.

When you select a user from the **Users** tab in the far right, all aggregated candidate roles are automatically highlighted in the central pane.

OUs aggregated with the selected entitlement

The **Organization Units** tab lists all candidate roles containing the entitlement previously selected in the **Entitlements**tab .

The attributes described in the table below are displayed for each candidate role:

Table 247. Candidate Role attributes

Attribute	Description
Role Name	Indicates the name of the role.
Exportation (Report/Release)	The role can have one of the following statuses: - ! **Scheduled to be exported** - ! **Exportation in progress** - ✓ **Successfully exported** - ✗ **Error**
Users	Indicates the number of users for the selected candidate role.
Entitlements	Indicates the number of entitlements for the selected candidate role.
Assignments	Indicates the number of user-entitlement assignments for the selected candidate role.
OU Spread	"Spread" on page 468 is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization. OU spread indicates the tendency towards a scattered/localized role distribution in the OU hierarchy.
Org Units	Indicates the number of OUs for the selected candidate role.
Applications	Indicates the number of applications for the selected candidate role.

Table 247. Candidate Role attributes (continued)

Attribute	Description
Entitlement Type	Entitlement types include the following ones: - **Permission** - **IT role** - **Business role** - **External role**
Attribute 0... **Attribute 9** (for Users)	Attributes that are configured in the User Attributes section.
Attribute 0... **Attribute 9** (for Entitlements)	Attributes that are configured in the Entitlements Attributes section.

When you select a candidate role in the central pane, the OUs joined to the candidate role are automatically highlighted in the **Organization Units** tab in the far right.

The listed OUs are characterized by the attributes shown in the table below:

Table 248. OU attributes.

Attribute	Description
In/Out	The OU status can be one of the following: - ✓ In Role (Role aggregated to the OU) - ✗ Out of Role (Role not aggregated to the OU)
Code	Code assigned to the OU.
Name	Name of the OU, in which the user is registered.
Farness	Farness is a numeric index that provides an estimate of the virtual distance between OUs having the same entitlement/candidate role. It can measure the distance between OUs in which different registered users are assigned the same entitlement/candidate role.
Coverage (%)	Percentage of users in the OU who are assigned to the entitlement.
Users	Number of users assigned to the selected entitlement.

When you select an OU from the **OU** tab in the far right, all the aggregated candidate roles are automatically highlighted in the central pane.

User analysis

This section provides several ways of investigating the nature and structure of Candidate Roles from a User approach.

You can use the filters shown in the table below to help you find Users (click on **Filter**):

Table 249. User filters.

Attribute	Description
Master UID	Univocal identifier of the User
Last Name	Surname of the User.
First Name	Name of the User.
Organization Unit	Indicates the OU in which the User is registered.
Hier.	Flag this check box to get the tree view of the Organization unit.
Entitlement Coverage	This filter can assume three distinct values: • ◌ **Out of Role**: the User is not aggregated to any Entitlement through the Candidate Roles. • ◕ **Partially covered**: the User is aggregated only to a subset of Entitlements through the Candidate Roles. • ● **Covered**: the User is aggregated to ALL Entitlements through the Candidate Roles.

Upon selecting a User in the **Users** tab on the left, the **User Details** tab, on the right, is shown by default with the relevant information, distinguished in the following groups: **User - Entitlements - Applications**.

Table 250. User details.

User	
Attribute	**Description**
Last Name	Indicates the User's last name
Name	Indicates the User's name
User ID	Indicates the User's User ID
Organization Unit	Indicates the OU in which the User is registered
Entitlements	
Entitlements	Indicates the number of Entitlements assigned to the selected User
Entitlement Support (%)	Indicates the percentage of Entitlements that should be assigned to the User from the entire set of Entitlements involved in the Request
Covered Entitlements	Indicates the number of Entitlements assigned to the User

Table 250. User details. (continued)

User	
Attribute	**Description**
Entitlement Coverage (%)	Indicates the percentage of Entitlements actually assigned to the User from the entire set of Entitlements that should be assigned to the User
Applications	
Applications	Indicates the number of Applications involving the selected User
Application Support (%)	Indicates the percentage of Applications that should be assigned to the User from the entire set of Applications involved in the Request
Covered Applications	Indicates the number of Applications assigned to the User
Application Coverage(%)	Indicates the percentage of Applications actually assigned to the User from the entire set of Applications that should be assigned to the User

The other operations for User analysis are:

- Entitlements assigned to the selected User
- Applications assigned to the selected User

Applications assigned to a selected User

Select the User to be examined in the left frame and click on the **Applications** tab.

All Candidate Roles aggregated to the selected User are listed in the central frame.

Selecting a Role, the Applications involved with this Role are shown in the **Applications** frame on the right.

For every row of Candidate Roles, the data set is shown in the table below:

Table 251. Candidate Role attributes

Attribute	Description
Role Name	Indicates the name of the role.
Exportation (Report/Release)	The role can have one of the following statuses: • ❗ **Scheduled to be exported** • ❕ **Exportation in progress** • ✓ **Successfully exported** • ✗ **Error**
Users	Indicates the number of users for the selected candidate role.
Entitlements	Indicates the number of entitlements for the selected candidate role.
Assignments	Indicates the number of user-entitlement assignments for the selected candidate role.

Table 251. Candidate Role attributes (continued)

Attribute	Description
OU Spread	"Spread" on page 468 is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization. OU spread indicates the tendency towards a scattered/localized role distribution in the OU hierarchy.
Org Units	Indicates the number of OUs for the selected candidate role.
Applications	Indicates the number of applications for the selected candidate role.
Entitlement Type	Entitlement types include the following ones: • **Permission** • **IT role** • **Business role** • **External role**
Attribute 0... **Attribute 9** (for Users)	Attributes that are configured in the User Attributes section.
Attribute 0... **Attribute 9** (for Entitlements)	Attributes that are configured in the Entitlements Attributes section.

For each row of Applications, the following data set is displayed:

Table 252. Application attributes.

Attribute	Description
In/Out	The Application status can be one of the following: • ✓ **In Role**: Application aggregated to the Role/User • ✗ **Out of Role**: Application not aggregated to the Role/User
Name	Indicates the name of the Application

Role analysis shortcut

Select a Role to be examined from the central **Role Search** frame, then click **Actions** > **Show Role**.

View Entitlement details

In the **Entitlement Details** (opened by default), are automatically shown the data summarized in the table below:

Table 253. Entitlement details.

Attribute	Description
Application	Indicates the name of the Application
Entitlement Name	Indicates the name of the Entitlement
Users	Indicates the number of Users assigned the selected Entitlement
User Support (%)	Indicates the percentage of Users that should be assigned the Entitlement from among the entire set of Users involved in the Request
Covered Users	Indicates the number of Users covered by the Entitlement
User Coverage (%)	Indicates the percentage of Users actually possessing the Entitlement from among the entire set of Users that should have the Entitlement
Org Units	Indicates the number of OUs involved in the selected Entitlements
Org Unit Support (%)	Indicates the percentage of OUs that should be assigned the Entitlement from among the entire set of OUs involved in the Request
Covered Org Units	Indicates the number of OUs covered by the Entitlement
Org Unit Coverage(%)	Indicates the percentage of OUs actually assigned with the Entitlement from among the entire set of OUs that should be assigned with the Entitlement
OU Spread	“Spread” on page 468 is a numeric index that provides an estimate of the "homogeneous diffusion" of a Role in the hierarchical structure of an Organization. OU Spread indicates the tendency towards a very scattered/localized Entitlement distribution in the OU hierarchy.
Minimum Farness	“Farness” on page 469 is a numeric index used that identifies the path and calculates the minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an Entitlement.
Average Farness	Indicates the average distance of all OUs from the centroid of distribution.
Average Coverage (%)	Indicates the average percentage of OUs covered by (assigned with) the Entitlement
Maximum Coverage (%)	Indicates the maximum percentage of OUs covered by (assigned with) the Entitlement
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the section Entitlement attributes.

View User details

In the **User Details** (opened by default), are automatically shown the data summarized in the table below:

Table 254. User details.

User	
Attribute	**Description**
Last Name	Indicates the User's surname.
Name	Indicates the User's name.
User ID	Indicates the User's User ID.
Organization Unit	Indicates the OU in which the User is registered
Entitlements	
Entitlements	Indicates the number of Entitlements assigned to the selected User
Entitlement Support (%)	Indicates the percentage of Entitlements that should be assigned to the User, from among the entire set of Entitlements involved in the Request
Covered Entitlements	Indicates the number of Entitlements assigned to the User
Entitlement Coverage (%)	Indicates the percentage of Entitlements actually assigned to the User, from among the entire set of Entitlements that should be assigned to the User
Applications	
Applications	Indicates the number of Applications involving the selected User
Application Support (%)	Indicates the percentage of Applications that should be assigned to the User, from among the entire set of Applications involved in the Request
Covered Applications	Indicates the number of Applications assigned to the User
Application Coverage(%)	Indicates the percentage of Applications actually assigned to the User, from among the entire set of Applications that should be assigned to the User

Configure

Use the following functions for configuring the listed elements:

- Risk data sets
- Risk criteria

Data snapshot

Use this tool to upload a data snapshot that you can utilize to run analyses other than role mining.

To view the details of a data snapshot on the right pane, select one of the items listed under **Data Snapshot**.

The following details are listed:

Table 255. Data snapshot details

Detail	Description
Type	The data source. It can be: • IAG-DB • File Import
Status	One of the following upload states: • ✓ : In progress • ! : Deleting data not allowed (Disabled) • ✓ : Data uploaded successfully (Completed) • ✗ : Error • ! : Warning (Old data snapshot)
Start Date	Upload start date (mm/dd/yy; hh/mm/ss)
End Date	Upload end date (mm/dd/yy; hh/mm/ss)
Uploading Time	Time needed to upload files
Upload	
Item	**Description**
Organization Units rows	Number of OUs rows uploaded or discarded
Users rows	Number of users rows uploaded or discarded
Applications rows	Number of applications rows uploaded or discarded
Entitlements rows	Number of entitlements rows uploaded or discarded
Assignments rows	Number of assignments rows uploaded or discarded

Click History to view the data snapshot history.

Click Data to view the data uploaded.

To start a new data snapshot operation, click **Actions** > **Add**. The Import Type window displays the options for choosing the data source:

- File Import
- IAG-DB

Note: You can run only one snapshot per day. If you need to add another snapshot on the same day, you must first remove the former one. To do so, select the snapshot and click **Actions** > **remove**.

Add data: File Import

When you choose **File Import** as the data source for the data snapshot or bulk data load operation, a window is displayed. You are required to provide data files for the following items:

- Organization Units

- Users
- Applications
- Entitlements
- Assignments

Optionally, for a bulk data load you can also provide a data file for entitlement hierarchies.

You are required to provide the following information For each type of data file:

Table 256. File import details

Attributes	Description
File location	Enter the name of the folder where the file is located. A **Browse** button is available.
File separator	The character used to separate fields in the file. For example, a semicolon (;).
File Name	The name of the file

Click **Load Data** to confirm the operation.

Click **Undo All** button if you need to clear all fields.

Click **Cancel** to cancel the data snapshot or bulk data load operation.

When the operation completes with success, the status changes to ✓ **Completed**. If errors occur, the status is ✗ **Error**.

If errors are returned, click **Back** to return to the file specification window and repeat the operation. The **Request History** phase is not available until the Upload phase is terminated.

Note: If errors occurred during the Data Validation process, the error type is shown in the same frame.
Attention: If the file format for the upload operations does not comply with the required format, a diagnostic window is displayed. Every incorrect value is traced.

Add data: IAG-DB Import

When you choose **IAG-DB** as the data source for the data snapshot or bulk data load operation, the data is loaded from the AG Core data base.

While the operation is in progress, the status is shown as ✓ **In progrss**. When the operation completes successfully, the status changes to ✓ **Completed**. If errors occur, the status is ✗ **Error**.

History

The **History** tab contains the list of requests made on a selected risk criteria with different data sets in different data snapshots.

You can use filters to search for a request.

Table 257. History filters

Attribute	Description
Dataset	The name of the data set created from a snapshot. Click ... to search for a data set.
Relevance Criteria	Click ... to search for a criterion.
Status	The status of the data snapshot can be: • In progress • Complete • Error • Deleting • Warning

Data

Select this tab to view the data included in the data snapshot or bulk data load.

The data is displayed in the following tabs:

- Organization Units (OU search - OU Structure)
- Users
- Applications
- Entitlements
- Entitlement Hierarchy
- Assignments

Organization unit (OU search - OU structure)

In the **OU** tab, select one of the listed items and click **Actions** > **View Tree** to open the **OU Structure** tab and view the exact position of the OU in the hierarchy.

Users

Select this tab to search and view users.

You can use the following filters to search for users:

- Master UID
- Surname
- Name
- Organization Unit

Select a user and click **Actions** > **View Tree** to get the exact position of the User OU.

Applications

Select this tab to search and view applications.

Entitlements

Select this tab to search and view entitlements.

You can use the following filters to search for entitlements:

Table 258. Filters for entitlements

Filter	Description
Name	Entitlement name
Entitlement Type	The entitlement type can be one of the following: • Permission • IT Role • Business Role • External Role
Application	Entitlement application

Entitlement hierarchy

Select this tab to search and view entitlement hierarchies.

You can use the following filters to search for hierarchies:

Table 259. Filters for Entitlement hierarchies

Filter	Description
Parent Entitlement Name	The name of the parent of the selected entitlement
Parent Entitlement Type	The entitlement type can be one of the following: • Permission • IT Role • Business Role • External Role
Parent Application	The name of the application associated with the parent entitlement. If the parent entitlement type is Business Role, it is associated with a default virtual application.
Child Entitlement Name	The name of the child of the selected entitlement
Child Entitlement Type	The entitlement type can be one of the following: • Permission • IT Role • Business Role • External Role
Child Application	The name of the application associated with the child entitlement. If the child entitlement type is Business Role, it is associated with to a default virtual application.

Click **Hierarchical View** to display the Entitlement Hierarchy Search window and to set the filter data.

Select the entitlements to be examined from the list produced and click **View Tree** in the Entitlement Hierarchy Search window to view hierarchy details.

Assignments

Select this tab to view the assignments associated with users and entitlements. You can use the following filters to search for assignments:

Table 260. filters for assignments

Filter	Description
Entitlement Name	The name of the entitlement
Entitlement Type	The entitlement type can be one of the following: • Permission • IT Role • Business Role • External Role
Application	The name of the application associated with the entitlement. If the entitlement type is Business Role, it is associated with a default virtual application.
Person Code	The User ID of the user
Person Surname	The surname of the user
Person Name	The name of the user
Organization Unit	The OU name
Redundant/Inherited	The parent of the entitlement. This filter is available only for the following operations: • Redundant • Inherited

Access data sets

This section explains the operations needed to create a data set from the snapshot uploaded.

The **Datasets** tab, displays the data sets listed in the system. In this pane, you can find the following buttons:

- **Filter/Hide Filter**: allows you to show/hide the filters option.
- **Search**: allows you to get results according to the filters setting.
- **Add**: allows you to perform empty data sets. The empty data set is displayed in the **Datasets** pane (left).
- **Remove**: allows you to delete data sets.

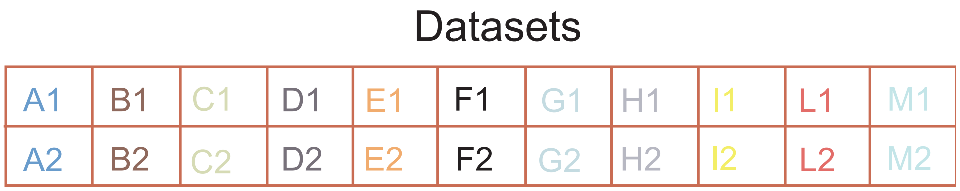
In this tab, the **Automatic** button enables you to create automatically a combination of data sets.

This mechanism can be useful, for example, if the administrator of a big company wants to know how many U.S.A. and Italian users there are in eleven selected OUs of the company.

In this way, the administrator has the possibility to choose two sets of objects, for example:

- 11 first level OUs (named A, B, C, D, ..., M)
- 2 attributes (named 1, 2)

and get the automatic combination of 22 data sets, as graphically shown below:



Datasets

A1	B1	C1	D1	E1	F1	G1	H1	I1	L1	M1
A2	B2	C2	D2	E2	F2	G2	H2	I2	L2	M2

Figure 117. Data set combinations.

The filters available (clicking **Filter/Hide Filter**) are **Name** and **Dataset Type**.

The data sets details/attributes and W/B list details are described in the table below:

Table 261. Data sets details/attributes.

Attribute	Description
Name	Data set name.
Created by	Data set author.
Creation Date	Date (dd/mm/yyyy) and Hour (hh/mm/ss) of data set creation.
Dataset Type	Label name.
Description	Brief description of data set contents.
White and Black Lists Details	
Attribute	**Description**
Organization Unit	OUs involved (White list)/ not involved (Black list) in the data set.
Users Attributes	Users attributes involved (White list)/ not involved (Black list) in the data set.
Applications	Applications involved (White list)/ not involved (Black list) in the data set.
Entitlements Attributes	Entitlements attributes involved (White list)/ not involved (Black list) in the data set.

⚠	**Note:** Removing a data set also removes the aggregated requests.

From the tabs on the right pane, you can view the subset of detailed data:

- **Details**. From this tab, you can view the detailed data of the selected data set.

- **History**
- **Data Filters**

Relevance criteria

The Relevance Criteria tab is described.

The buttons available in this section are:

- **Filter/Hide Filter**: allows you to show/hide the filters option.
- **Search**: allows you to get results according to the filter settings.
- **Add**: allows you to add an object to the W/B lists (available only in the right pane).
- **Remove**: allows you to remove objects from the W/B lists (available only in the center pane).

The only available filter in the **Relevance Criteria** tab is the **Name** filter. For a complete introduction to this section, see The Access approach.

Selecting an item from the **Relevance Criteria** tab on the left, the **Details** tab opens on the right.

Table 262. Relevance Criteria details.

Properties	Description		
Name	Risk criteria name		
Created by	Risk criteria creator		
Creation Date	Creation date (dd/mm/yyyy). Creation hour (hh/mm/ss)		
Description	Brief description of risk criteria		
Relevance attributes			
Name	**Description**	**ON**	**OFF**
User Relevance	Number of assigned permission	Considered in the risk analysis	Unconsidered in the risk analysis
	Number of SOD violations		
Entitlement Relevance	Number of assigned business activity		
	Number of SOD constraints		
Assignments Relevance	Similarity divergence		
	Last certification age		

History

The **History** tab on the right contains the list of requests performed on the selected risk criteria with different data sets in different data snapshots.

Note: The contents in this section are the same as those of of the risk analysis section. To start a new request, go to the risk analysis section.

In these frames, the following filters can be used for a request search (click **Filter/Hide Filter**):

Table 263. History filters

Attributes	Description
Status	• ! : Deleting data not allowed (Disabled) • ✓ : Data uploaded successfully (Completed) • ✗ : Error • ! : Warning (Old data snapshot)
Data Snapshot	Snapshot upload date. Click ⋯ **Data Snapshot** to quickly search for the data snapshot.
Dataset	Risk criteria name. Click ⋯ **Dataset button** to quickly search for the risk criteria.

Click **Details** in the upper section of the pane, to view the results of your request in the Map window.

See Map. For the functionality of the map, see Map management.

Monitor

The functions that are available for monitoring some elements are contained in the following list.

- Access Distribution
- Coverage Factors
- Access Trend
- "Access summary" on page 522
- Report
- "Scheduled tasks" on page 525

Access distribution

The access distribution and its related filters are described.

The risk distribution is used to consult the following analysis items:

- **Average Score**
- **Score**
- **Assignments**
- **Users**
- **Entitlements**

The filters available for this section are described in the table below:

Table 264. Access distribution filters.

Filter	Description
Dataset Name	Name of the data set analyzed.
Type	Dataset label name.

Table 264. Access distribution filters. (continued)

Filter	Description
Order By	These filters can be activated by selecting the corresponding check boxes under the filters text boxes: • **Average Score** • **Score** • **Assignments** • **Users** • **Entitlements**

The Dashboard Tree pane on the left (**Relevance Criteria** tab) lists the relevance criteria involved in the analysis, and the related snapshot.

By clicking the **DataSnapshot** tab, the same information is available, starting from the snapshot. The dashboard results reference information contained in the Dataset that is created according to the snapshot considered.

If there are no items selected in the Dashboard pane on the left, the filter section is disabled.

Clicking a single column, opens and displays the Risk Map (see also Map Management) for the selected OU.

Coverage factors

This section provides you with the graphical visualization of the analysis results.

Risk coverage is used to consult the following analysis items:

- **Assignments**
- **Users**
- **Entitlements**

In this section, searching is limited to the data set search and the only filter available is the Dataset Type filter. The dashboard tree pane on the left lists the snapshots involved in the analysis and the related data sets (second level of the hierarchy). By selecting the **Datasets** tab, the information is available starting from the data set view.

Clicking one of the red points, displays the related Risk Map (see also Map management) .

Access summary

The Analysis tab and its functions are described.

The **Analysis** tab, displays the access summary operation already performed. In this pane, you can find the following buttons:

- **Filter/Hide Filter**: allows you to show/hide the filters option.
- **Search**: allows you to get results according to the filter settings.
- **Add**: allows you to perform a new request.
- **Remove**: allows you to delete a request.

The following tables describe the filters for the access summary request and its related attributes:

Table 265. Analysis filters

Filter	Description
Data Snapshot	Click ⋯ **Search entity** to search requests from the data snapshot upload date. Click ⊗ **Clear** to clear the fields.
Dataset	Click ⋯ **Search entity** to search requests from the data set. Click ⊗ **Clear** to clear the fields.
Relevance Criteria	Click ⋯ **Search entity** to search requests from the relevance criteria applied. Click ⊗ **Clear** to clear the fields.
Status	Status of the request: • ✓ : Complete • ✓ : In progress • ✗ : Error • ! : Warning • ! : Deleting

Table 266. Analysis attributes.

Attribute	Description
Code	Progressive code number automatically attached to the request.
Data Snapshot	Analyzed data snapshot.
Dataset	Analyzed data set.
Relevance Criteria	Applied relevance criteria.
Status	Status of the request: • ✓ : Complete • ✓ : In progress • ✗ : Error • ! : Warning • ! : Deleting
Average Score	Score percentage.
Score	Quantity for evaluating access analysis.
Assignments	Number of involved assignments.
Users	Number of involved users.

Table 266. Analysis attributes. (continued)

Attribute	Description
Entitlements	Number of involved entitlements.

When you select a request and click 🔍 **Details**, the Map window displays.

For information about the map features, see Map.

From this entry point, you can select several Map analysis operations.

Access trend

In this section, you can view the results from the snapshot comparison and use them for monitoring the score trend.

Access trend is used to consult the following analysis items:

- **Average Score**
- **Score**
- **Assignments**
- **Users**
- **Entitlements**

This web interface is the desktop page of the module and allows the administrator to continuously monitor the access trend development before starting any new analysis.

The filters available for this section are described in the table below:

Table 267. Access distribution filters.

Attribute	Description
Dataset Type	Dataset label name.
View Graph	These filters are activated by selecting the corresponding check boxes in the Trend Analysis pane on the right: • **Average Score** • **Score** • **Assignments** • **Users** • **Entitlements**

The **Dashboard tree** pane on the left lists the snapshots involved in the analysis and the related data sets (second level of the hierarchy). By selecting the **Relevance Criteria** tab, the information are available starting from the **Relevance Criteria view**. Clicking one of the red points, shows the related Map (see also Map management).

Report

Scheduling and downloading are the main functions in Reports.

- Request schedules reports.
- Download downloads reports.

For unauthorized users, this menu is not available.

Scheduled tasks

In this section, are displayed all scheduled tasks still running or just started.

In the **Actions** menu, the **Remove** item allows you to remove the scheduled tasks from the list.

These tasks are scheduled using the **Task Planner** module.

Tools

Several functions speed up and facilitate the tasks of the following modules:

- Bulk Data Load
- Reset Flags

Bulk data load

Use this tool to upload a data snapshot that you can utilize for the Role Mining process.

To view the details of a bulk data load on the right pane, select one of the items listed under **Bulk data Load**.

The following details are listed:

Table 268. Bulk data load details

Detail	Description
Upload Date	The date and time that the upload of data was started.
Type	The data source. It can be: • IAG-DB • File Import
Status	One of the following upload states: • ✓ : In progress • ! : Deleting data not allowed (Disabled) • ✓ : Data uploaded successfully (Completed) • ✗ : Error • ! : Warning (Old data snapshot)
Start Date	Upload start date (mm/dd/yy; hh/mm/ss)
End Date	Upload end date (mm/dd/yy; hh/mm/ss)
Upload	
Item	**Description**
Org Units rows	Number of OUs rows uploaded or discarded
Users rows	Number of users rows uploaded or discarded

Table 268. Bulk data load details (continued)

Detail	Description
Applications rows	Number of applications rows uploaded or discarded
Entitlements rows	Number of entitlements rows uploaded or discarded
Entitlements Hierarchy rows	Number of entitlement hierarchies rows uploaded or discarded
Assignments rows	Number of assignments rows uploaded or discarded

Click Data to view the data uploaded.

To start a new bulk data load operation, click **Actions** > **Add**. The Import Type window displays the options for choosing the data source:

- File Import
- IAG-DB

Note: There is only one bulk data load at a time. Every time you add one, the previous one is automatically deleted. Only one data load is displayed at anytime.

Add data: File Import

When you choose **File Import** as the data source for the data snapshot or bulk data load operation, a window is displayed. You are required to provide data files for the following items:

- Organization Units
- Users
- Applications
- Entitlements
- Assignments

Optionally, for a bulk data load you can also provide a data file for entitlement hierarchies.

You are required to provide the following information For each type of data file:

Table 269. File import details

Attributes	Description
File location	Enter the name of the folder where the file is located. A **Browse** button is available.
File separator	The character used to separate fields in the file. For example, a semicolon (;).
File Name	The name of the file

Click **Load Data** to confirm the operation.

Click **Undo All** button if you need to clear all fields.

Click **Cancel** to cancel the data snapshot or bulk data load operation.

When the operation completes with success, the status changes to ✓ **Completed**. If errors occur, the status is ✗ **Error**.

If errors are returned, click **Back** to return to the file specification window and repeat the operation. The **Request History** phase is not available until the Upload phase is terminated.

Note: If errors occurred during the Data Validation process, the error type is shown in the same frame.
Attention: If the file format for the upload operations does not comply with the required format, a diagnostic window is displayed. Every incorrect value is traced.

Add data: IAG-DB Import

When you choose **IAG-DB** as the data source for the data snapshot or bulk data load operation, the data is loaded from the AG Core data base.

While the operation is in progress, the status is shown as ✓ **In progrss**. When the operation completes successfully, the status changes to ✓ **Completed**. If errors occur, the status is ✗ **Error**.

Reset flags

This section allows you to reset the flags for the exportation of the roles into the reports.

In the **Reset** tab (right), you can view the flag details:

Table 270. Reset details.

Detail	Description
Flag	Name of the flag.
Last Reset Date	Last date in which the flags have been reset (dd/mm/yyyy; hh:mm:ss)
Last Reset User	Last user who reset the flags.
Flags to Reset	Number of flags to reset.
Reset Flags	Number of flags already reset.
Misalignments	Number of unsuccessful reset operations.
Status	Status of the reset operation: • In Progress • Complete • Error

To reset flags, after selecting a flag in the **Flags** tab (left), click **Reset** in the **Reset** tab.

Settings

The following functions are available for setting values of some elements of the module:

- Attributes
- Data File Templates

User – Entitlement Attributes

When you select one of two categories (User/Entitlement) in the Attributes frame, 10 attributes (numbered from 0 to 9) appear in the Parameters Details frame.

Note that only the Attributes with selected check-boxes are displayed in the Analysis.

User Attributes can be coupled with **USER ERC column Names**, according to the USER ERC settings.

Mining Attributes

Select this tab to map parameters for bulk data loads used for role mining.

Map the parameters before you run the data snapshot. The mapping has no effect on an existing snapshot.

The **Parameter** tab lists the attributes that you can configure. Typically they are User attributes and Entitlement attributes.

Select a parameter to display a list of attributes on the right pane. The list contains ten editable fields where you can enter the name of an attribute.

Enter the names that you want to be displayed in the data snapshot.

For User attributes, you can enter names that replace the names of attributes of the User ERC table. The replacement is visible only in Access Optimizer.

Select the **Used** check box next to an attribute to make it available in the analysis.

Click **Save** to save your mapping.

Data file template

Use the data file templates to setup your import files before you run a data snapshot. You do not need to do this task if you plan to import the data from the IAG data base.

The data file templates are fixed structures that you must use to build your import files. The structure is common to all data types. It comprises the following column details for the file records:

Table 271. Column details

Detail	Description
Position	Position of the column in record
Name	Column name
Length	Column width in number of characters

Table 271. Column details (continued)

Detail	Description
Mandatory	Column is mandatory (Yes/No)
Key	Column is a key field. If true, it must be populated and duplicates yield errors.
Foreign Key	Secondary key
Description	Column description

Select a data type in the left pane to view the record structure in the right pane.

By default records are separated by a semicolon (;). You can use other separation characters, such as the vertical bar (|), or more than one character, such as |#|. To upload an empty value, in a not mandatory position, use two consecutive separators, for example:

```
;;
```

See the following import file examples for each data type:

- Organization Units
- Users
- Applications
- Entitlements
- Assignments

Organization units

The organizational units upload is described.

This is the sample text file for the organizational units upload:

```
11;Finance;

111;Temporary Assistance (Finance);11

12;Marketing;

121;Temporary Assistance (Marketing);12

.............

.....
```

There are four OUs in this sample file.

The OU code (11 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as an OU ID.

The OU name is in position 2. It is neither a mandatory element nor a key.

The parent OU code is in position 3. It is the parent of the OU in position 2. It is not mandatory but is a foreign key.

Therefore, the template item row is as follows:

OU Code;OU Name;Parent OU Code

For the Description field of position 3, you must follow the formatting rule described below:

- Organization Unit Parent ID. This field must be null for direct children of the root.

Users

The users upload is described.

This is the sample text file for the users upload:

```
EXMPL001;Sebrle;Vaclav;11;;20002406 - Member of   K Analysis Team;49000;305 - Finance
Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava -
Apolo;;;N-Z;20;3

EXMPL002;Neumannova;Katerina;11;;20002406 - Member of   K Analysis Team;49000;305 -
Finance Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava -
Apolo;;;A-M;12;0

EXMPL003;Sorokina;Elena;11;;20007693 - Revenue Assurance Specialist;49000;305 - Finance
Division;10003202 - Revenue Assurance & Billing Unit;10005801 - Revenue Assurance
Team;Bratislava - Apolo cebtrum;;;A-M;32;7
```

There are three users in this sample file.

The code (EXMPL001 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as a User ID.

The user surname is in position 2. It is a mandatory element but is not a key.

The user Name is in position 3. It is a mandatory element but is not a key.

The OU code is in position 4. It is mandatory and a foreign key.

User attributes are in positions 5-14.

Therefore, the item row is as follows:

User Code; User Surname; User Name; OU Code; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Permission; Number of SOD Violations

Applications

The applications upload is described.

This is the sample text file for the applications upload:

```
Active Directory

SAP

RACF

SAPIST

IRS

.............

.....
```

This sample file has five applications.

The application name is in position 1. It is a mandatory element and a data key.

Therefore, the item row is as follows:

Application Code

Entitlements

The entitlements upload is described.

This is the sample text file for the entitlements upload:

```
Supervizor;1;Active Directory;;;;;;;;;;a;23

Operator1;1;SAP;;;;;;;;;;a;54

Operator2;2;SAP;;;;;;;;;;a;10

SAP1;1;SAP;;;;;;;;;;a;6

CCA2;2;Oracle;;;;;;;;;;a:13

.............

.....
```

This sample file has five entitlements.

The entitlement name, with a maximum length of 256 characters, is a mandatory element in position 1.

The entitlement type, with a maximum length of 15 characters, is a mandatory element in position 2.

The application name in position 3 has a maximum length of 256 characters, is a mandatory element and is a foreign key.

The data described in the first 3 positions makes a unique set of data keys.

Entitlement attributes are in positions 4 to 13.

Therefore, the item row is as follows:

Entitlement Name; Entitlement Type; Application Name; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Business Activity; Number of SOD Constraints

The mandatory formatting rules described below apply to the Description field of positions 2 and 3:

- Types: 1) Profile 2) IT role 3) Job role.
- This field must be null for job roles. It will be replaced by the technical application `JOB_ROLE_APPLICATION`.

Assignments

The assignments upload is described.

This is the sample text file for the assignments upload:

```
Operator_Query;1;CLF;EXMPL001;28/06/2012

FRAUD;1;CLF;EXMPL001; 29/06/2012

INFOLINE_SUPER;2;SAPIST;EXMPL001; 28/07/2012

READ;1;IRS;EXMPL001; 29/07/2012

H_READ;3;;EXMPL001; 30/07/2012

.............

.....
```

This sample file has five assignments: three profiles (Type=1), one IT role (Type=2) and one job role (Type=3).

In this scheme, all elements are data key, foreign key and mandatories.

Position 1 contains the entitlement name, with a maximum length of 256 characters.

Position 2 contains the entitlement type, with a maximum length of 15 characters.

Position 3 contains the application name, with a maximum length of 256 characters.

Position 4 contains the user code, with a maximum length of 256 characters.

Therefore, the item row is as follows:

Entitlement Name; Entitlement Type; Application Name; Person Code; Last Certification Age

In the Description field of position 2 and 3, you can find the formatting rules described below that you must follow:

- Types: 1) Profile 2) IT role 3) Job role
- Job roles must have this field null. It will be replaced by the technical application `JOB_ROLE_APPLICATION`.

Mining Data file template

Use the mining data file templates to setup your import files before you run a bulk data load. You do not need to do this task if you plan to import the data from the IAG data base.

The data file templates are fixed structures that you must use to build your import files. The structure is common to all data types. It comprises the following column details for the file records:

Table 272. Column details

Detail	Description
Position	Position of the column in record
Name	Column name
Length	Column width in number of characters
Mandatory	Column is mandatory (Yes/No)
Key	Column is a key field. If true, it must be populated and duplicates yield errors.
Foreign Key	Secondary key
Description	Column description

Select a data type in the left pane to view the record structure in the right pane.

By default records are separated by a semicolon (;). You can use other separation characters, such as the vertical bar (|), or more than one character, such as |#|. To upload an empty value, in a not mandatory position, use two consecutive separators, for example:

```
;;
```

See the following import file examples for each data type:

- Organization Units
- Users
- Applications
- Entitlements
- "Entitlements hierarchy" on page 536
- Assignments

Organization units

The organizational units upload is described.

This is the sample text file for the organizational units upload:

```
11;Finance;

111;Temporary Assistance (Finance);11

12;Marketing;

121;Temporary Assistance (Marketing);12

.............

.....
```

There are four OUs in this sample file.

The OU code (11 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as an OU ID.

The OU name is in position 2. It is neither a mandatory element nor a key.

The parent OU code is in position 3. It is the parent of the OU in position 2. It is not mandatory but is a foreign key.

Therefore, the template item row is as follows:

OU Code;OU Name;Parent OU Code

For the Description field of position 3, you must follow the formatting rule described below:

- Organization Unit Parent ID. This field must be null for direct children of the root.

Users

The users upload is described.

This is the sample text file for the users upload:

```
EXMPL001;Sebrle;Vaclav;11;;20002406 - Member of   K Analysis Team;49000;305 - Finance
Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava -
Apolo;;;N-Z;20;3

EXMPL002;Neumannova;Katerina;11;;20002406 - Member of   K Analysis Team;49000;305 -
Finance Division;10003200 - K Management Unit;10003206 - K Analysis Team;Bratislava -
Apolo;;;A-M;12;0

EXMPL003;Sorokina;Elena;11;;20007693 - Revenue Assurance Specialist;49000;305 - Finance
Division;10003202 - Revenue Assurance & Billing Unit;10005801 - Revenue Assurance
Team;Bratislava - Apolo cebtrum;;;A-M;32;7
```

There are three users in this sample file.

The code (EXMPL001 in the sample) is in position 1, has a maximum length of 256 characters (like all other data in this set), is a mandatory element, and is a data key that must be interpreted as a User ID.

The user surname is in position 2. It is a mandatory element but is not a key.

The user Name is in position 3. It is a mandatory element but is not a key.

The OU code is in position 4. It is mandatory and a foreign key.

User attributes are in positions 5-14.

Therefore, the item row is as follows:

User Code; User Surname; User Name; OU Code; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Permission; Number of SOD Violations

Applications

The applications upload is described.

This is the sample text file for the applications upload:

```
Active Directory

SAP

RACF

SAPIST

IRS

.............

.....
```

This sample file has five applications.

The application name is in position 1. It is a mandatory element and a data key.

Therefore, the item row is as follows:

Application Code

Entitlements

The entitlements upload is described.

This is the sample text file for the entitlements upload:

```
Supervizor;1;Active Directory;;;;;;;;;;a;23

Operator1;1;SAP;;;;;;;;;;a;54

Operator2;2;SAP;;;;;;;;;;a;10

SAP1;1;SAP;;;;;;;;;;a;6

CCA2;2;Oracle;;;;;;;;;;a:13

.............

.....
```

This sample file has five entitlements.

The entitlement name, with a maximum length of 256 characters, is a mandatory element in position 1.

The entitlement type, with a maximum length of 15 characters, is a mandatory element in position 2.

The application name in position 3 has a maximum length of 256 characters, is a mandatory element and is a foreign key.

The data described in the first 3 positions makes a unique set of data keys.

Entitlement attributes are in positions 4 to 13.

Therefore, the item row is as follows:

Entitlement Name; Entitlement Type; Application Name; Attribute 0; Attribute 1;...; Attribute 9; Number of Assigned Business Activity; Number of SOD Constraints

The mandatory formatting rules described below apply to the Description field of positions 2 and 3:

- Types: 1) Profile 2) IT role 3) Job role.
- This field must be null for job roles. It will be replaced by the technical application `JOB_ROLE_APPLICATION`.

Entitlements hierarchy

The entitlement hierarchy upload is described.

This is the sample text file for the entitlement hierarchy upload:

```
I_EXT_CARE_ACADEMY_DELIVERY_R;2;YOYODYNE;I_EXT_PAMS_C;2;YOYODYNE

I_EXT_VERTU_PROJECT_C;2;YOYODYNE;I_EXT_VERTU_LOGISTICS_C;2;YOYODYNE

I_EXT_VERTU_PROJECT_C;2;YOYODYNE;I_EXT_VERTU_MANUFACTURING_C;2;
YOYODYNE

I_EXT_YOYODYNE_HR;2;YOYODYNE;I_EXT_YOYODYNE_HR_ADDITIONALS;2;
YOYODYNE

I_EXT_AMS_R;2;YOYODYNE;I_AMS_R;2;YOYODYNE

.............

.....
```

This sample file has five hierarchies.

In this scheme, all elements make up a unique set of data keys, foreign keys and mandatory elements.

The parent entitlement name in position 1 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

The parent entitlement type in position 2 has a maximum length of 15 characters, is a mandatory element and is both a data and foreign key.

The parent entitlement application name in position 3 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

The child entitlement name in position 4 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

The child entitlement type in position 5 has a maximum length of 15 characters, is a mandatory element and is both a data and foreign key.

The child entitlement application name in position 6 has a maximum length of 256 characters, is a mandatory element and is both a data and foreign key.

Therefore, the item row is as follows:

Parent Entitlement Name; Parent Entitlement Type; Parent Entitlement Application Name; Child Entitlement Name; Child Entitlement Type; Child Entitlement Application Name

The mandatory formatting rules described below apply to the Description field of positions 2, 3, 5 and 6:

- Types: 1) Profile 2) IT role 3) Job role.
- This field must be null for job roles. It will be replaced by the technical application `JOB_ROLE_APPLICATION`.
- The child entitlement type cannot be bigger than the one of the parent.
- This field must be null for job roles. It will be replaced by the technical application `JOB_ROLE_APPLICATION`.

Assignments

The assignments upload is described.

This is the sample text file for the assignments upload:

```
Operator_Query;1;CLF;EXMPL001;28/06/2012

FRAUD;1;CLF;EXMPL001; 29/06/2012

INFOLINE_SUPER;2;SAPIST;EXMPL001; 28/07/2012

READ;1;IRS;EXMPL001; 29/07/2012

H_READ;3;;EXMPL001; 30/07/2012

.............

.....
```

This sample file has five assignments: three profiles (Type=1), one IT role (Type=2) and one job role (Type=3).

In this scheme, all elements are data key, foreign key and mandatories.

Position 1 contains the entitlement name, with a maximum length of 256 characters.

Position 2 contains the entitlement type, with a maximum length of 15 characters.

Position 3 contains the application name, with a maximum length of 256 characters.

Position 4 contains the user code, with a maximum length of 256 characters.

Therefore, the item row is as follows:

Entitlement Name; Entitlement Type; Application Name; Person Code; Last Certification Age

In the Description field of position 2 and 3, you can find the formatting rules described below that you must follow:

- Types: 1) Profile 2) IT role 3) Job role
- Job roles must have this field null. It will be replaced by the technical application `JOB_ROLE_APPLICATION`.

Chapter 26. Introduction to Access Risk Controls for SAP

Access Risk Controls for SAP (ARCS) engine extends the capabilities of ARC to the authorization framework of SAP systems, enabling the implementation of a SoD analysis based on the SAP system transactions.

The activity-based SoD model defines SoD conflicts in terms of high-level business-oriented activities. This approach allows business experts to define and maintain SoD policy separately from the low-level entitlements, which are administered by IT specialists.

Starting from the activity-based SoD model of an organization, ARCS supports native inspection of SAP roles involved in the activities modeled and low-level SAP authorization objects.

The ARCS module enables you, using the functions implemented by the RBAC engine of the ISIG platform, to assign cluster roles to users of a SAP system; the cluster roles are defined as SAP roles aggregates.

A generic SAP role is composed by a specific set of transactions (T) and authorizations objects (AO).

The transaction object is a specific type of AO, which determines the elementary operation performed by the user on the system.

The real access privileges which a user has on a SAP system do not depend exclusively on the enabled transactions, but derive from the specific combination of AOs associated to the transaction.

The transaction represents the main object that determines what a user is enabled to do but this alone is not sufficient; it is necessary to analyze the combined presence of multiple AOs which determine what and how to operate using the transaction.

The ARCS module can perform a SoD transaction-oriented analysis considering possible AO combinations that can significantly modify the behavior of the transaction.

ARCS Data Model

The basic entities of the ARCS Data Model are in compliance with the main entities described in “IBM Security Identity Governance and Intelligence extended data model” on page 24.

The main differences regard the structure of the SAP Roles and Risk Entitlements.

From a Business Model point of view, a valid approach is to associate Risk Entitlements to the Business Activities hierarchy, that in ARCS is recognized as Business Activity Mapping.

For the purpose of modeling then, the:

- Business Activity Tree of ARCS is an exact clone of Business Activity Tree of ARC.
- The associations of Activities and Risks in ARCS are exact replicas of the ones defined in ARC.

To make and keep this correspondence over time, see “Activity Tree: aligning ARC to ARCS” on page 542.

For a coherent model, when Business Activity Mapping is defined on ARCS, we need to match it in ARC.

To obtain such alignment, see “Business Activity Mapping: ARCS to ARC” on page 541.

SAP roles and risk entitlements

Considering all the processing steps the ARC module provides the following indications.

A SAP role can be identified by:

1. A generic transaction Tk
2. A transaction set (T1, T2,... Tn)
3. A generic authorization object AOj
4. An authorization object set (AO1, AO2, ..., AOn)
5. The aggregation between one or several transactions with one or several authorization objects.

Usually, when a SAP role is aggregated to a generic transaction `Tk`, the SAP system automatically detects the authorization objects set which is needed to run the transaction `Tk`.

The most common case is the one described in bullet 5, where a SAP role is identified from the aggregation between TRs and AOs.

A risk entitlement can be aggregated to each SAP role.

A risk entitlement identifies a composition of a transaction and authorization objects that are a potential risk for the SAP system.

An example follows to better clarify this concept.

Consider the four different and structured SAP roles:

- SR1 (T1, O1, O2, O3)
- SR2 (T2, O4, O5)
- SR3 (T3, O1)
- SR4 (T3, O5)

Based on the TRs (T1, T2 and T3) and the AOs (AO1, AO2, AO3, AO4 and AO5), five risk entitlements are identified:

- RISK1 (T1, O1)
- RISK2 (T1, O4)
- RISK3 (T2, O5)
- RISK4 (T2, O3, O5)

- RISK5 (T3, O2, O5)

These five combinations of TRs and AOs can be a potential risk for the SAP system.

They are, therefore, aggregated in the following way:
- SR1 (T1, O1, O2, O3) -->RISK1 (T1, O1)
- SR2 (T2, O4, O5) ------> RISK3 (T2, O5)
- SR3 (T3, O1) -----------> RISK5 (T3, O2, O5)
- SR4 (T3, O5) -----------> RISK5 (T3, O2, O5)

If you consider two combinations of risk entitlements in SoD conflict:
- (RISK1, RISK2)
- (RISK1, RISK5)

you will easily recognize that a user U1, with assigned SR1 and SR2, is not enabled to perform potentially risky SAP operations, because the combination (RISK1, RISK3) is not in SoD conflict.

Consider now a cluster role composed by a set of SAP roles; consequently, also the cluster role is aggregated to a different risk entitlement set.

Consider two cluster roles:
- CR1 (SR1, SR2), that are automatically characterized by RISK1 and RISK3.
- CR2 (SR1, SR3), that are automatically characterized by RISK1 and RISK5.

Now consider again the same user U1 and assign to him CR2, in addition to SR1 and SR2.

The risky profile of U1 will evolve as shown below:

U1 ---> SR1, SR2 and CR2 ---> RISK1, RISK3, RISK5 ---> **SoD conflict ---> (RISK1, RISK5)**

Business Activity Mapping: ARCS to ARC

When a Business Activity Mapping is defined on ARCS, it is needed to align it into ARC.

To build a new Business Activity Mapping, you need to associate a Business Activity with an SAP Risk Entitlement, which is built on a set of Authorization Objects (AOs).

The SAP Risk Entitlement is associated with an SAP Role, through the AOs objects that characterize the SAP Role.

The SAP Role is related to an SAP Application.

To align the Business Activity Mapping in ARC, you need to define a new Permission (in AG Core) with the same name of the previous SAP Role.

The Permission must be associated to an Application named with the same name of the SAP Application.

According to this scheme, a scheduled Task, named **AccessRiskControls4SAPSync** (Task Planner module) automatically aligns the Business Activity Mapping that is built in ARCS to ARC.

If you want to test this aligning procedure, run the following steps:

1. Access the Task Planner module and select the **Manage** > **Task** tab
2. In the list of Tasks, verify whether the Task AccessRiskControls4SAPSync is active (✓ icon), otherwise select it and start it (**Actions** > **Start**)
3. In the **Manage** > **Task** > **Scheduling** tab, define the scheduling settings, and click **Save**.
4. In the Access Risk Controls module, associate an SAP Risk Entitlement to an Activity (go to **Manage** > **Business Activities** > **Risk Entitlement** and select **Actions** > **Add**).
5. In the Access Governance Core module, add a Permission (go to **Manage** > **Roles** and select **Actions** > **Add**) with the same name of the SAP Role that is related to the SAP Risk Entitlement (step 4).
6. The Permission must be added to an Application (**Manage** > **Applications** > **Permissions**) and its name must be the name of the SAP Application that is related to the SAP Role (step 5).
7. After the completion of the **AccessRiskControls4SAPSync** task, verify in the ARC module that the Business Activity Mapping is aligned (**Manage** > **Business Activity Mapping**).

Activity Tree: aligning ARC to ARCS

The Activity Tree of ARCS is a direct clone of the Activity Tree of ARC.

The ARC Activity Tree can vary any time.

Every Activity of ARC can be associated to a set of Risks (Business Model - RBAC Model).

In the fist period of administration of the operative environment, the structure of the ARC Activity Tree can vary and the same for the risk set that is associated to Activities.

When you add/remove an Activity into the ARC Activity Tree or if you associate a Risk to an Activity, a scheduled task, named **AccessRiskControls4SAPSync** (Chapter 28, “Introduction to Task Planner,” on page 637module) is engaged.

This task automatically aligns the ARCS Activity Tree or the relations Activity-Risk.

The scheduling period is decided by the administrator (generally, it's reasonable to schedule this task at least one time per day).

To test the alignment procedure, run the following steps:

1. Access the Task Planner module and select **Manage** > **Task** .
2. In the list of Tasks, verify whether the Task AccessRiskControls4SAPSync is not active (✗ icon), otherwise select it and stop it (**Actions** > **Stop**).
3. Go to **Manage** > **Task** > **Scheduling**, edit the settings, and click **Save**.
4. In the Access Risk Controls module, add/remove an Activity (**Manage** > **Business Activities** > **Actions** > **Add/Remove**).

After the run of **AccessRiskControls4SAPSync** task, verify the alignment of the ARCS Activity Tree (**Manage** > **Business Activities**).

Introduction to the ARCS-SAP adapter agent

The ARCS-SAP adapter agent is a specialized module of the IBM Security Identity Governance platform, integrated with the Access Risk Compliance Control for SAP (ARCS) module.

The ARCS-SAP adapter agent must be installed on the SAP side and is interrogated by the ARCS module to download specific data sets from the SAP server.

The scope of this documentation is to provide:

- An outline of the installation procedure for the ARCS-SAP adapter agent.
- A brief description of the agent functions.

The installation of the ARCS-SAP adapter agent does not require special prerequisites. The agent was developed and tested on the following SAP versions:

- R/3 4.6c
- R/3 4.7
- ERP 6.0

Distribution

The distribution structure is made for managing two distinct sets of Change Requests: Workbench Requests and Customizing Requests

Workbench Requests

In this area, you can make structural updates of the environment (for example, to drop or to update a table of the DB).

The distribution for Workbench is differentiated based on the type of SAP system coding.

If the SAP system is Unicode-based, you have to use the package `Unicode.zip`.

If it is a non-Unicode system, you have to use the package `Non_Unicode.zip`.

Each package is an SAP Change Request.

Each package contains exactly two files, named:

- Kxxxxxx.xxx
- Rxxxxxx.xxx

Customizing Requests

In this area, you can make customizations actions (for example, to add an authorization object or to update the configuration related to a process).

For the SAP system, the package `Role.zip` must be used.

Here you can find the definition of the role Z_ARCS_REMOTE.

Each package contains exactly two files, named:

- Kxxxxxx.xxx
- Rxxxxxx.xxx

Installation procedure

Before starting with the installation procedure, import the SAP libraries `sapjco3.jar` and `libsapjco3.so`.

For addressing this prerequisite, see the section related to the SAP libraries import.

To install the ARCS SAP adapter agent, you must perform the following steps:

1. Import the two preselected Change Requests into the SAP system (Workbench Requests (Unicode or Non-Unicode) and Customizing Requests).
2. Extract the two preselected packages: for each package, two files named `Kxxxxxx.xxx` and `Rxxxxxx.xxx` are extracted.
3. Copy the file `Kxxxxxx.xxx` into the directory `<DIR_TRANS>/cofiles`.
4. The owner of the files must be <SID> adm (or equivalent role in Microsoft environment) and the permissions must be set to 755.
5. Copy the file `Rxxxxxx.xxx` into the directory `<DIR_TRANS>/data`.
6. The owner of the files must be <SID> adm (or equivalent role in Microsoft environment) and the permissions must be set to 755.
7. Import the change requests into the target system:
   - In the STMS transaction, select the import buffer of the target system.
   - Append the two CR <SID>`Kxxxxxx` to the import buffer.
   - Import the two CR <SID>`Kxxxxxx` into the target system.
8. In the SU01 transaction, create a user of type “Communication” and then assign it to the SAP role Z_ARCS_REMOTE.

Generally, the suffix *<DIR_TRANS>* coincides with the path `/usr/sap/trans`.

However, this indication might vary from system to system.

ARCS-SAP adapter agent functions

The agent functions are:

- z_start_synch
- z_get_job_status
- z_get_synch_data
- z_get_single_role
- z_get_tcode

z_start_sync

This feature creates a SAP job that makes mass extractions of SAP authorization data and populates the relative data and log tables.

Synchronization can be done in the following modes:

- Delta mode: if the parameter `SYNCH_DELTA_DATE` is set
- Full mode: if the parameter `SYNCH_DELTA_DATE` is not set

The job is called dynamically.

For a Delta mode extraction the job is called Z_CCS_SYNCHDATA_DELTA.

In case of a Full mode extraction the job is called Z_CCS_SYNCHDATA_FULL.

The two tables below show all the parameter features, grouped according to Input (Import) or Ouput (Export) parameters:

Table 273. z_start_sync - INPUT parameters.

Field	Type	Dimension	Values	Description
SYNCH_DATA	Numeric	1	0	Extraction of all data types
			1	Extraction of roles and other data Extracted roles are all those associated to authorization objects (OA) (table agr_1251) to obtain the object detail which is then used to create the range. For the extraction of other data, a range containing the transactions (table tstc) is first created. OAs are associated to every transaction (table usobt_c). Therefore, for each OA, reference is made to the tactz table (range created in the Role extraction phase) to obtain the ACTVT value.
			3	Account details extraction First, all accounts are extracted from the table usr04. With the USR_USER_PROFS_PROFILES_GET function, all profiles associated to the account are extracted. Finally, using BAPI_USER_GET_DETAIL all account details, such as name and surname, are read.
			4	Massive profile extraction Access to the table usr10 with the filter set to type "G"
			5	Extraction of all the roles Access to the table agr_define
SYNCH_DELTA_DATE	Dats	8	ggmmaaaa	To be set for Delta mode If not set, full synchronization will be assumed.

Table 274. z_start_sync - OUTPUT parameters.

Field	Type	Dimension	Values	Description
SYNCH_DATE	DATS	8	ggmmaaaa	Synchronization data

z_get_job_status

This function returns the status and log of the SAP job launched with the z_start_synch command.

The function reads the job name from the job summary table (TBTCO), and if multiple jobs are present, selects the last in order of date/time.

Output (Export) parameters are described in the following table:

Table 275. z_get_job_status - OUTPUT parameters.

Field	Type	Dimension	Values	Description
JOB_STATUS	CHAR	1	R, A, F, C	Indicates the status of the job: • R: Ready • A: Active • F: Finished • C: Cancelled
START_TIMESTAMP	CHAR	14	ggmmaaaaoommss	Job start date/time
END_TIMESTAMP	CHAR	14	ggmmaaaaoommss	Job end date/time
RUNTIME	CHAR	6	oommss	Job execution time
SYNCHTYPE	CHAR	5	DELTA, FULL	Synchronization type

z_get_sync_data

This command allows the ARCS module to receive packaged authorization data from the tables in the queue.

The packet size can be configured by setting the Input (Import) parameters which will define the package number and size as well as the type of data to be extracted.

This data is taken from the custom tables based on the value of SYNCH_DATA.

This type of transmission helps avoiding possible timeout issues related to SAP processes and ensures data consistency if the system should fail during the transmission between SAP and ARCS.

Table 276. z_get_sync_data - INPUT parameters.

Field	Type	Dimension	Values	Description
PACKET_NUM	CHAR	16		Identifies which packet must be sent
PACKET_SIZE	CHAR	8		Identifies packet dimension (Num. of table records)
SYNCH_DATA	NUMERIC	1	1, 2, 3, 4, 5	Identifies type of data to be extracted: • 1: Roles • 2: Other data • 3: Accounts • 4: Profiles and profile types • 5: Collective roles

Table 277. z_get_sync_data - OUTPUT parameters.

Field	Type	Dimension	Values	Description
ROLE_DATA	CHAR	TBD		Package with the required data describing the structure of a single SAP role
OTHER_DATA	CHAR	TBD		Package with required data

The following tables describe the structure (data track) of the packages:

- ROLE_DATA
- OTHER_DATA

Table 278. ROLE_DATA.

Field	Elementary Data	Type	Dimension	Description
AGR_NAME	AGR_NAME	CHAR	30	Role
TEXT	AGR_TITLE	CHAR	80	Role description
OBJECT	XUOBJECT	CHAR	10	Authorization object (OA)
ATEXT	XUTEXT	CHAR	60	OA description
TIMESTAMP	ZTIMESTAMP	CHAR	14	Timestamp from the last OA modification
FIELD	XUFIELD	CHAR	10	"FIELD" field name
VON	XUVAL	CHAR	40	"From" value
BIS	XUVAL	CHAR	40	"To" value

Table 279. OTHER_DATA.

Field	Elementary Data	Type	Dimension	Description
ID_DATA	ZTRAK	CHAR	1	Identifies two types of data, characterized by the same structure (record track), distinguished by the letters A or B
NAME	TCODE	CHAR	20	Cod. transaction
TEXT	TTEXT_STCT	CHAR	36	Transaction description
OBJECT	XUOBJECT	CHAR	10	OA
ACTVT	ACTIV_AUTH	CHAR	2	ACTVT value: • A: transaction scope • B: explosion diagram for the asterisks

z_get_single_role

This function returns the authorization information to ARCS for an individual role, provided as an Input (Import) parameter.

Table 280. z_get_single_role - INPUT.parameters.

Field	Type	Dimension	Values	Description
ROLE_NAME	CHAR	30		Unique SAP role identifier

Table 281. z_get_single_role - OUTPUT.parameters.

Field	Type	Dimension	Values	Description
ROLE_DATA	CHAR	TBD		Package with the required data describing the structure of a single SAP role

z_get_tcode

This function returns to ARCS the existing transaction codes associated to the Input (Import) data values.

Table 282. z_get_tcode - INPUT parameters.

Field	Type	Dimension	Values	Description
TCODE_FROM	CHAR	20		Initial code of the transaction to be searched for
TCODE_TO	CHAR	20		Final code of the transaction to be searched for

Table 283. z_get_tcode - OUTPUT parameters.

Field	Type	Dimension	Values	Description
TCODE_DATA	CHAR	TBD		Data structure of the transactions found

The following table describes the structure (data track) of the package TCODE_DATA:

Table 284. Structure of TCODE_DATA.

Field	Elementary Data	Type	Dimension	Description
TCODE	TCODE	CHAR	20	Transaction code
TTEXT	TTEXT_STCT	CHAR	36	Transaction description

ARCS-SAP adapter Agent:User Role

For integrating two systems, IGI and SAP, a custom role that is named Z_ARCS_REMOTE is needed.

This role manages the authorization for:

- RFC calls
- Creating of jobs

For examining the structure of the role, proceed as follows:

1. Log in to SAP console.
2. In **SAP Easy Access** pane window page, specify the name of transaction: PCFG
3. Click green icon on the left (or click **Enter** by keyboard).
4. In the filter **Role**, set the name of the role: Z_ARCS_REMOTE.
5. Click **Display** button.
6. Select the tab **Authorizations**.
7. Click **Display Authorizations Data** button.
8. Now you can view the hierarchical structure of the role Z_ARCS_REMOTE
9. Clicking the nodes of the hierarchy you can browse into all components of the role.

The Z_ARCS_REMOTE is structured into two main segments:

- Segment AAAB (Cross-application Authorization Objects).
- Segment BC_A (Basis: Administration).

Manage

The following functions for managing the main entities of this module are available:

- Business Activities
- Business Activity Mapping
- Risk Definitions
- Domains

Business activities

You can view the business activity details and other information of the data model that are related to them.

In the left pane **Business Activity** are present two tabs.

In the **Tree View** tab, you can:

- Browse in the business activity tree for selecting the wanted activity.
- Add or remove activities (**Actions** menu)

In the **Search** tab is available the set of filters to search for an activity (click **Filter/Hide Filter**) and the **Actions>View** for toggling to the **Tree View** tab.

The table lists the available filters:

Table 285. Business activity filters.

Filter	Description
Name	Name of the business activity.

Table 285. Business activity filters. (continued)

Filter	Description
Identifier	The univocal identifier of the business activity.
Description	Brief description of the business activity.

The contents of the right pane changes depending on the tab clicked in the upper side of the pane. When the Business Activity web interface is accessed, the **Details** tab is active by default. Under this tab are available two different panes:

- **Activity details**
- **Activity property**

After an activity is selected in the left pane, the **Activity details** pane shows the related data that is contained in the AGCore database.

The table lists the activity details:

Table 286. Activity details.

Detail	Description
Parent Activity	Name of the parent activity (automatically set after the activity selection in the left frame).
Name	Name that is used within the organization to identify the activity.
ID Code	The univocal identifier of the activity.
Description	Brief description of the activity.
Owner	User who is responsible for the considered activity. Use the ⋯ **User** button on the right side of the attribute box to insert a user.

An activity can be aggregated to a set of properties that characterize it.

The Activity property pane displays properties that can add specific information to the selected activity.

For example, a property can have, as value, an external link to the set of implementing regulations and standards compliance that must be implemented by that activity. Another example consists of considering the values of properties into the structure of a rule.

A property is identified by a pair of attributes <Name,Value>.

Note:

It is possible to have multi-values properties, where a property **`PROP_1`** is indicated in two or more different rows and, in every row, is indicated a different value.

In the list, are described the main operation groups that are related to the business activities:

- Details

- “Risk entitlements”
- “Risk memberships” on page 336
- “Applicable domains” on page 337

Risk entitlements

In this section, you can link risk entitlements to activities.

Selecting an activity from the left pane, the **Risk Entitlements** tab (right) is enabled and shows a list of the risk entitlements associated to the selected activity.

From the **Risk Entittlemnts** tab, you can **Add** or **Remove** a risk entitlement (**Actions** menu).

For adding a risk entitlement, by clicking **Actions > Add** , the window Add Risk Entitlement opens. In this window, the following filters can be used for the risk entitlement search (click **Filter/Hide Filter**):

Table 287. Permission filters.

Filter	Description
SAP system	Name of the SAP system for filtering risk entitlements. Use the ⋯ **Set SAP system** button on the right side of the attribute box to set the SAP system.
Type	Type of filtered risk entitlements. Use the ⋯ **Set Risk Entitlement Type** button on the right side of the attribute box to set a permission type.
Name	Risk entitlement name.
Status	This filter can have one of the following four values: • **TBD**: when a risk entitlement is not associated to any activity but is not in the status Ignored or Missing Activity. • **Linked**: a risk entitlement is associated to an activity. • **Ignored**: when a risk entitlement is not associated to any activity. • **Missing Activities**: when the operator does not know to which activities to associate the risk entitlement.

Risk memberships

This section allows you to display all risks aggregated to a selected activity.

The **Risk Membership** tab contains the list of risks associated with the activity selected in the left frame.

Selecting a risk from the list and clicking **Actions>Risk**, the Activities risk window opens displaying the list of all activities associated with the risk selected.

If the **Hier** column is flagged with the ✓ icon, the Risk selected is associated with all activities included in the selected activity.

After selecting an activity, by clicking **Actions>View**, the Tree View window opens and displays the exact position of the activity in the hierarchy.

Applicable domains

This section allows you to display all domains aggregated to a selected activity.

The **Applicable Domains** tab contains the list of domains that are already aggregated to the activity selected in the left frame. In the **Applicable Domains** tab, the filters that can be used to perform a domain search are **Name** and **Description**.

Activities and permissions

From this tab, you can associate the permissions to one or more activities.

The relationship between activities and permissions is "many to many".

An activity can be described using a set of aggregated permissions that are necessary for its implementation; in addition, a single permission can be aggregated to more than one activity.

In the **Permission** tab (left), you can search for a specific permission according to the filters summarized below (clicking **Filter/Hide Filter**):

Table 288. Permission filters.

Filter	Description
Application	Name of the application in which the illegal permission are filtered. Use the ⋯ Set Application button on the right side of the attribute box to insert an application.
Type	Type of filtered permission. Use the ⋯ Set Permission Type button on the right side of the attribute box to insert a permission type.
Name	Permission name.
Status	This filter can have four values: • **TBD**: when a permission is not associated to any activity but is not in the status Ignored or Missing Activity. • **Linked**: a permission is associated to an activity. • **Ignored**: when a permission is not associated to any activity. • **Missing Activities**: when the operator does not know to which activities to associate the permission

The results are displayed in the same pane according to the attributes summarized below:

Table 289. Permission attributes.

Attribute	Description
Status	Status of the permission.
Name	Name of the permission.
Type	Type of application.
Application	Name of the application.

From the **Permission** tab, by clicking a permission, the **Details** tab (right) is enabled.

In the upper section of this pane information is displayed about the selected permission and two check boxes that allow to switch the status of the selected permission: from TBD to Ignore or Missing activity.

Table 290. Permission details.

Detail	Description
Name	Name of the permission.
Application	Name of the application.
Description	Brief description of the permission.

To add an activity, click **Add** and, from the Add window, choose the desired activity from the **Tree view** tab or clicking the **Search** tab entering the filters for the search operation (clicking **Filter/Hide Filter**).

Table 291. Activity filters.

Filter	Description
Name	Activity name.
Identifier	Unambiguous identifier of activity.
Description	Brief description of the activity.

To remove an activity, in the **Details** tab from the list of the associated activities, select the desired activity, then click **Remove**.

When the Permission-Activity association is removed, the status of the permission returns in TBD status.

After the desired operation has been performed, click **Save** in the bottom right part of the pane.

ℹ	**Note:** When a permission is in Linked status, it is not possible to switch it to any other status. To switch the status of the Linked permission is necessary to remove the associated activity.

Risk Definitions

This page lists the risks defined in the system and their associated activities.

The `Risk` tab on the left displays the list of risks defined in the system.

Use the `Filter` button to find a specific risk definition or to narrow down the search to specific definitions. The following filters are available:

Table 292. Available filters to find a Risk definition.

Filter	Description
Name	Risk name
Description	Description of the risk
Status	Risk status. It can be: **Assigned Risk** The risk is already assigned to the mitigation **Not Assigned Risk** The risk is not yet assigned to the mitigation
Type	The risk type. It can be: **Risk** A possible threat or potential damage **SoD** A segregation of duties conflict

The list of risk definitions is imported from Access Risk Control.

As you select a risk definition from the list in the Risk tab, its details are displayed on the right. The details are:

Table 293. Details of a Risk definition.

Detail	Description
Name	Risk name
Description	Description of the risk nature
Type	Type of risk (**SoD** or **Risk**)
Scope Type	Type of visibility scope: • **Model**: Risk is assigned as a user role • **Scope**: Risk is assigned directly to a user (owner) • **Both**: Risk can be assigned using a model or a scope
Level	Level of risk (measured from 0 to 9)
Impact	Description of the risk impact
Likelihood	Value between 0 and 1
Tolerance	Description of the risk tolerance
Trend	Description of the risk trend
Risk acceptance rational	Description of the manageable risk acceptance. Risk acceptance is a value < tolerance
Owner	Name of the person responsible for an activity in a company. Use the ⋯ **User** button on the right side of the attribute box to insert a user (owner)
Creation Date	Date of the risk creation (dd/mm/yyyy; hh/mm/ss)

Click the **Activity** tab in the right-hand page to display the list of activities associated with the selected risk. Select an activity and click **Actions** > **View** to view the exact position of the selected activity in the tree structure of business activities. You can run this task also by:

1. Selecting a risk definition from the list in the left page.
2. Clicking **Actions** > **Risk** to display a panel with the associated activities.
3. Selecting an activity and clicking **Actions** > **View**.
4. Scrolling the tree structure until you find the highlighted activity.

Domains

In this section, you can define an unlimited number of domains.

The **Domain** tab contains the list of domains registered in the system. Select a domain to view its details in the **Details** tab.

In the **Domain** tab, a domain can be added (**Add** button) or removed (**Remove** button).

The filters available for a domain search are name and description (click **Filter/Hide Filter**).

The domain details are described in the table below:

Table 294. Domain details.

Detail	Description
Type	Type of domain.
Name	Name of the mitigation action.
Description	Brief description of the mitigation.
Extended Description	Extended description.
Note	This attribute can be utilized to indicate a specific message.

In the list below are shown the main operation groups related to the domains:

- Details
- Permissions
- Applications
- Mitigation Controls
- Activities

Permissions

In this section are available the procedures to aggregate permissions to domains.

In the **Permissions** tab are listed all the permissions already aggregated to the domain selected in the **Domain** tab. In the same pane it is possible to add and remove a permission by clicking **Add** or **Remove**.

Clicking **Add**, opens the Add window that shows the list of all permissions listed in the system.

In the **Permissions** tab and in the Add window, the following filters can be used for the permissions search (click **Filter/Hide Filter**):

Table 295. Permissions filters.

Filter	Description
Application	Application of the permission. Use the … **Set Application** button on the right side of the attribute box to insert an application.
Name	Name of the permission.
Type	Type of permission. Use the … **Set Permission Type** button on the right side of the attribute box to insert a type.

Applications

In the **Applications** tab are listed all applications already aggregated to the domain selected in the **Domain** tab.

In the same tab you can add and remove an application by clicking **Add** or **Remove**.

Clicking **Add** opens the Add window that contains the list of all applications listed in the system.

In the **Applications** tab and in the Add window, the **Name** (name of the application) filter can be used for applications search (click**Filter/Hide Filter**).

Mitigation controls

In the **Applicable Domains** pane are listed all the mitigations already aggregated to the domain selected in the **Domain** tab.

In the same pane you can remove a mitigation by clicking **Remove**. The **Add** pane contains the list of all the mitigations listed in the system. From this pane, you can add a mitigation to a domain by clicking **Add**.

The filters available for a mitigation search are **Name** and **Description** (click **Filter/Hide Filter**).

Activities

This paragraph allows to view the activities aggregated to a domain.

In the **Activities** tab are listed all the activities already aggregated to the domain selected in the **Domain** tab, on the left. In this tab, the following filters can be used for the permissions search (click **Filter/Hide Filter**):

Table 296. Activities filters.

Filter	Description
Name	Name of the activity.
Identifier	Univocal identifier of the business activity.
Description	Description of the activities.

Configure

The following functions for configuring the main entities of this module are available:

- Configuration Set
- SAP System
- Rules

Configurations

Different configurations can be activated for testing different authorizations patterns.

A configuration is built by:

- A set of business activities
- A set of conflicts that are associated to the activities
- A set of domains

In the **Configuration** tab is listed all the configurations available.

The filters **Name** and **Description** can be used for the configuration search (click **Filter/Hide Filter**).

Select a configuration and click **Actions** > **Current** for setting the ✓ working configuration.

Click **Actions** > **Add** for adding a configuration.

The new configuration can be empty or copied from an existing configuration.

In this last one case, you can decide whether to copy the entire configuration or select only some elements:

- Only the activities
- The activities and all the associated conflicts
- Some specific domain or all registered domains

Select a configuration and click **Actions** > **Edit** for changing the settings of the configuration.

SAP System

This section describes the basic operations that you can use to manage your SAP systems.

The **SAP system** tab displays a list of the SAP systems available to Access Risk controls for SAP.

You can enter a SAP system name and description as filters to find a particular system or group of systems (after clicking **Filter**).

As you select a SAP system, the SAP system details are displayed on the right.

After you select a SAP system, click **Actions** to:

- Make the SAP system the one in use, by clicking **Switch**.

- Add a SAP system.
- Remove the SAP system.

Under **SAP system details** you can view and edit the SAP system:

- Name
- Description
- IAM Target
- Realm

You can also set the connection parameters of the SAP System and verify the connection. You can set the following connection parameters:

- User ID
- SAP Client
- Password
- Packet size
- System number
- Version
- Language
- Host Name

Rules

Use rules to manage events based on event types or to automate particular policies for making interactions with SAP systems.

Only one Rule Class is available:

- **Advanced** groups all the rules that can be scheduled through Task Planner, for customizing SAP interactions.

The **Actions** menu of the tab **Rules** in the left frame lists the following actions:

Import
For importing the XML representation of a Rule or of a Rule Sequence (Rule Flow).

Export
For exporting a Rule or a Rule Sequence (Rule Flow).

Add
Adds a Group of Rules (function that is maintained for legacy reason).

Remove
Removes a Rule or a Group of rules (for Groups, function that is maintained for legacy reason).

Enable/Disable
Enable or disable a Rule execution into a sequence.

Move Up/Down
Move the Rule up/down in the Rule sequence.

Find the following accordion panes in the right frame:

Rules Package
Includes functions that manage the Rule that is selected in the left frame.

Package Imports
Includes functions that manage rule packages.

Rules Package

This pane includes functions that manage rules with the Rules editor.

Based on your selections in the left tab **Rules**, a set of rule are listed in this pane.

The **Actions** menu lists the following actions:

Verify Checks the formal structure of the code that defines a rule (needs the selection of one of the rule listed).

Modify
Opens the Rules editor to modify a rule.

Delete Deletes a selected rule.

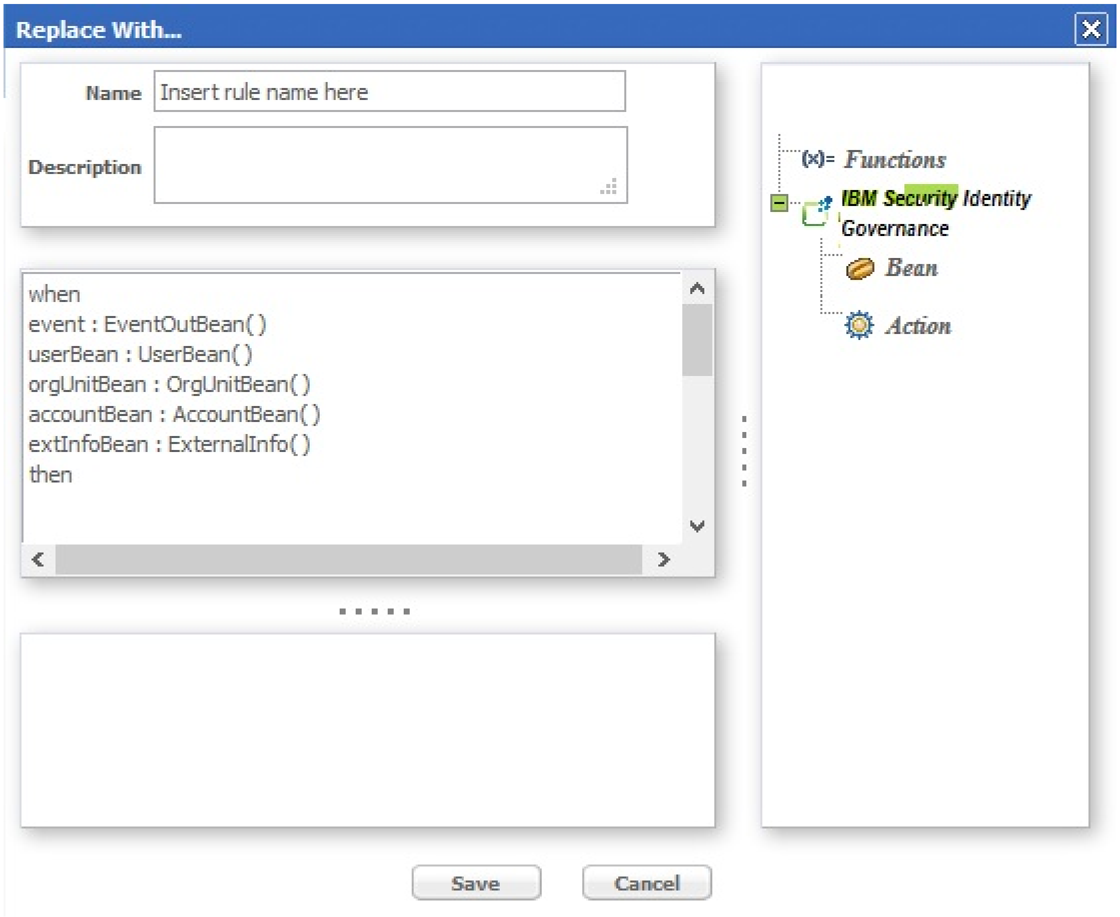
Create Creates a rule.

Add
Adds a rule that is selected in the list to a **Group** (legacy versions) or **Rule Sequence** that is selected in the **Rules** tab, on the left.

Rules Editor

The Rules Editor speeds up the writing of code contained in a Rule.

The next figure shows the Rules Editor panel:



```
when
event : EventOutBean()
userBean : UserBean()
orgUnitBean : OrgUnitBean()
accountBean : AccountBean()
extInfoBean : ExternalInfo()
then
```

Figure 118. The Rules Editor panel.

The next table shows what buttons and icons are present in the Rules editor:

Table 297. Symbols of the Rules editor.

Icon	Description
C	Import a Java class
C	Java class
	New variable
(x)=	New function
	Bean
⚙	Action
	Associated rule: rule that is associated to a rules group
	Split: used to construct flow processes in situations that require a branch point.
◇	Constraints
📁	Rules group

Table 297. Symbols of the Rules editor. (continued)

Icon	Description
	Flow process

All the Rules must have the following structure:

- **Condition Area** (between “when” and “then”)
- **Action Area** (immediately after “then”).

The word **when** identifies the beginning of the conditions area.

Any number of conditions can be inserted and the actions will be executed only if all the conditions are verified (logic AND between each condition)

The word **then** identifies the beginning of the actions area.

Actions are written in normal Java code; all classes making up the libraries delivered with the product are available for writing actions.

A complete list and descriptions are available in the **Replace with...**.

The conditions are written according to Drools syntax.

Every condition verifies, within the Working Memory, whether or not there are one or more objects identified by the Beans. If such objects are actually found, the actions described above will be executed on them.

The **Replace with...** window contains the code obtained from the Editor.

From the frame on the right side of the window, predefined code blocks can be selected and placed directly into the **Replace with...**.

The objects are grouped in a hierarchy and managed through a tree structure.

The **Object** frame contains the nodes corresponding to the higher level object categories. The two initial main categories are:

- Functions
- Ideas

Based on the selection, the objects can be **Functions**, **Bean** or **Action** and their methods are visible below the selected object (fourth level of the tree):

Now, select a leaf object (a method) and insert it into the **Replace With...** frame (left) using the **Actions**>**Add** button.

This operation can be performed to modify or create a Rule.

Note: The name of a Bean can be written without its system path ONLY if it has been imported into the Package that contains the Rule.

Functions

The Functions category contains functions for fundamental Rule-writing constructs; the same frame lists the following four elements:

- if
- ifelse
- ifelseif
- for

Select one of the functions and click **Add** to insert the related parametric code into the **Replace with...** frame, at the end of the already-listed code. The parameters to edit are easily recognized because they are between two '$' symbols.

For example, in the IF ELSE construct, you have to edit the parameters CONDITION1, ACTION1 and ACTION2.

Proceed in one of two ways to edit the parameters:
- Directly write the code instead of the corresponding symbolic string (e.g., CONDTION1 included between two '$' characters);
- Use the editor again.

In this last case, click **Field** > **Bean** > **AccountBean** and select one of the objects listed, then click **Add**:

Selecting $ACTION2$ places the selected code block in the position that was covered by $ACTION2$. If none of the parameters in the window are selected, click **Ok** to place the code block at the end of the already-present code. To eliminate a potentially wrong insertion, cancel the corresponding code directly in the **Replace With...** frame.

Bean and Action Elements

The IBM Security Identity Governance folder contains the following two folders:
- Bean
- Action

These folders contain ALL the Beans and Actions imported into the Rules Package; in particular, the Bean folder contains the Beans imported into the Package that are part of the libraries delivered with the product. Client users of the AG Core can create additional personalized Beans.

This paragraph analyzes how to use a Bean in the Bean folder. By selecting Bean, the content of the Bean folder is presented in the form of a tree, where every Bean is a node and its child nodes represent its methods.

After selecting the Bean, click Add to insert it into the **Replace With...** frame.

Be sure to insert a semicolon (;) at the end of each line and put the code in order.

Be sure to assign the String parameter a string that makes sense.

The Action folders contain ALL Actions imported into the Package of the selected Rule; in particular, the Action folder contains all Actions imported into the Package that are part of the libraries delivered with the product.

The procedure for inserting Actions (even custom Actions) is exactly the same as that for inserting Beans.

Package Import

This pane includes functions that import and configure rule packages.

From the tabs bar, select **Configure** > **Rules** then click on the **Package Import** accordion pane on the right.

Configuring a Package consists of declaring certain objects available to all Rules in the Package.

Such a declaration consists of specifying an appropriate Java code in the allotted text box.

To make configuration of the Packages easier, insert blocks of predefined code (on the right side of the frame there is a small vertical toolbar with buttons).

The following actions are available for each Package:

- Import specific classes
- Insert variables
- Insert functions

The Rules programmer can write the Rule's code to directly call the objects that are set up for the Package containing the Rule.

Importing a class into a Package adds a class to a Rule without having to specify the entire path.

For example, after importing the class UserBean() into the Package, it is possible to directly write `UserBean()` instead of `com.engiweb.profilemanager.common.bean.UserBean()`.

Package Editor

An administrator familiar with programming languages can insert any object in the Package by writing the code directly in the text box.

A Package Editor is also available to assist administrators to accomplish this task.

The Editor uses the following buttons, located on the right-hand side of the text box:

- New Import
- New Variable
- New Function

Variables usually support objects that are already instanced with global visibility to all the Rules of the Package; if, for example, there is an object that contains all the parameters required to connect to the DB, the object can be assigned to an "sql" variable (always visible to the Package's Rules) and can be used in the Rule code, as shown in figure above.

Lastly, it is possible to create Functions that always have global visibility to all the rules of a package. For example, if several rules request an operation for the arithmetic average of two numbers, this can be created directly in the Package instead of in each single rule.

Import a Class

To import a class, click on **New Import** button in the vertical toolbar on the right-hand side of the Package Imports pane.

The Classes window opens (figure below) with a list of available classes

Choose a class, then click **Ok**.

The Java code corresponding to the selected class is written in the text area on the right-hand side of the Replace With... window.

Enter a New Variable

To insert a new variable, click on **New Variable** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Insert the object (specify entire system path) in the space <your class here>.

Insert a variable name in the space <variable name>; this name can then be used in every Rule of the Package.

Enter a New Function

To insert a new function click on (x)= **New Function** in the vertical toolbar on the right-hand side of the Package Imports accordion pane.

The text box displays the code corresponding to the declaration of a new variable.

The code is parametric and thus must be edited in the allotted spaces, defined by the characters <>.

Edit the parameters as follows:

- Replace <return Type> with the type of objects that result from processing the function (e.g. an integer, a string, a class, etc.).
- Replace <args here> with the list of parameters given to the function at input.
- {} needs to contain the body of the function, i.e., all the code that implements the function.

How to schedule a rule sequence

You can link a sequence of rules to a scheduled job.

The Task Planner module is dedicated to scheduling several types of jobs that optimize different tasks in the Identity Governance and Intelligence platform.

After you create a rule flow in Access Governance Core or in other modules, open the upper toolbar and click .

In Task Planner, select **Manage** > **Jobs** to access the Job Classes GUI.

From the list of **Job Classes**, choose AdvancedRuleFlow or DeferredEventsRuleFlow (depending on what your requirement is) and choose a relevant job from the resulting list.

In the lower frame of the **Details** tab, you find the parameters of the Job Class that you can set with the suitable values.

Monitor

The following functions for monitoring the main entities of this module are available:

- User Violations
- SAP Role Violations
- SAP Authorization Violations
- Role Warnings
- Reports

User Violations

This section enables you to view:

- Information on risky or conflicting activities related to a selected user
- Domains and activities that are associated with a user
- SAP Roles and Authorizations associated with a user

The User Violations tab displays conflicting users listed by the system for SoD and FSoD violations.

A user is qualified as `conflicting` as a consequence of having two or more SAP authorizations that are in conflict.

You can use the following filters to find a conflicting user (after clicking **Filter**):

Table 298. Filters to find conflicting users

Filter	Description
Organization Unit	OU to which the user belongs. Use the **OU Search** button on the right to get a list of OUs.
Hierarchy	When this check box is selected, the operation is executed starting from the selected OU root and down through the entire subtree originating from the root.
Search Identity	The user's name, last name, or ID.
DN	The distinguished name of the user.
Search Type	Can be: **All** The search is made on all users **Conflicting** The search is made on conflicting users only.

Table 298. Filters to find conflicting users (continued)

Filter	Description
Conflict level	Can be: - Low - Medium - High This filter becomes unavailable if you set **Search Type** to **All**.

After you select a user with violations, you can use the following tabs on the right-hand panel to view related information:

Risk Info
Displays risk information details for each domain.

Assignment details
The **Domain** accordion pane lists the domains associated with the user.

The **Activity search** accordion pane lists the activities associated with the user. Click **Actions** > **View** to find the position of the activity in the OU tree view.

In either accordion pane, you can use the following filters to search information (after clicking **Filter**):

Table 299. Filters helpful for searching a domain or an activity for conflicting users.

Filter	Description
Name	Name of the domain/activity
Description	Description of the domain/activity

SAP Roles
Shows all the SAP roles and authorizations associated in hierarchy with:

- SAP Roles (SoD process)
- User directly (Full SoD process)

SAP Authorizations
Lists all the SAP Authorizations associated with the user in a flat mode.

SAP Role Violations

This section enables you to view and analyze conflicting SAP roles.

A conflicting SAP role allows users to run conflicting activities.

The **Roles** tab displays a list of SAP roles. You can use the following filters to find a specific SAP role (after clicking **Filter**):

Table 300. Filters you can use to find SAP roles.

Filter	Description
Role Type	One of the following types of entitlement: - SAP Role - Collective Role
Name	The role name

Table 300. Filters you can use to find SAP roles. (continued)

Filter	Description
Search type	Can be: **All** The search is made on all roles **Conflicting** The search is made on conflicting roles only
Conflict level	Can be: • Low • Medium • High This filter becomes unavailable if you set **Search type** to **All**.

You ca use the **Actions** button to:

- Refresh a selected role
- Download a new role
- Download a selected role
- Remove a selected role

After you select a SAP role, you can use the following tabs on the right-hand panel to view related information:

SAP Role details
Shows the following details of the selected role:

- Name
- Description
- Role type
- Created by
- Creation date
- Modified by
- Last modification date and time

Warning
Lists any warnings released for the selected role. You can use a search filter to find specific warnings, based on the warning code or severity.

Conflict Info
Provides a tree view of conflict information details for all domains.

Activity
Displays a list of the activities associated with selected role. Click **Actions** > **View** to find the exact position of the activity in the OU tree structure.

Transaction
Lists the transactions related to the selected SAP role. You can use a search filter to find specific transactions, based on the transaction group, name, and description.

Authorization Object

Lists the authorization objects related to the selected SAP role. You can use a search filter to find specific authorization objects, based on any of their attributes.

SAP Authorization

Lists the SAP authorizations related to the selected SAP role. You can use a search filter to find a specific SAP authorization objects, based on its name and on whether there is or not a segregation of duties.

SAP authorization violations

This section enables you to view and analyze conflicting SAP authorizations.

A conflicting SAP authorization allows for the execution of conflicting activities.

The **SAP Authorizations** tab displays a list of SAP authorization names, their conflict level, and their application (their set of permissions). You can use the following filters to find specific authorizations (after clicking **Filter**):

Table 301. Filters you an use to find SAP authorizations.

Filter	Description
Name	The SAP authorization name
Search type	Can be: **All** The search is made on all SAP authorizations **Conflicting** The search is made on conflicting SAP authorizations only
Conflict level	Can be: • Low • Medium • High This filter becomes unavailable if you set **Search type** to **All**.

After you select a SAP authorization, you can use the following tabs on the right-hand panel to view related information:

SAP Authorization details

Shows the following details of the selected role:

- Name
- Description
- Created by
- Creation date
- Modified by
- Last modification date and time

Conflict Info

Provides a tree view of conflict information details for all domains.

Activity
Displays a list of the activities associated with the selected authorization. Click **Actions** > **View** to find the exact position of the activity in the OU tree structure.

Role warnings

This section enables you to view and analyze role-related warnings.

The **Warnings View** tab displays a list of roles on which warnings were raised, the role description, the warning code, the severity of the warning, and a description of it. You can use the following filters to find specific warnings (after clicking **Filter**):

Table 302. Filters you an use to find role warnings.

Filter	Description
Role Name	The name of the role on which the warning was raised
Severity	The level of severity of the warning. It can be: • Low • Medium • High
Code	The code that identifies the warning.

After you select a role, you can click the **Actions** menu and select:

Statistics
To view a graphical display of the number of occurrences of the warning code.

Details
To view the details of the role.

Report

You can request and download reports.

The main functions in this section allow you to:

- Request (configuration of the assigned reports)
- Download

You can start the following reports for a SAP System:

SAP and Collective Role Risks
List of SoD Risks for SAP and Collective roles

SAP Authorizations Risks
List of SoD Risks for SAP Authorizations

User Risks
List of FSoD-SoD Risks for Users

User with FSoD Risks
List of FSoD Risks for Users

SAP Authorization Definition
List of SAP Authorizations

SAP Authorization and Business Activity Catalog
List of SAP Authorizations linked to Business Activities

SAP Role Catalog
List of SAP Roles

SAP Role and AuthObj Catalog
List of AuthObj for each SAP Role

SAP Role and Business Activity Catalo
List of SAP Roles linked to Business Activities

SAP Role and Transaction Catalog
List of Transactions for each SAP Role

You can download the reports in PDF or XLSX format.

Tools

Several functions speed up and facilitate the tasks of the following modules:

- Data Refresh
- Bulk Data Load
- Configuration Set Comparison

Data refresh

You can view a list of the currently scheduled Operations and the scheduled operations history.

The main functions in the section allow you to:

- Start one of the scheduled jobs listed in the **Scheduled Operations** tab
- Monitor or remove the status listing of a scheduled job in the **Scheduled History** tab

In the **Scheduled Operations** tab, you find a list of the following scheduled jobs:

- Load Data from SAP
- SAP Role Analysis
- User Analysis
- Collective Role Analysis
- Warning Analysis
- SoD Analysis

After any update related to SAP/Collective Roles or Users, the first operation that you have always to run is the SoD Analysis.

After the SoD Analysis, you can choose the operation that you need.

A best practice is to run this sequence:

1. SoD Analysis
2. SAP Role Analysis (if you need)
3. Collective Role Analysis (if you need)
4. User Analysis (if you need)

Click **Actions** > **Start** to start the job immediately if it is not in the `Waiting` or `Executing` state.

In the **Scheduled History** tab, you find a list of the scheduled job instances. When you select a job that analyses roles or users, the list of related roles is displayed below. Click **Actions** > **Remove** to remove a selected job status from the list.

Bulk Data Load

You can run several types of bulk data-loading in the AG Core database.

The **Actions** tab (left) shows the supported operations.

After you select an operation in **File Batch**, select one of the following options:

- **Download** to get a template (XLS file), related to the currently selected operation.
- **Browse** to search in the file system for an XLS file for the selected loading operation.

When the operation is completed, an information record is appended in the lower-right pane to the list of the previously completed operations.

In the same pane, you can select:

- **Input File** to get the file used in the operation.
- **Log File** to get the operation report.
- Add Risk Entitlement to Activity
- Insert Risk Entitlement
- Remove Risk Entitlement
- Remove Risk Entitlement from Activity

A generic record track distinguishes between **Mandatory** and **Optional** fields.

If a mandatory field is empty or populated with unexpected values, the row is skipped unless specified otherwise in the documentation.

According to the data load behavior, populating an Optional field with unexpected/wrong values could cause a row to be skipped.

For information about the procedure, see “Creating a bulk load operation” on page 89.

Add Risk Entitlement to Activity Record Track

This batch procedure can be used to aggregate Risk Entitlement to an Activity. It verifies that **Mandatory** fields are populated.

The XLS source file is organized into **2 sheets**.

Table 303. Add Risk Entitlement to Activity Track (sheet 1).

Information	Description	Validation
SAP_SYSTEM	SAP application name	Mandatory
RISK_ENTITLEMENT	Risk Entitlement name	Mandatory
TRANSACTION	Transaction name.	Mandatory

Table 303. Add Risk Entitlement to Activity Track (sheet 1). (continued)

Information	Description	Validation
ACTIVITY_REF	Reference to Activity on sheet 2 of the file XLS.	Mandatory

Table 304. Add Risk Entitlement to Activity Track (sheet 2).

Information	Description	Validation
ACTIVITY_REF	Reference to Activity.	Mandatory
CODE	Activity code.	Mandatory
ACTIVITY	Activity name.	Mandatory
ENVIRONMENT	Environment name.	Optional

The SAP_SYSTEM field contains the name of the SAP application, already registered in the system. If there is no such SAP application, the row is skipped.

The RISK_ENTITLEMENT field contains the name of a Risk Entitlement, already registered in the system. If not, the row is skipped.

The ACTIVITY_REF column on sheet 1 refers to the same column on sheet 2.

Values possibly contained in this column on sheet 1 must also be present in the same column on sheet 2. Conversely, the ACTIVITY_REF column on sheet 2 can contain values that are not present or referenced in sheet 1.

The ENVIRONMENT field is optional. If this field is populated, existence of an environment with the specified name is verified. Otherwise the row is skipped. If left blank, the default Environment is used.

Insert Risk Entitlement Record Track

This batch procedure can be used to insert Risk Entitlement (with the joined Transaction) in the system.

Table 305. Insert Risk Entitlement Track.

Information	Description	Validation
SAP_SYSTEM	SAP application name	Mandatory
RISK_ENTITLEMENT	Risk Entitlement name	Mandatory
RISK_ENTITLEMENT_DESCRIPTION	A brief description about Risk Entitlement.	Optional
TRANSACTION	Transaction name (into SAP Authorization Model, Transaction is a specific type of Authorization Object).	Mandatory
TRANSACTION_DESCRIPTION	A brief description about Transaction.	Optional

Table 305. Insert Risk Entitlement Track. (continued)

Information	Description	Validation
AUTH_OBJ	Authorization Object (AO) name linked to the Transaction. AO can be characterized: • by a condition (AO_CONDITION) • by several fields (AO_FIELD) • for every field a condition (AO_FIELD_CONDITION) might be specified.	Optional
AO_CONDITION	Two values are allowed (with other values, the row is skipped): AND/OR.	Mandatory ONLY if AUTH_OBJ field is not empty
AO_FIELD	AO field name	Optional
AO_FIELD_CONDITION	Four values are allowed (with other values, the row is skipped): • ANY_FROM • NONE_FROM • ANY_BUT • ALL_INTO	Mandatory ONLY if AO_FIELD field is not empty
AO_FIELD_VALUE	The value related to AO_FIELD	Mandatory ONLY if AO_FIELD field is not empty

It verifies that **Mandatory** fields are populated.

It provides the insertion of the new Risk Entitlement with its Transaction and the Authorization Objects possibly involved in the Transaction.

The `SAP_SYSTEM` field contains the name of the SAP application, already registered in the system. If there is no such SAP application, the row is skipped.

The `RISK_ENTITLEMENT` field contains the name of a Risk Entitlement, already registered in the system. If not, the row is skipped.

The `TRANSACTION` field contains the name of a Transaction, already registered in the system. If not, the row is skipped.

If the Transaction indicated is not registered in the system, it is added.

If the `AUTH_OBJ` is indicated and is not registered in the system, it is added.

If `AUTH_OBJ` is present, `AO_CONDITION` become a mandatory field.

Remove Risk Entitlement Record Track

This batch procedure can be used to remove Risk Entitlements. In absence of any mandatory information, the row is skipped.

Table 306. Remove Risk Entitlement Track.

Information	Description	Validation
SAP_SYSTEM	SAP application name	Mandatory
NAME	Risk Entitlement name	Mandatory
DESCRIPTION	A brief description about Risk Entitlement.	Optional

Remove Risk Entitlement from Activity Record Track

This batch procedure can be used to remove Risk Entitlement from an Activity.

The structure of the record track is as outlined in Add Risk Entitlement to Activity.

Configuration Set Comparison

In this section, you can compare two different configurations, and check whether or not the changes made in a specific configuration alter the model compared to the operating configuration.

The **Compare Configuration** tab displays all the configurations listed by the system. To compare another configuration with the operating configuration (which is already selected), select that configuration in the **Compare Configuration** pane.

You can run the following operations related to mitigation controls:
- "Configurations"
- "Comparison Dashboard"
- "Comparison Details" on page 575

Configurations

Select an additional configuration in the **Compare Configuration** pane and click the **Configurations** tab on the right to view information about the User and the Entitlement analyses of the configurations:

- The ✓ icon shows that the analysis completed successfully.
- The ✗ icon shows that the analysis failed.

The bordered green configuration is the operating configuration information.

Comparison Dashboard

Select an additional configuration in the **Compare Configuration** pane and click the **Comparison Dashboard** tab on the right: Four dashboards for the two configurations are displayed:
- **Conflicting Collective Roles**
- **Conflicting SAP Roles**
- **Conflicting SAP Authorizations**
- **Conflicting Users**

These dashboards show the structure of the compared configurations.

Comparison Details

Select an additional configuration in the **Compare Configuration** pane and click the **Comparison Details** tab on the right: With this operation you can compare detailed reports of paired configurations.

In this situation, additional information is provided about changes in the number and types of conflicts on a single ARCS model entity present in both configurations. The **Comparison Details** tab enables you to access the following two tabs:

- **Users**
- **Entitlements**

In the **Users** tab, you can define filters to list sets of conflicting users registered on the system. You can use the following attributes:

Table 307. Filters available to search for conflicting users in a configuration set comparison.

Filter	Description	
Organization Unit	OU to which the user belongs	
Hierarchy	Select this check box to set the operation to start executing from the root of the selected OU and down through the hierarchy originating from that root	
Search Identity	Enter the user's name and surname, or the User ID	
DN	The user's Distinguished Name.	
Conflicting state	**All**	All possible conflicting states
	Unaltered	The user remains with the same number of risks in both configurations
	Altered	Every user with a modified number of risks (**Enhanced**, **Worsened**)
	Enhanced	In the operating configuration the user has a lower number of risks than the compared configuration
	Worsened	In the operating configuration the user has a higher number of risks than the compared configuration

The risk level distribution provides a view of the qualitative mix of risk levels among the total number of risks. For example: a user has 11 total risks. Of these, 4 have a low risk level and 7 have a high risk level. Therefore, the user is characterized by the low/high qualitative mix of risk levels.

In the **Entitlement** tab, you can define filters to list sets of conflicting entitlements registered on the system. You can use the following attributes:

Table 308. Filters available to search for conflicting entitlements in a configuration set comparison.

Filter	Description	
Type	Choose one of the following types of entitlement: • SAP Authorization • SAP Role • Collective Role	
Application	The name of the application on which the conflicting entitlements are filtered	
Name	Name of the entitlement	
Conflicting state	**All**	All possible conflicting states
	Unaltered	The entitlement remains in a conflicting state with the same mix of conflict level values (High, Medium, Low) in both configurations
	Altered	Every user with a modified number of risks (**Enhanced**, **Worsened**)
	Enhanced	In the operating configuration the entitlement has a lower number of risks than the compared configuration
	Worsened	In the operating configuration the entitlement has a higher number of risks than the compared configuration

The concept of risk level distribution, described in the **Users** tab, applies also here.

Chapter 27. Introduction to Report Designer

Report Designer (RD) module provides a modeler capable of outlining every type of report.

Using this module, the administrator can visually describe the report creation process from beginning to end.

Using the Access Governance Core authorization system, authorized users can access and run a set of reports from within each IBM Security Identity Governance and Intelligence module.

In case of unauthorized users, the **Report** tab, if present, is not active.

The Report Designer module is used to:

- Create queries and scopes.
- Assign one or more scopes to a query.
- Define a new report and associating a query to it.
- Aggregate the same query to one or more reports.
- Define the report-entitlement assignment (the report is available to the user that holds the entitlement).
- Localize the report.
- Assign a report status.

Report modeling for the Identity Governance and Intelligence platform

Report Designer (RD) is the Identity Governance and Intelligence module dedicated to the design and definition of reports.

This module is used to:

- Create queries and scopes.
- Assign one or more scopes to a query.
- Define a new report, adding a query to it.
- Add the same query to one or more reports.
- Define the report-entitlement assignment (the report will be available if you have the entitlement).
- Localize the report.
- Assign a report status.

This section outlines the main concepts about creating a report with the RD module.

Note: An administrator experienced in the SQL language must manage this section.

Create a query

In the RD, the administrator can create free handwritten SQL queries in a dedicated text area. Click the **Query management** tab, and specify the following information about the query in the **Query details** section:

Name Name of the query. The following text is an example: `Remediations to risks Batch QUERY`

Description
Description of the query. The following text is an example: `Batch query to assign remediation to risks`

SQL query
Query text. The following text is an example:

```
select distinct rem.name   as BATCH_REMEDIATION,
            rem.code   as BATCH_CODE,
            rem.description as BATCH_DESCRIPTION,
            rem.desc1  as BATCH_EXT_DESCR,
            r.name     as BATCH_RISK_NAME,
            e.name     as BATCH_ENVIRONMENT
from #PMSCHEMA#.environment  e,
   #PMSCHEMA#.risk
   #PMSCHEMA#.risk_remediation rr,
   #PMSCHEMA#.remediation  rem
where e.id = r.environment
and r.id = rr.risk
and rr.remediation = rem.id
and lower(e.name) = lower ('#env_name#')
```

Additional support is also provided for writing more efficient and flexible queries, based on three main concepts:

- "Schema" on page 579
- Scopes
- Filters

The following figure shows the text area used to specify a query:

The next table summarizes the set of product queries available in the RD module:

Table 309. Product queries

Query name	Query description
Access Certification Campaign Status	Access certification completion status
Access Certification Status query	User certification completion details by OU
Access Rights not assigned to any user query	Entitlement published but not assigned
Access Rights not assigned to any OU query	Entitlement not assigned to any OUs
Access Rights Visibility by OUs query	Role visible to users because of belonging OU
Account Status query	User ID and account status on common target pool
Activities hierarchy Batch query	Batch insert activities hierarchy
Applications Batch query	Batch query to find application
Application Entitlements dictionary query	Entitlement by application
Delegation assignments details query	User assigned roles by delegation

Table 309. Product queries (continued)

Query name	Query description
Entitlements Batch query	Batch query to find entitlements
Entitlements to Users Batch query	Not applicable
Events-IN from HR system query	User Event-IN
Events-OUT to Targets query	User Event-OUT
IBM Security Identity Governance Audit query	Not applicable
IBM Security Identity Governance Report Structure query	Report columns, sequence and localization information
IBM Security Identity Governance Report Visibility query	Reports assignment on entitlements
Mitigations assigned to Risk query	Batch remediation to risks
Organizational Units Batch query	Not applicable
OU visibility: campaign status query	Roles visibility certification completion status by OU
Profile to domain Batch query	Batch query to add profile to domain
Profile to Activity Batch sheet 1 query	Batch add profile to activity sheet 1- Role realm
Profile to Activity Batch sheet 2 query	Batch add profile to activity sheet 2- Role realm
Remediation to Risks Batch query	Batch query to assign remediation to risks
Resources Batch query	Not applicable
Role hierarchical structure query	Role tree structure
Risk Structure query	Risk definitions
Risk Structure Batch query	Batch risk definition
Role Risk Overview query	Operates on the role realm
Role Structure Changes query	Query to detect role changes in applications
Technical error event log from last targets import query	Query to detect target application import events
Technical mapping query	Entitlement mapping on business activity
User Assignments query	User with assigned roles
User Assignments Changes query	Query to detect the user access entitlement assignments changes
Users Batch query	Not applicable
Users by Application query	User list with scope on OU and application
User Risks and Assigned Mitigations query	Not applicable
User Risk Count query	Not applicable

Schema

A schema is a set of tables related to a specific subsystem of a generic database. A set of schemas characterizes Identity Governance and Intelligence and the entire list of available schemas is determined at installation time. Every schema is associated to a database administrator name that is specified during the installation process.

In the **System Entities** tab, the RD administrator can register all the schemas used for building queries and reports.

Every schema is inventoried using a name-value pair. Generally, the name is built using a generic string of characters that clearly identifies the database subset. The value must match the database administrator name. When defining a query in the report designer module, specify at least one schema.

The next table describes two different ways of specifying a schema:

Table 310. Schema specification

Procedure 1	Procedure 2
from #PMSCHEMA#.application a, #PMSCHEMA#.entitlement e1, #PMSCHEMA#.entitlement e2, #PMSCHEMA#.task_profile tp, #PMSCHEMA#.task tk, #SCHEMA#.environment env	from REALM_DEMO.application a, REALM_DEMO.entitlement e1, REALM_DEMO.entitlement e2, REALM_DEMO.task_profile tp, REALM_DEMO.task tk, Report.environment env

In **Procedure 1**, the system keys #**PMSCHEMA**# and #**SCHEMA**# enable the administrator to have a multi-schema query without having to actually specify the name of the schema in the query.

This is very useful for managing the database schema of different organizations.

Suppose the following:

```
PMSCHEMA = Org_01
SCHEMA = Org_01_ENV
```

where `Org_01` and `Org_01_ENV` are two schemas for `Organization01`.

But what if `Organization02` requires the same query?

This requires changing the settings in the System Entities tab, as follows:

```
PMSCHEMA = Org_02
SCHEMA = Org_02_ENV
```

Therefore, the Report Designer administrator only writes the query once and can use it for different organizations.

The Identity Governance and Intelligence data model uses the realm concept to represent a generic organization.

Identity Governance and Intelligence allows for multi-realm management whereby the administrator can create individual models to manage several organizations while keeping the different realm-related contexts separate. A realm is essentially a model that describes an organization in terms of a set of objects and the relationships between them. A realm is implemented using a database.

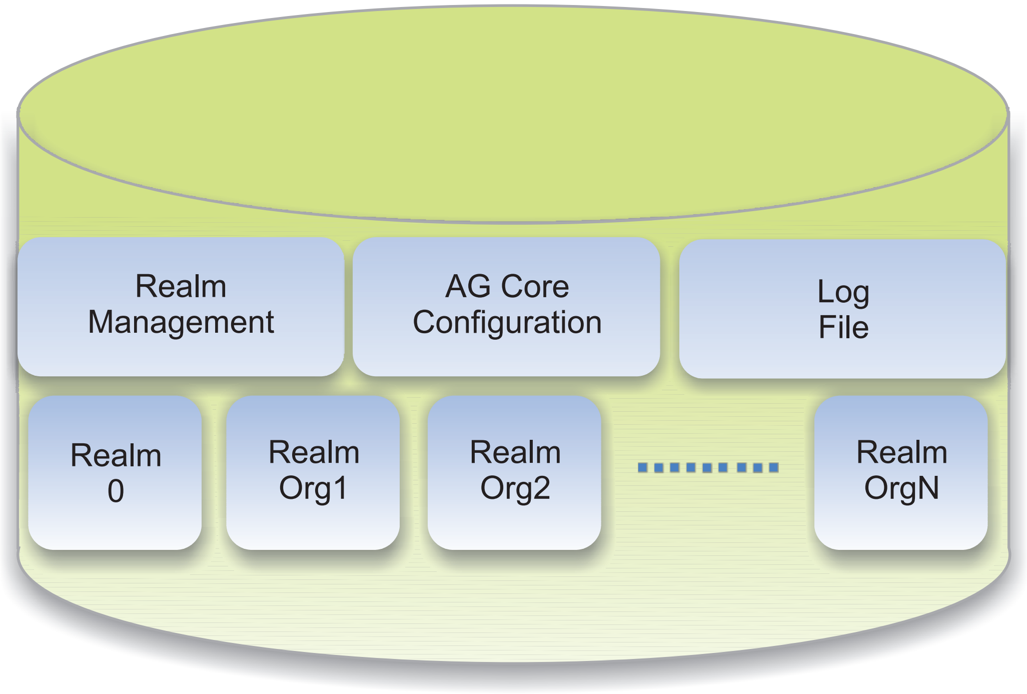


Figure 119. Realms.

In the Identity Governance and Intelligence data model, the schema value, defined in the **System Entities** tab, usually matches a realm name.

Procedure 1 could be a management model called "Multi Schema/Multi Realm Parametric Queries".

The general structure of this procedure is:

```
#Name of Schema#.Name of Table
```

In **Procedure 2** the **REALM_DEMO** and **Report** keys are the names of two different schemas that match two different realms. The **Procedure 2** query only works for these two schemas.

The general structure of this procedure is:

```
Name of Schema.Name of Table
from swim.request r,
swim.applications app,
swim.roles ro,
report.tmp_application tmpa
```

Scope

When writing a query, the administrator can define one or more temporary tables (tmp.) to which the administrator can add one or more scopes.

The scope is a selective breakdown of database data. The scope functions as a filter and a collector between the temporary tables and the database entities (OUs, Applications, Entitlements, Users).

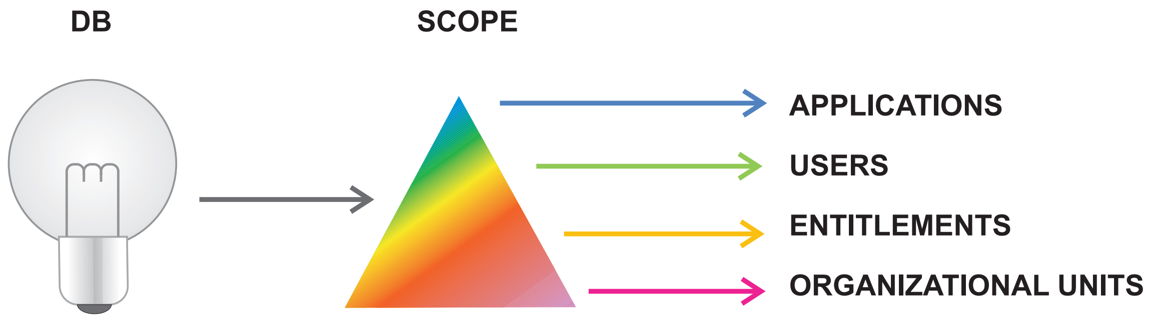


Figure 120. Scopes.

For example, a user needs a query to select data for all transactions <$100.000 made in the month of March in a national real estate franchise.

When dealing with such a large volume of data, how is it possible to isolate the owners of the corresponding agencies? This requires a user scope that can extract all the data-of-interest related to a given user.

What if a user needs to classify local transaction density? In this case, how can the user associate transactions to the territories where they took place? Invoking the Organization Unit scope, it will extract all OU-related data.

Additionally, different users (who have different roles and access rights for data within the Identity Governance and Intelligence database) can call the same report. If two different users, who have the same role but different visibility rights to an organization data set, execute the same report (but with different specialized visibility tags), they will both get different results.

The administrator in charge of designing reports can use the scope concept in situations that require a parametric configuration, relating to the visibility of a particular entity of the Identity Governance and Intelligence data model, based on the rights of the users executing the report.

The Report Designer module offers the following product scopes:

Table 311. Product scopes

Scope name	Scope description	Entity name
AG-Core Entitlement	Entitlement scope	Entitlement
AG-Core Org. Unit-Hierarchy	Organization unit scope- including hierarchy	Org_unit
AG-Core Application	Application scope	Application
AG-Core User	User scope	User
AG-Core Org. Unit	OU certification status	Org_unit
AG-Core Business Activity	Business activity scope	Task
AG-Core Account	Account configuration scope	PwdCfg
AG-Core Working Environment	Procedure that works only on production environment.	System
AG-Core Role Structure Procedure	Allows the visibility of roles hierarchical structure	System
AC Org. Unit Scope	Organization unit scope	System

Table 311. Product scopes (continued)

Scope name	Scope description	Entity name
AC User	User roles certification status	System
AC OUUser Procedure	Users (of specific OUS) certification status	System
ARC Role Procedure	Procedure to calculate risks on roles	System
ARC User Procedure	Procedure to calculate risks per users	System

In the highlighted portion of the query below, **#PMSCHEMA#** refers to the main Identity Governance and Intelligence database tables and **#SCHEMA#** refers to the Report Designer database. In the example below, an application entity of the Identity Governance and Intelligence model serves to manage the concept of application visibility.

The Report Designer administrator needs to link a temporary table to the application scope:

```
select distinct e.name as ROLE_NAME,

e.description as ROLE_DESC,

a.name as APPLICATION_NAME,

a.description as APPLICATION_DESC

from #PMSCHEMA#.entitlement  e,

#PMSCHEMA#.application    a,

#SCHEMA#.tmp_application    tmp

where a.id = tmp.id

and eap.entitlement = e.id

and eap.application = a.id

.........
```

After writing the query and defining the relationship between the database and the temporary tables, the next logic step is to associate the scope to the query in the Scope management tab.

The administrator might also write a query and define the temporary tables without associating a scope. In this case, the temporary tables do not contain any data and the scope is not visible in the report wizard.

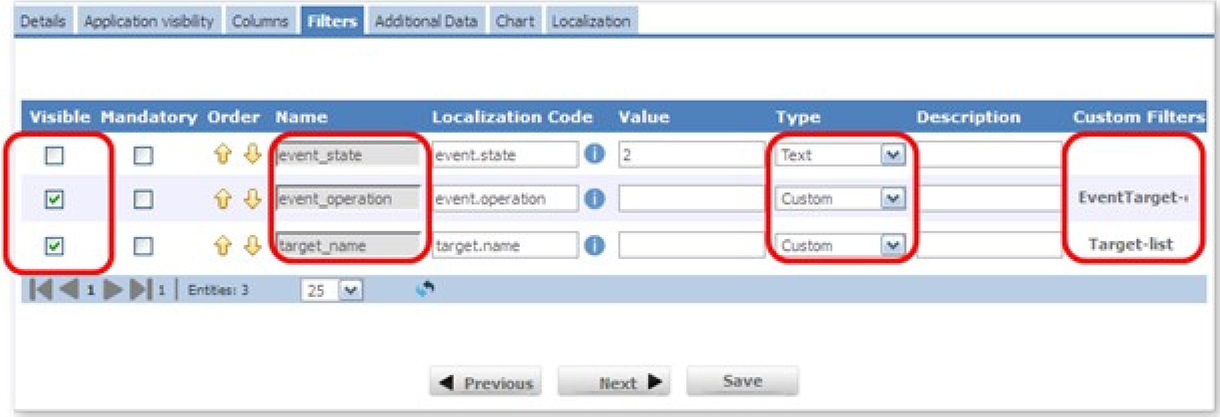
The administrator can configure a joined scope (which is, consequently, visible in the Report Wizard) in the Report tab. It must be taken into account that the scopes, present in the module, are product scopes, and have their entity visibility configured by default, but is possible to configure their Entity Visibility according to your needs.

Filters and custom filters

As the following sample code shows, the `where` condition of a generic query can specify one or more filters in order to produce well-tailored data:

```
select...

...where

    t.state = '#event_state#'

    and t.operation = '#event_operation#'

    and t.target = '#target_name#'

    and t.process_id = ...
```

In the wizard, the **Filters** tab shows the set of filters specified in the `where` condition. As the figure below shows, the user might associate a label to an **X value** to create a custom filter:



Visible	Mandatory	Order	Name	Localization Code	Value	Type	Description	Custom Filters
□	□	⇧ ⇩	event_state	event.state	2	Text		
☑	□	⇧ ⇩	event_operation	event.operation		Custom		EventTarget-‹
☑	□	⇧ ⇩	target_name	target.name		Custom		Target-list

Figure 121. Filters tab in Filter configuration.

For example, in the third row of the figure above, the aggregated label **Target-list** customizes the `target_name` data model element. In the final report, the data related to `target_name` will display under the `Target_list` heading and will be more meaningful for the user requesting the report.

This feature is particularly useful when the original name of the data model element is not very easy to understand.

For example, if the data model element is a numeric value that indicates a specific system (for example, "1" = "Create User", "2"= "Modify User", "3"= "Remove User"), it is easier to associate a meaningful label that, in the report, represents the literal status value:

```
"1": User is present
"2": User has been amended
"3": User is not present
```

In the wizard, you can configure the filters using the Filters tab.

Report classification: product reports and new reports

The RD module provides a large set of product reports.

Product reports are marked with the product icon.

The RD Administrator can assign these reports as they are, or modify their settings as needed. The list of product reports is continuously updated as the RD module evolves.

Note:

Modification of any product report is strictly forbidden.

Be careful with the batch-type reports. Their behavior is closely linked to the AG Core database. Any change might affect the report execution.

The RD Administrator can also create customized reports.

Report configuration is extremely flexible; a dedicated set of tabs (such as Details or Localization) offers several options to determine which set of data the report will display.

The Report wizard: how to design a report

Designing a report is very easy. A specific wizard organizes all the required steps. The following figure shows the conceptual scheme of the wizard:

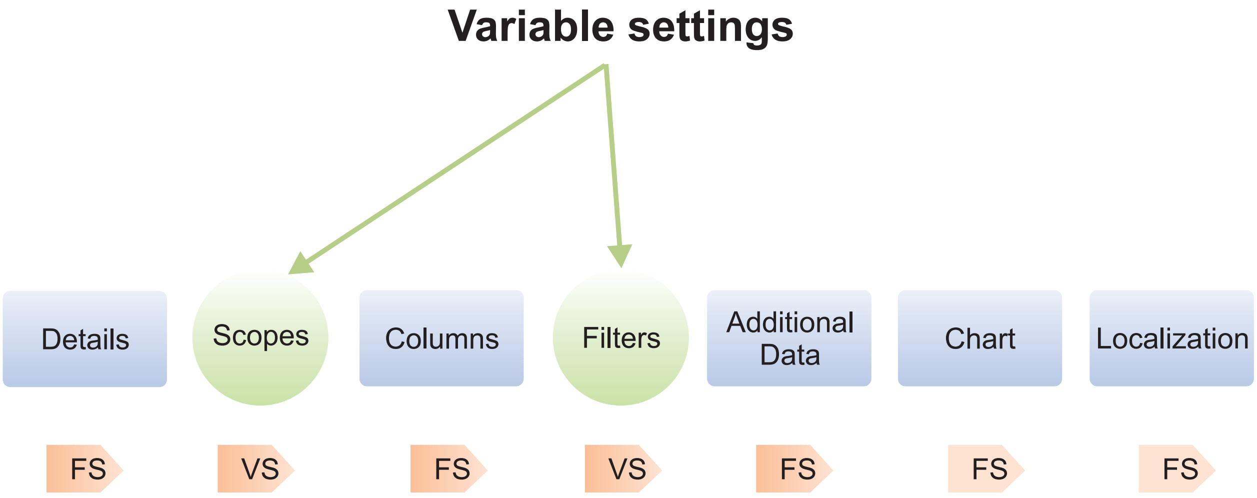


Figure 122. Wizard Steps.

The wizard is composed by five fixed settings and two variable settings.

The **Fixed Settings (FS)** tabs are available and visible in all report configurations, while the **Variable Settings (VS)** tabs are associated only to specific reports:

- Details
- Scopes
- Columns

- Filters
- Additional Data
- Chart
- Localization Tab

Using the wizard specific tabs, the RD Administrator can configure the scopes and filters present in a query.

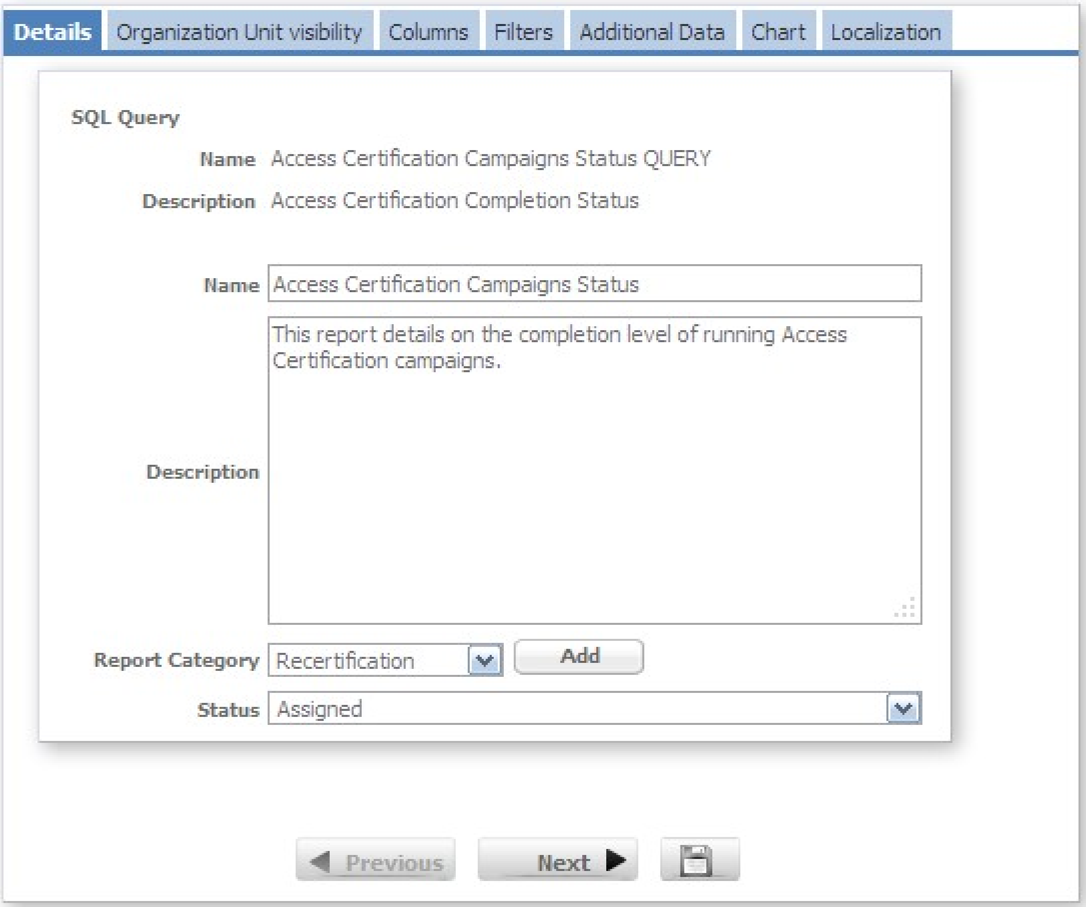
The RD Administrator can also write a simple query without defining any additional settings; in that case the report configuration will not display such settings.

Below are shown all steps of a generic report wizard, along with all characteristics of the main configuration frame.

Details tab

The **Details** tab is present in all report configuration wizards and consists of:
- A box with the associated query information.
- A text area for selecting a report name, writing a brief report description.
- An **Add** button for adding report category.
- A text area for selecting an inventoried report category.
- A text area for configuring the report status (New, Assigned, Locked).

The following figure describes the layout of the **Details** tab:



SQL Query

Name: Access Certification Campaigns Status QUERY

Description: Access Certification Completion Status

Name: Access Certification Campaigns Status

Description: This report details on the completion level of running Access Certification campaigns.

Report Category: Recertification

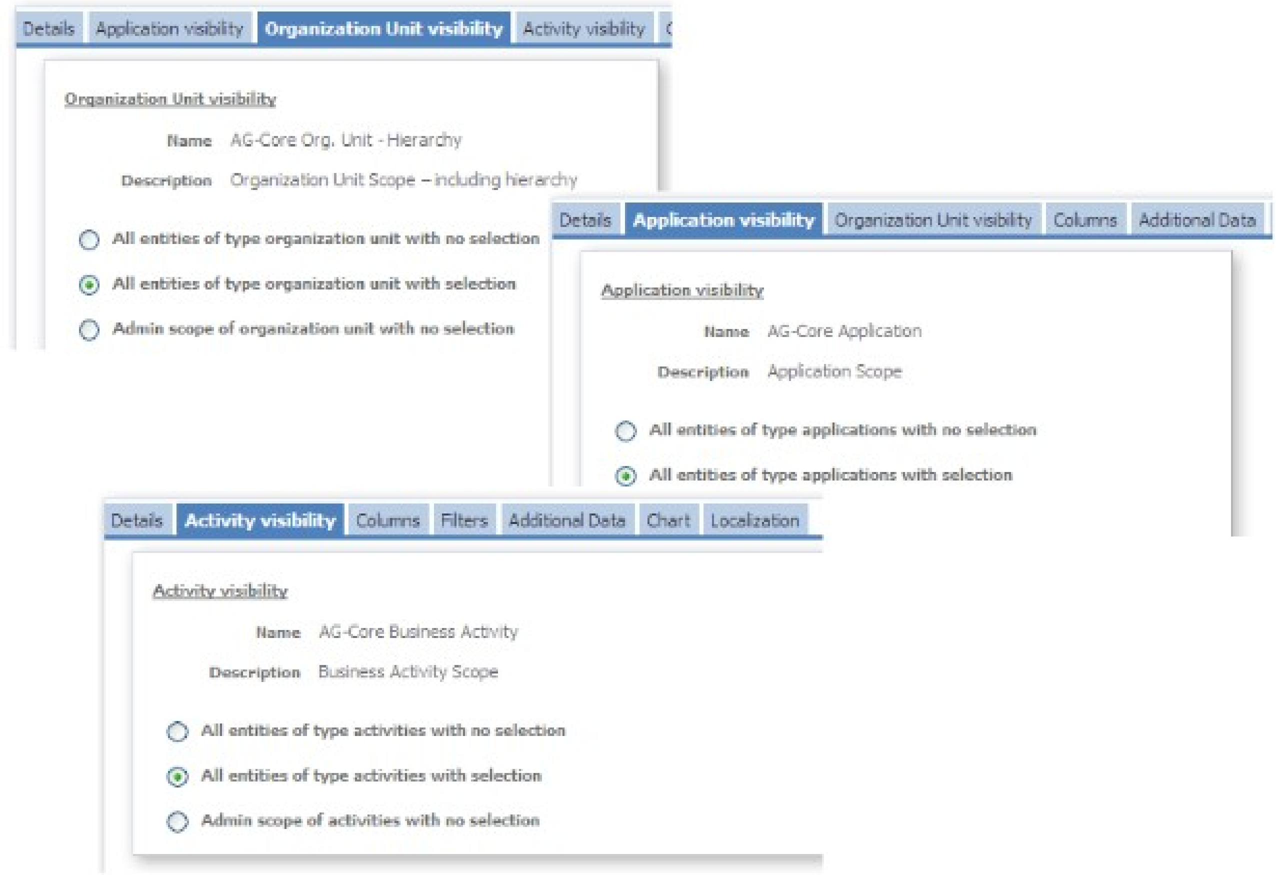
Status: Assigned

Figure 123. The Details tab of the Report Configuration wizard.

Scope configuration: Visibility tabs

After the **Details** tab, the wizard displays a subset of tabs based on the number of scopes that are linked to the report aggregated query.

The following figure shows some possible scope subset tabs:



Organization Unit visibility

Name AG-Core Org. Unit - Hierarchy

Description Organization Unit Scope – including hierarchy

○ All entities of type organization unit with no selection

● All entities of type organization unit with selection

○ Admin scope of organization unit with no selection

Application visibility

Name AG-Core Application

Description Application Scope

○ All entities of type applications with no selection

● All entities of type applications with selection

Activity visibility

Name AG-Core Business Activity

Description Business Activity Scope

○ All entities of type activities with no selection

● All entities of type activities with selection

○ Admin scope of activities with no selection

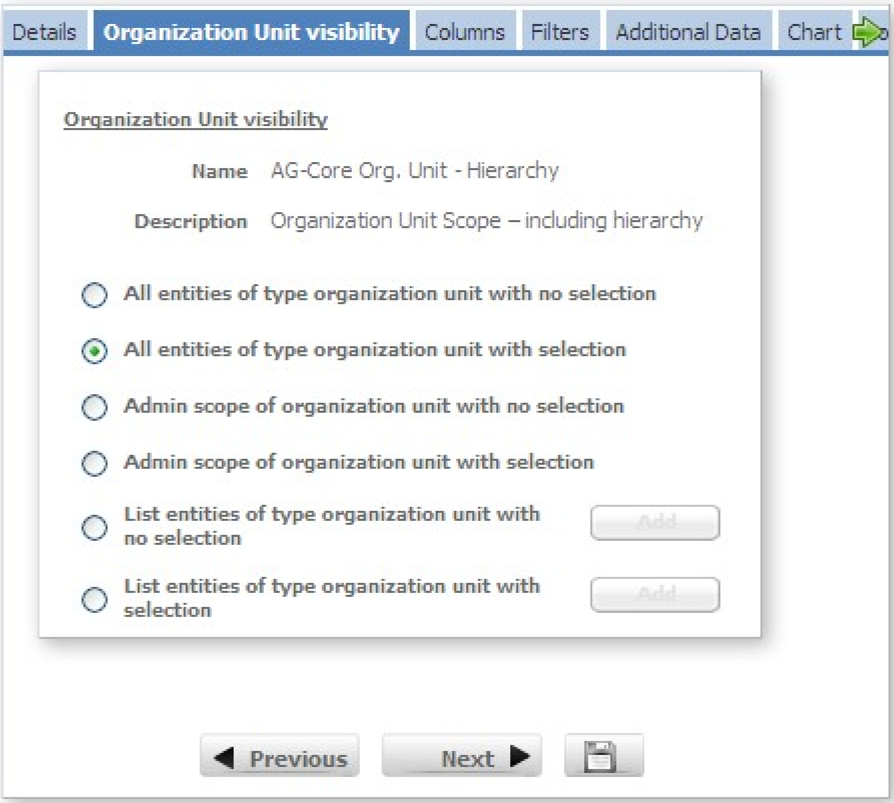
Figure 124. Scope subsets: some combinations.

The model has a **Scope** tab for any available, distinct *Scope Entity*. The following table shows the complete list of entities:

Table 312. Available entities.

Scope	Description
Activity	This entity is related to the business activity concept of the IBM Security Identity Governance data model.
Application	This entity is related to the application concept of the IBM Security Identity Governance data model.
Entitlement	This entity is related to the entitlement concept of the IBM Security Identity Governance data model.
Organization unit	This entity is related to the organization unit concept of the IBM Security Identity Governance data model.
Password configuration	This entity is related to the environment configuration defined in the Access Governance core module.
User	This entity is related to the user concept of the IBM Security Identity Governance data model.

To set the entity visibility for each *Scope Entity*, the RD administrator can click the related radio-button from a fixed list, as the next figure shows:



Organization Unit visibility

Name AG-Core Org. Unit - Hierarchy

Description Organization Unit Scope – including hierarchy

○ All entities of type organization unit with no selection

● All entities of type organization unit with selection

○ Admin scope of organization unit with no selection

○ Admin scope of organization unit with selection

○ List entities of type organization unit with no selection

○ List entities of type organization unit with selection

Figure 125. Entity visibility configuration.

The following table shows the visibility options for all available *Scope Entities*:

Table 313. Visibility options for each entity.

Visibility	Description
All entities of type entity with no selection	The authorized user can view all entities but cannot select any of them.
All entities of type entity with selection	The authorized user can select the desired entities.
Admin scope of entity with no selection	Authorized users cannot select from entities within their visibility (Applications, Entitlements, Organization Unit, and so on).
Admin scope of entity with selection	Authorized users can select from entities within their visibility (Applications, Entitlements, Organization Unit, and so on).
List entities of type entities with no selection	The authorized user cannot select any entity from the limited list (defined by the administrator).
List entities of type entities with selection	The authorized user can select any entity from the limited list (defined by the administrator).

Columns tab

From this tab, the RD administrator can choose which columns to display in the report.

The following table shows eight parameters that characterize each item:

Table 314. Report columns configuration.

Column	Description
Visible	If this check box is selected, the report will show the column.
Order	With the up arrow/down arrow is possible to choose the column position.
Name	Column name
Localization Code	The localization code is defined in this field.
Type	The data type is set in this field.
Column Width	The column width is defined in this field.
Order By	Column sorting order

The RD Administrator can click the ⓘ **Localization Help** button, near the Localization Code text area, to verify that a localization code exists and is correct. From the Localization Help window, the RD Administrator can only search for the localization code and its aggregated localized messages but cannot perform any operation.

The RD Module displays these codes according to the chosen default language.

The Localization Help window opens and, if the localization code is registered, the **Localization Code** and **Code Type** fields are automatically populated with the specified value. If the localization code is not registered, the search operation does not show any results. In this case, see Edit Labels.

To order the columns in ascending or descending order, click AZ **Order By**.

The **Column to order** pane (right) lists columns available for insertion in the frame, **Column to use for order condition** (left). Select the column to order and click the **Add** button ◀. The Order condition window opens. Click the Ascending or Descending radio buttons to choose the sorting order.

The Column to use for order condition frame on the left is now automatically populated with the selected column.

Click **Ok**. The columns are now displayed with the AZ↓ **Order by** icon.

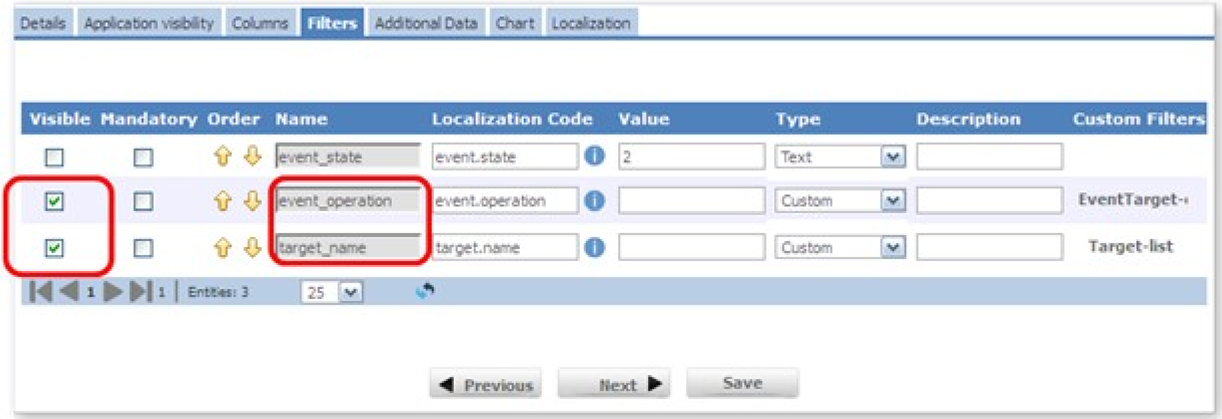
The **Order By** heading indicates the sorting order of the columns in a given report.

If the ZA↓ icon (**Descending order**) is present, the number in parenthesis next to the icon indicates the column element that is listed as first. If the ↓ icon (**Ascending order**) is present, the number in parenthesis next to the icon indicates the column element that is listed as last.

Note: The module save any changes made in this window, allowing the administrator to verify the label localization.

Filters tab

After writing the query, the RD administrator can set and customize the **Filters**. To display the filters, select the related check box in the **Visible** column, as the following figure shows:



Visible	Mandatory	Order	Name	Localization Code	Value	Type	Description	Custom Filters
□	□	⇧ ⇩	event_state	event.state	2	Text		
☑	□	⇧ ⇩	event_operation	event.operation		Custom		EventTarget-‹
☑	□	⇧ ⇩	target_name	target.name		Custom		Target-list

Figure 126. Filters tab.

An authorized user can now configure these filters (event_operation and target_name) when executing the report from a generic IBM Security Identity Governance application.

The RD module provides a set of custom filters. The administrator can assign these custom filters directly as they are, or modify their settings as needed. The following table lists all custom filters delivered with the product:

Table 315. Product custom filters.

Filter name	Custom filter description
Target-list	List of targets
EventIN-operation	EventIN codes
EventTarget-operation	EventTarget codes
SoD Type	Names of SoD types

The RD Administrator can modify the current localization code in the **Localization Code** field. If the localization is unsuccessful, it is displayed in red in the **Report Filters Localization** section of the Localization tab. The administrator can add a filter value in the **Fixed Value** text field.

This option is a suggested filter structure for the authorized user executing the report from a generic IBM Security Identity Governance application. The user can also modify this value as needed.

For example, might be configured the filter **user_code** with a fixed value of `03*` and type `Text`. The report available will have a preset filter value of `03*`, meaning that the report will contain all users whose user code begins with 03.

However, the user can change this preset value in the **Type** area, as the following table outlines:

Table 316. Filter type.

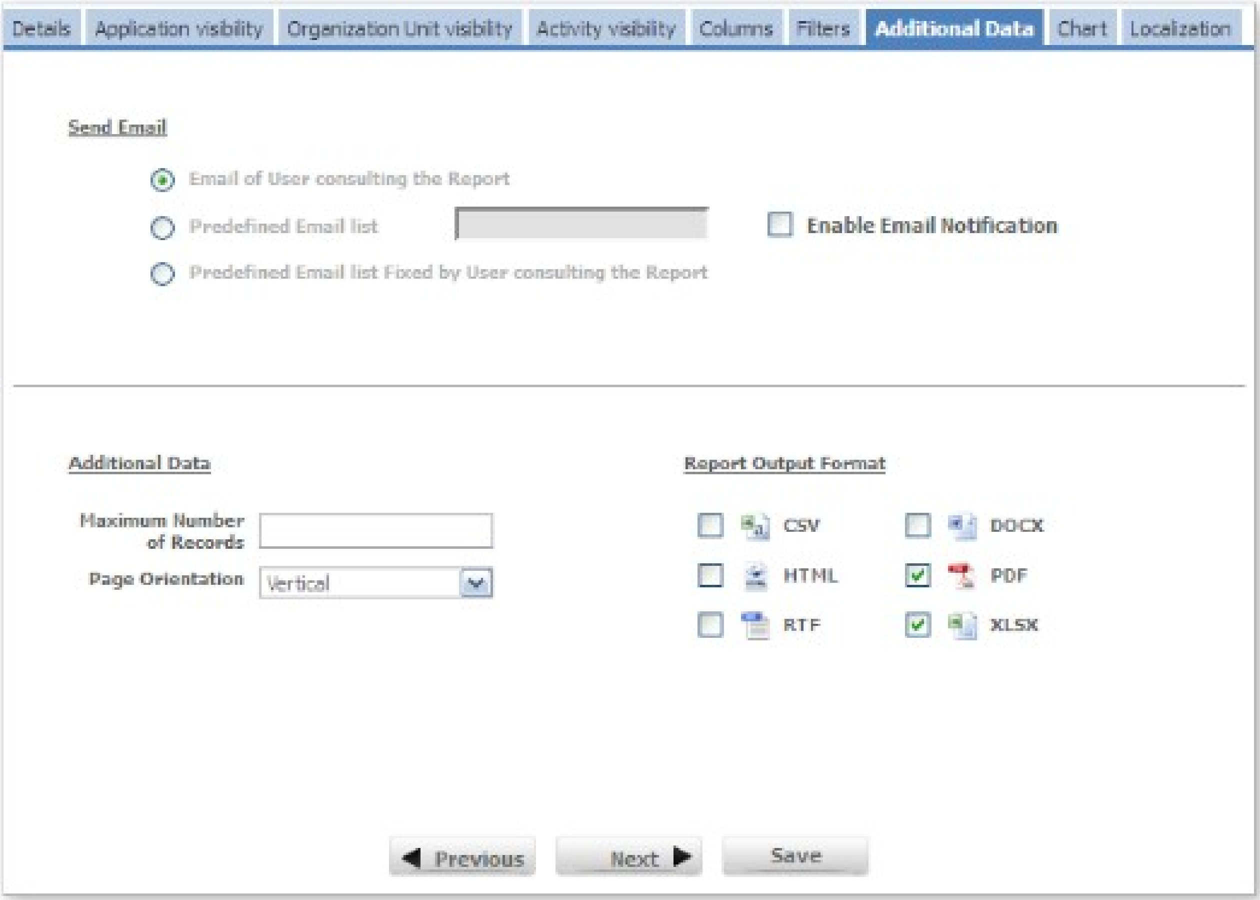
Item	Description
Custom	Relabeled filter
Date (DD/MM/YYYY)	Only date format allowed for this filter type
Extended Date	Both `hh:mm:ss` and `DD/MM/YYYY` formats allowed for this filter type (Inserting hour before date automatically populates the current `hh:mm:ss`, which you can modify)
Number	Only number format allowed for this filter type
Text	Only text format allowed for this filter type

Additional data tab

The RD Administrator can configure additional information in the following three panes:

- **Send Email** pane
- **Additional Information** pane
- **Report Output Format** pane

The following figure shows these panes:



Send Email

● Email of User consulting the Report

○ Predefined Email list

○ Predefined Email list Fixed by User consulting the Report

□ Enable Email Notification

Additional Data

Maximum Number of Records

Page Orientation: Vertical

Report Output Format

□ CSV
□ DOCX
□ HTML
☑ PDF
□ RTF
☑ XLSX

Figure 127. Additional data tab.

In the **Send Email** pane, the RD Administrator can choose to select the **Enable Email Notification** check box to enable the email notification. The following table lists the available email options:

Table 317. Send email pane details.

Available options	Description
Email of User Consulting the Report	A default setting to send an email notification to the user executing the report.
Predefined Email List	List of email addresses to send notifications to: Separate multiple addresses by a semi colon.
Predefined Email List Fixed by User consulting the Report	This option allows the user executing the report to define the list of email addresses to send notifications to.

The following table lists the options available in the **Additional Data** pane:

Table 318. Additional data pane details.

Available options	Description
Maximum Number of Records	Allows a maximum limit to be set on the amount of data drawn by the report.

Table 318. Additional data pane details. (continued)

Available options	Description
Page Orientation	Allows to choose the orientation of the page for the report output: • **Vertical** • **Horizontal**

The RD Administrator can choose one or more of the following output formats in the **Report Output Format** pane:

- **CSV**
- **HTML**
- **RTF**
- **DOCX**
- **PDF**
- **XLSX**

Note: To proceed with the report configuration, the RD Administrator must choose at least one report output format.

Chart tab

Under this tab, the RD Administrator can configure the following summary chart types:

- Bar Chart
- 3D Pie Chart

as shown:

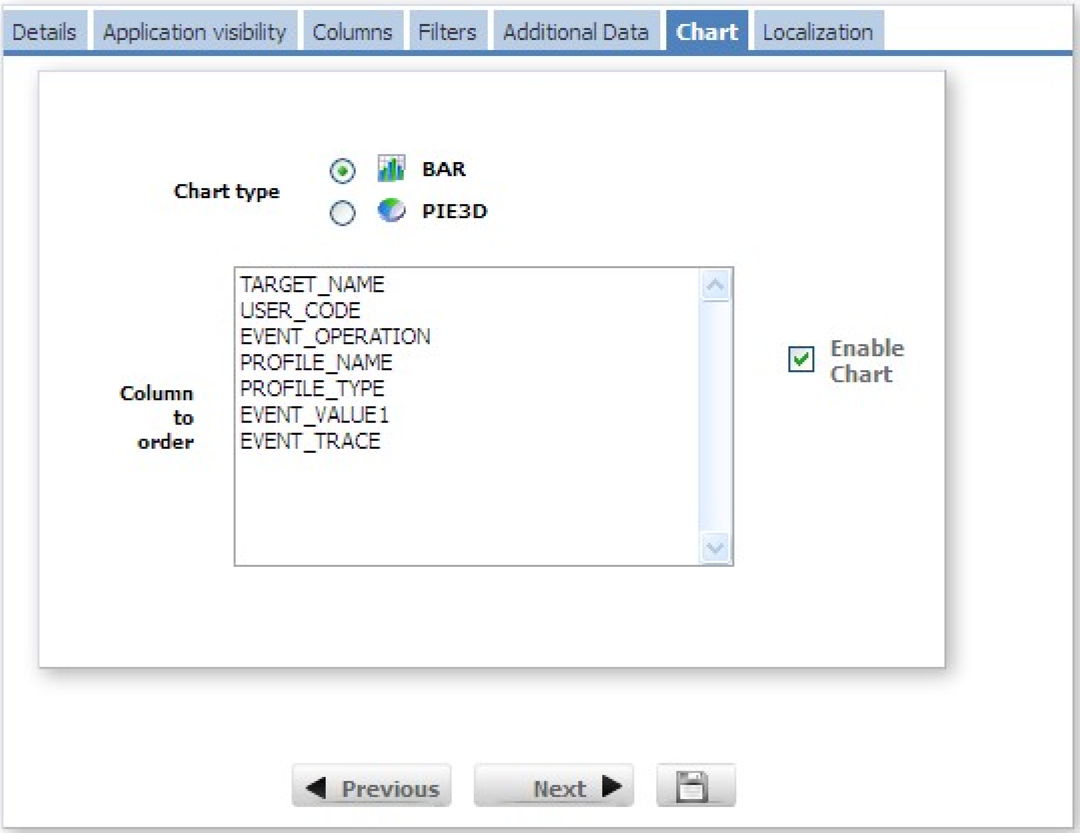


Chart type ● BAR ○ PIE3D

Column to order

TARGET_NAME
USER_CODE
EVENT_OPERATION
PROFILE_NAME
PROFILE_TYPE
EVENT_VALUE1
EVENT_TRACE

☑ Enable Chart

Figure 128. Chart tab.

To enable the chart, the RD Administrator can select the **Enable Chart** check box. The columns available in the **Column to order** box, depend on which columns the RD Administrator selects in the Columns tab.

To make a given column visible in the report, the RD Administrator must select that column in the **Column to order** box. The RD Administrator cannot choose more than one column.

The following figure shows a sample bar chart in the *Report*5.20-Status/Report Visibility:

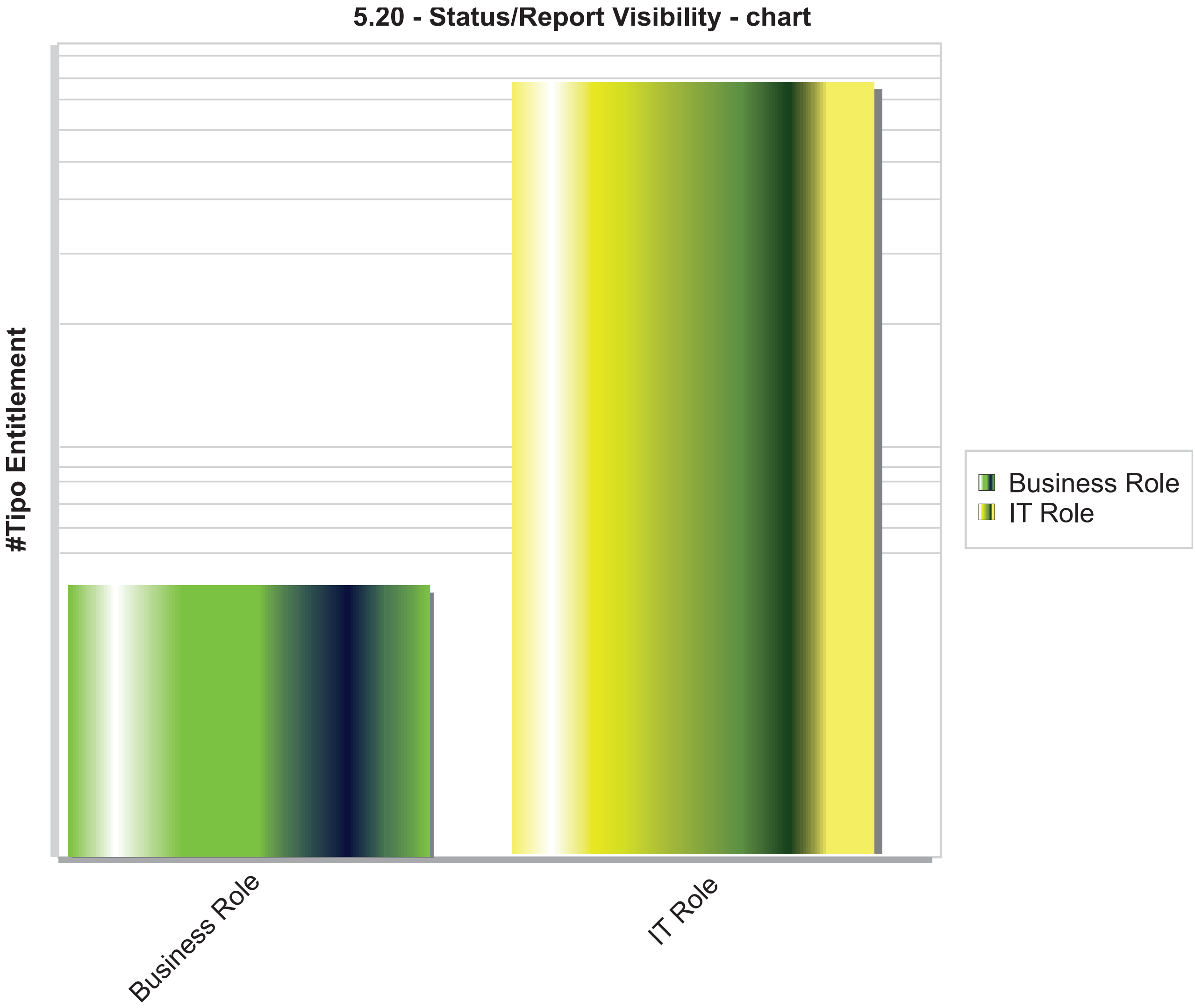


Figure 129. Bar chart.

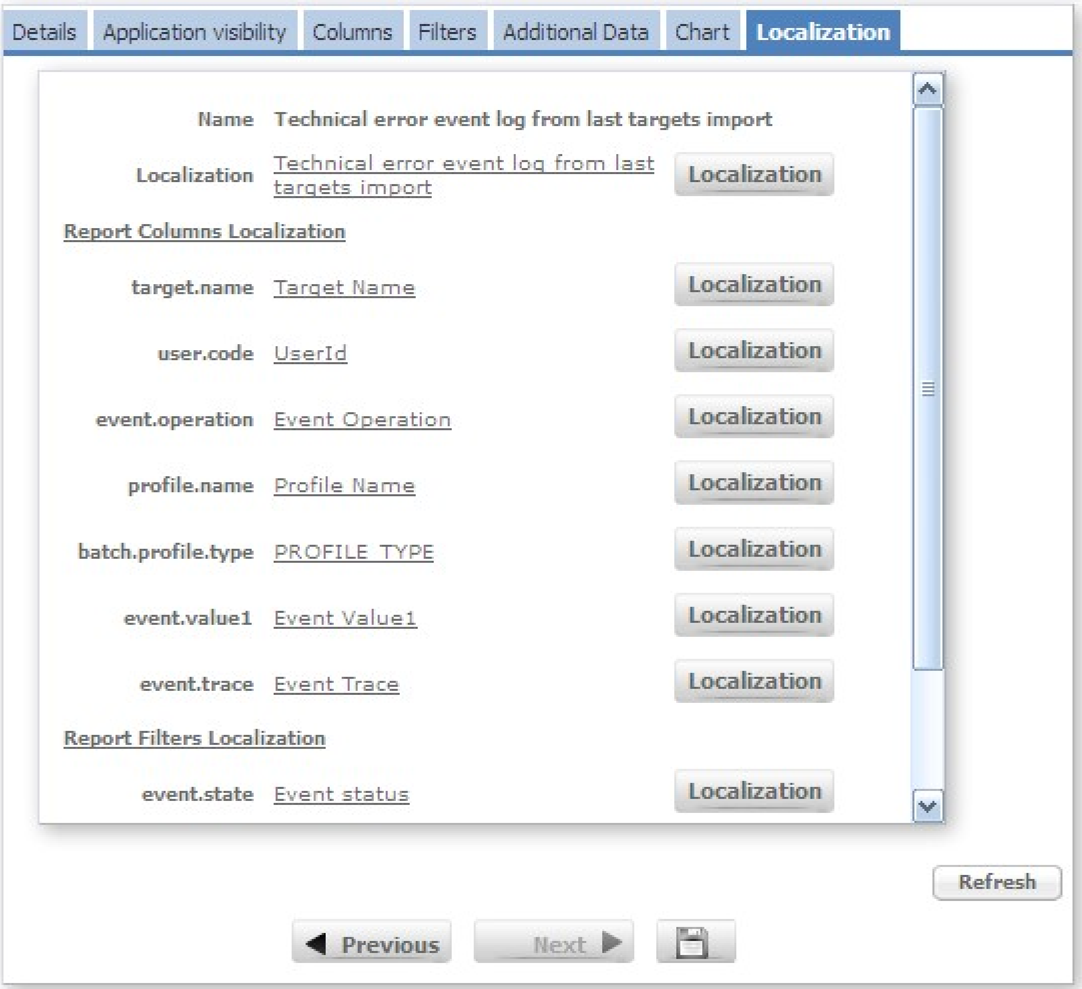
This example illustrates a chart that summarizes the type (horizontal axis) and quantity (vertical axis) of the entitlements that are involved in the report. The chart shows that the report involves Business Role and IT Role entitlements. Four are Business Role entitlements and seventy-seven are IT Role entitlements.

The report output format in the example is an XLSX file. The RD Administrator can configure a report output format under the Additional Data tab.

Localization tab

The following figure shows how to use the **Localization** tab to edit and localize:

- Report labels
- Column labels
- Filter labels



Name	Technical error event log from last targets import	
Localization	Technical error event log from last targets import	Localization

Report Columns Localization

target.name	Target Name	Localization
user.code	UserId	Localization
event.operation	Event Operation	Localization
profile.name	Profile Name	Localization
batch.profile.type	PROFILE_TYPE	Localization
event.value1	Event Value1	Localization
event.trace	Event Trace	Localization

Report Filters Localization

event.state	Event status	Localization

Figure 130. Localization tab.

To edit and localize labels, click **Localization**.

The localization process is based on two main elements:

- The localization code
- The localization message

For each configured language, the RD Administrator must associate each localization code to a specific localization message (**Languages** button in **Edit Labels** section). If the localization message is not configured, the module automatically populates the corresponding language field with the localization code.

Insert the appropriate localization message in the field and click **Ok** to update and automatically save it. Or, if needed, keep the default localization code.

Note: You should first set your preferred language in the **Languages** window of the **Edit Labels** tab.

If the localization message is not localized in any languages, the localization code will be displayed in red.

In this case, the field in the Localization windows displays the localization code. If the codes are not correct, write the appropriate localization message. Otherwise, keep the localization code and click **Ok** to complete the configuration. The color of the localization code changes to black.

Scroll down the list to verify that all values are localized. If, after saving the transaction, some values are not localized, a Warning window provides suggestions.

Note: The field values are automatically refreshed but the **Refresh** button is still active.

Report status and report category

An appropriate status value must characterize a report.

There are three possible values for the status:

- **New**: Report is not yet executed by an IBM Security Identity Governance module (ARC, AGC, ARCS)
- **Assigned**: Report is assigned like an entitlement (of type profile) to an application role (IT Role, BRole)
- **Locked**: Report is locked and cannot be executed by any IBM Security Identity Governance module (this status is reversible).

After the creation, the default status for a report is **New**, but it can change to **Assigned** or **Locked**.

The RD administrator can also decide to catalog the reports into categories:

- **Audit**
- **Changes Detection**
- **Export**
- **Orphaned**
- **Recertification**
- **Status**
- **Sync**
- **Tech Info**
- **Violations**

Categories group together a set of reports that have the same characteristics, for example the user category groups together all user reports, while the audit category groups together all audit reports.

The RD administrator customizes the categories as needed.

Available reports

Report Designer includes a set of categorized reports.

Analysis reports

Table 319. Analysis reports available

Name	Description
Export Tech Transformation (*if External SoD is set, this report is not relevant*)	Produces a downloadable xlsx file containing the complete Business Activity Mapping data associated to an Environment. Use this report to migrate a configuration from one deployment to another or to create a backup of your system.
Role Usage Status Summary	Role usage details for identifying candidate Roles for deletion.
Access Rights not assigned to any OU	Access Entitlements (Business Roles, IT-Roles, Permissions) that are not assigned to any OU as standard privileges belonging to the specific OU (visibility).
Access Rights not assigned to any user	Entitlements (Roles and Permissions) that are not assigned to any user.

ARCS reports

Table 320. ARCS reports available

Name	Description
ARCS - User with FSOD Risks	Full SOD (FSOD) Risks by users. For each of the selected user, the report shows the FSOD Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, Risk type and severity, Domain of reference. You can select by Risk type and user attribute (code, name and surname).
ARCS - SAP and Collective Role Risk overview	Risks joined to SAP and Collective Role. For each of the selected SAP and Collective Role, the Report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, SAP Role type, Risk type and severity, Domain of reference. You can select Risks based on involved activities.
ARCS - User Risks	Risks joined to Users. For each of the selected user, the Report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, Risk type and severity, Domain of reference. You can select by Risk type and user attribute (code, name and surname).
ARCS - SAP authorization Risk overview	Risks joined to SAP authorization. For each of the selected SAP authorization, the Report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the SAP System, Risk type and severity, Domain of reference. You can select Risks based on involved activities.
SAP Authorization and Business Activity Catalog	Technical Transformation, that is the associated SAP Authorization for each Business Activity.
SAP Role and AuthObj Catalog	SAP Role Catalog filtered by SAP System. It also shows SAP Role links to Authorization Objects.

Table 320. ARCS reports available (continued)

Name	Description
SAP Role and Transaction Catalog	SAP Role Catalog filtered by SAP System. It also shows SAP Role links to Transactions.
SAP Role Catalog	SAP Role Catalog filtered by SAP System. It also shows SAP Role incompatibility by level (Low/Medium/High).
SAP Authorization Definition	SAP Authorization definition, showing how an SAP Authorization is joined to Transactions, Authorization Objects, and Fields. It also shows the logical conditions among objects.
SAP Role and Business Activity Catalog	SAP Roles by Business Activity.

Audit reports

Table 321. Audit reports available

Name	Description
Workflow history	Requests and steps from the audit trail.
Audit Trail - User authorizations history	Sequence of `add`, `remove` and `reviews` user requests, by user
IDEAS Audit	Collection of data for audit and compliance purposes. You can configure the amount of information displayed by selecting users reported (Visibility).

Campaigns reports

Table 322. Campaigns reports available

Name	Description
Certification - Fulfilment status summary	Status summary with details for the fulfilment status (applicable for Applications not subject to write back sync).
Certification - Status summary by OU	Report of Organization Unit Entitlements Certification. Each Reviewer in a Certification of this type reviews an Organization Unit, and is expected to review all access privileges. This report aggregates all entitlements that can be granted to users belonging to these OUs.
Certification - Status summary by Reviewer	Report of User Entitlement Certification. Reviewer in a certification of this type review the access privileges of the users in his scope.
Certification - OU visibility - Status summary	Completion status of an `OU visibility` Certification Campaign.
Access Certification Campaigns Status	Completion status of Access Certification Campaigns. For each Organization Unit the Report shows the number of Users that require a Review and the actual Certification statistics. Only Organization Units where an Access Certification action is required, are included in this Report.

Export reports

Export reports use an associated query that produce files that can be used with the Bulk Load tool.

Table 323. Export reports available

Name	Description
External Role Bulk	External Roles using the Export External Role Hierarchy query.
Export Tech Transformation	Business activity mapping data for an environment.
Remediations to risks Bulk (*if External SoD is set, this report is not relevant*)	Remediation details and the associated remediated risks.
Entitlements Bulk	List of the Entitlements.
Applications Bulk	List of all the Applications.
Organizational Units Bulk	Hierarchy of Organizational Units (OU).
Resources Bulk	List of Resources.
Entitlements to Users Bulk	List of users and their assigned Entitlements (Business Roles, IT-Roles, Permissions).
Users Bulk	List of the users
Activities hierarchy Bulk (*if External SoD is set, this report is not relevant*)	Business activities and their hierarchical structure.
Profile to domain Bulk (*if External SoD is set, this report is not relevant*)	Exports `Permissions to Domain` IDEAS configurations for editing and re-import.
Risk Structure Bulk (*if External SoD is set, this report is not relevant*)	Details on the `Risk` structure. You can select Risks based on the Environment.

Optimizer reports

Table 324. Optimizer reports available

Name	Description
User KRI summary	Extracts User Score indicators and computes the average overall Score index. This Report does not including the Similarity Divergence KRI.
Candidate Role - User List	Candidate Role users assigned. Use it to support shrinking of the number of user assignments in systems other than IGI.
Candidate Role - Entitlement List	Candidate Role entitlement list. Use it to support the manual constructions of roles in systems other then IGI
Candidate Role - Role Metrics	Candidate Roles core metrics dump.

Policies reports

Table 325. Policies reports available

Name	Description
IDEAS Report List	All reports available.
IDEAS Report Visibility	Administrative Roles (Entitlements) that include each report. Users who have an Admin Role for the report can configure and run the report.
IDEAS Report Structure	Reports structures, including columns and localization details.
Mitigations assigned to Risks (*if External SoD is set, this report is not relevant*)	For each Risk, the report shows the Mitigations assigned and Mitigation details.
Access Rights Visibility by OUs	Entitlements (Business Roles, IT-Roles, Permissions) that are directly assigned to each OU. Report visibility can be set based on Application.
Technical Transformation (*if External SoD is set, this report is not relevant*)	Business Activity Mapping relations, with entitlements (Roles/Permissions) for each Business Activity.
Risk Structure (*if External SoD is set, this report is not relevant*)	Shows detailed information on Risks. You can select Risks based on Activities and other parameters such as Risk Type and Environment. Details provided for each Risk include: name, description, type, severity and referred activities.

Status reports

Table 326. Status reports available

Name	Description
Users by Application	For each of the selected Applications, the Report shows the users (and the belonging Organization Unit) that have assigned entitlements from that Application.
User Assignments	Access rights by user. Users are selected depending on visibility settings. For each selected user, the report shows Entitlements (Permissions, IT-roles, Business Roles) assigned to the user.
Delegation assignments	Delegation assignments with information on delegated and represented users. Details include OU, email and delegated Entitlements, including validity start and end dates for the Entitlements).
Account Status	Account details and status are provided together with possible locking codes.
Account matching status	For every Account configuration, the number of matched, unmatched, and orphans accounts.
Accounts created in last X days	List of all accounts created in the last X days.
Account expiring in next X days AM	List of all accounts created that are going to expire in the next X days.
Activities created in last X days	List of all activities (Access Risk Controls module) created in the last X days.

Table 326. Status reports available (continued)

Name	Description
Permission created in last X days	List of all permission created in the last X days.
Technical transformation status	List of Business Activity Mapping relations defined in the system.
User Permission's indirect assignments	Permission assigned through the assignment of a Business Role or an IT Role.
Role hierarchical structure	Role Structure. Only structured Entitlements (such as Business Roles and IT Roles) are considered.
Application Entitlements dictionary	Entitlements (Business Roles, IT-Roles, Permissions), by Applications, with details for each entitlement.

Sync reports

Table 327. Sync reports available

Name	Description
Reconciliation - Sync Status by Target	Accounts and Permissions reconciliation status where conditions are applicable to the use IGI as Master repository or as a slave.
Reconciliation - Sync Status	Accounts and Permissions reconciliation status where IGI is the master source of data
Reconciliation - Sync Status [Coarse Grain]	Accounts and Permissions reconciliation status where IGI is the master source of data. No changes propagated from target system back to IGI. This version compares at permission level, ignoring rights name and values
Reconciliation - Target event queue extraction	Events arrived from the target system queue during the last synchronization.
Import from Target - error event log	Shows details of all Events generated during the last import from target system applications.
Events-OUT - Targets Queue extract	Events in the outbound queue applicable only in case of automatic provisioning towards target system applications.
Events-IN - HR Queue extract	Events in the inbound queue, received from HR system used as authoritative source.
User Assignments Changes	Lists all users changed their Permissions (Business Roles, IT-Roles, Permissions) assignments in the last 7 days. Users can be selected by Organization Units and Application. For applications, only Users that have assigned Entitlements from the specified Application are included.
Role Structure Changes	Roles that had changes in their entitlements in the last 7 days.

Violations reports

Table 328. Violations reports available

Name	Description
User Violations and Mitigations (*if External SoD is set, this report is not relevant*)	Allows Compliance Managers, or other authorized Reviewers, to certify Risks and related Mitigation Controls. Each Reviewer in a Certification of this type is focused on the set of users defined by his visibility settings, and is expected to review all Risks connected to access-privileges for each of these users. Furthermore, Mitigation Controls possibly linked to those Risks are reviewed.
Application - Licence status summary	Active accounts versus licence counts per Application.
User Violations Count (*if External SoD is set, this report is not relevant*)	Provides a number of statistics on users that have associated Risks. Visibility can be set at the Application, Organization Unit, and Activity levels.
Role Violations Overview (*if External SoD is set, this report is not relevant*)	Provides details on Risks associated to Entitlements. For each selected Entitlement, the report shows the Risks that are assigned and the Activities that cause the Risks. Other details include the belonging Application, Entitlement type, Risk type and severity, Domain of reference. You can select Risks based on involved activities.

Available dashboard items

Create and customize dashboard items in Report Designer. A set of configured dashboard items is provided.

Dashboard items are listed in the Report Designer in **Manage** > **Dashboard**. They are listed in the following table by name and the Administrative Role that they are assigned to in the product as shipped.

Table 329. Dashboard items available

Name	Intended Administrative Role
Access certification status	Available to any user who is assigned as a supervisor or reviewer in one or more access campaigns. Not listed in Report Designer. See the description in User Manager.
Access request history	Employee
Account matching status	Application Manager
Accounts created in last x days	Application Manager
Accounts expiring in next x days with application scope	Application Manager
Accounts expiring in next x days with OU scope	User Manager
Activities created in the last x days	Application Manager

Table 329. Dashboard items available (continued)

Name	Intended Administrative Role
Approval tasks	Available to any user who has an Admin Role with access to the Daily Work workflow. Not listed in Report Designer. See the description in User Manager.
Business activity mapping status	Application Manager
Approval tasks	User Manager
Days until the next password expiration	Employee
Delegation assignments	User Manager
Locked accounts	User Manager
My entitlements	Employee
My requests	Employee
Partial requests	Employee
Pending requests	User Manager
Permissions created in the last x days	Application Manager
Policy violation requests	Employee
Recent requests	Employee
Rejected requests	Employee
Unmatched accounts	Application Manager
User violations	User Manager
User violations without mitigation	User Manager

Building a new report: A brief roadmap

A roadmap is provided to configure a new report.

The RD administrator can use the following logical roadmap (not mandatory) to define the reports:

1. Create a query (found in the dedicated **Query Management** section).
2. Import the **Query Columns**.
3. If the query contains definitions for temporary tables, use the scope list from the scope management section to associate the scope to the query.
4. From **Manage** > **Report**, choose the query to associate to the report.
5. Follow the steps in the wizard to configure the report.

Manage

The following functions for managing the main entities of this module are available:

"Query" on page 606

In this section, the administrator can choose to create and customize queries or configure the report using an already existing query.

"Report" on page 610

In this section, you can find the procedures for customizing a report based on the values defined in the relevant query.

"Dashboard" on page 613
Create dashboards or configure dashboard items to be used on Dashboard home pages in Service Center.

Query

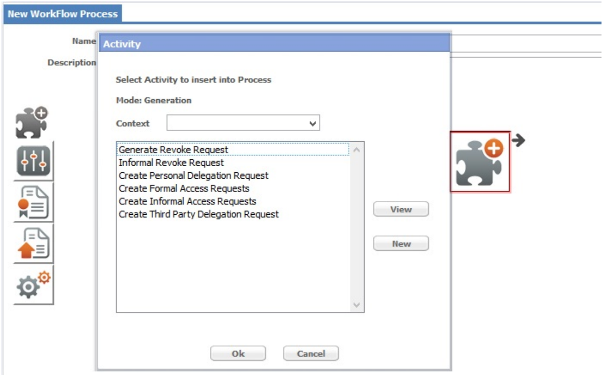
In this section, the administrator can choose to create and customize queries or configure the report using an already existing query.

The **Query** pane (left), contains the list of inventoried queries, filters for the query search and controls to perform the import/export operations.

The **Name** and **Description** filters are available for the query search.

The **Query** pane, lists the results, according to the following attributes:

Table 330. Query Attributes.

Name	Description
Name	Query name. An icon is present near the item name, depending on the type of item: • for a product item. •  New WorkFlow Process Name Description Activity View New Ok Cancel Select Activity to insert into Process Mode: Generation Context Generate Revoke Request Informal Revoke Request Create Personal Delegation Request Create Formal Access Requests Create Informal Access Requests Create Third Party Delegation Request for a custom item.
Description	Brief query description (maximum 256 characters)

The tabs on the right contains the following main sections:

- Query Management tab

- Scope Management tab
- Joined Report tab

ℹ	**Note:** In this section, switching from one tab to another does not discard intermediate changes. However, the **Save** button (top right corner of the host pane) is still active.

The main operations available in this section are listed below.

Query search

Proceed as follows:

1. In the **Query** pane, click **Filter/Hide Filter**.
2. Set the data filter (**Name** and **Description**) and click **Search**. The results are displayed in the same pane.
3. To import a query:
   - In the left pane, click **Import**.
   - In the Import Query/Report window that displays, click **Browse** to search for a file to upload (available formats are `.zip`, `.gzip`, `.tar` and `.gz`).
   - After the file selection, click **Ok** to confirm the operation.
   - An Import Query window opens, showing the process status.
   - After the process is finished, click **Ok** in the window showing the operation outcome.
   - At the end of the operation, a window displays, asking if the administrator wants to import another file. In the same window, click **Ok** to import a new file.
4. To export a query:
   - In the left pane, select the **Query** to be exported.
   - In the left pane, click **Export**.
   - A system-based window displays, prompting you to either open or save the file in XML format.
   - Click **Ok** in the window showing the operation outcome.

The XML file name contains:

- The name of the query.
- The date the query was created.
- The time the query was generated.

ℹ	**Note:** If an imported query has the same name as an existing query, a Warning displays a diagnostic message regarding the effects of the operation.

ℹ	**Note:** Attempting to import a file that is not in XML format generates a Warning which displays a diagnostic message regarding the effects of the operation.

Create a query

Proceed as follows:

1. In the **Query** pane (left), click **Add**.
2. In the **Query Details** pane (right), specify the query details and write the query according to your needs.
3. At the bottom right corner, click **Save**.
4. Click **Ok** in the window showing the operation outcome.

The query will be saved as custom query.

For help about the query processing, click **Help** at the bottom right corner in the same pane.

Modify a query

This operation is available only for the custom query.

Proceed as follows:

1. In the **Query** pane (left), select the query to be modified.
2. In the **Query Details** pane of the **Query Management** tab (right), modify the SQL query and any query data.
3. At the bottom right corner, click **Save**.
4. Click **Ok** in the window showing the operation outcome.

Remove a query

This operation is available only for the custom query.

Proceed as follows:

1. In the **Query** frame (left) select the query to be removed.
2. Click **Remove**.
3. Click **Ok** to confirm the operation.
4. Click **Ok** in the window showing the operation outcome.

Note: Removing a query eliminates its links with the scope and the report.

Query management tab

In the **Query Details** pane, the SQL query text area allows you to create a custom query.

If you need assistance writing the query, click **Help**, in the bottom right corner of the same pane. The Available query Keys window displays. After selecting the query key, click **Ok** to automatically insert the key into the **SQL Query** text area.

The RD administrator can add, modify or remove the report columns.

There are two ways to add and populate the columns:

- Individually, using the Add function.
- Automatically, using the Import query columns function.

Figure 131. The Query Management window.

Add and fill query columns individually

This operation is available only for a custom query.

Proceed as follows:

1. In the Query column pane, click **Add**.
2. Fill the column fields with the values defined in the query.
3. At the bottom right corner of the same pane, click **Save**.

If necessary, repeat the steps 2 and 3.

Add and fill query columns automatically

This operation is available only for the custom query.

Proceed as follows:

1. In the Query column pane, click **Import query columns** , this automatically adds the columns and populates them with the values defined in the query.
2. At the bottom right corner of the same pane, click **Save**.

Remove query columns

This operation is available only for the custom query.

Proceed as follows:

1. In the Query column pane, click **Remove**.
2. At the bottom right corner of the same pane, click **Save**.

Note:

Removing columns in this frame also eliminates them from the **Report Wizard section** > **Columns** tab.

Scope management tab

In this section, scopes can be associated to queries.

The **Query** tab, displays the queries listed in the system. The **Scope management** tab displays the list of scopes already associated to the selected query.

Clicking **Add**, the Scope List window opens, displaying the list of scopes that the RD Administrator can associate to the queries selected in the Query pane on the left. The Scope list windows provides **Name** and **Description** filters for a scope search (clicking **Filter/Hide Filter**). From this window, you can add a new scope by clicking **New**, and edit a custom scope by clicking **Edit**.

Note: The product scopes cannot be edited.

To view the scope details, click **Details**. You cannot perform changes in this window. To remove a scope, click **Remove**.

Note:

- Removing a scope results in the loss of its visibility configuration; the tmp. table is still part of the query but contains no data.
- After removing a scope from the selected query, all aggregations with any other query will be lost.

Joined Report tab

This section displays the reports associated to a selected query.

In the **Query** tab, when selecting a query, the list of associated reports is displayed in the right frame.

Report

In this section, you can find the procedures for customizing a report based on the values defined in the relevant query.

In this section, you can:

- Create a report
- Copy a report
- Attempt a query execution

The report filters are listed in the table below:

Table 331. Report filters.

Filter	Description
Name	Report name.
Description	Brief report description.
Status	Report status: • **Assigned** • **Locked** • **New**
Report Category	Inventoried reports category.

The same pane lists the results, according to the following attributes:

Table 332. Report attributes.

Attribute	Description
Name	Report name. An icon is present near the item name, depending on the type of item: • 🧩 🎚 📄 ⬆ ⚙ for a product item. • 🧩 🎚 📄 ⬆ ⚙ for a custom item.
Status	Report status: • **Assigned** • **Locked** • **New**
Report Category	Inventoried reports category. Click **Add** to inventory a new category.

The main sections described in this paragraph are listed below:

- Report Inventory
- Create a New Report
- Configure a Product Report
- Copy a Report
- Simulate a Report

Report Inventory

The RD module has a list of **Product Reports** that the RD Administrator can assign directly to the users. The administrator can also use the procedure in this section to create a new report.

Report search

Proceed as follows:

1. In the **Reports** tab, click **Filter/Hide Filter**.
2. Set the data filter and click **Search**. The results are displayed in the same pane.
3. To import a report:
   - In the left pane, click **Import**.
   - In the Import Report/Query window that displays, click **Browse** to search for a file to upload (available formats are `.zip`, `.gzip`, `.tar` and `.gz`).
   - After the file selection, click **Ok** to confirm the operation.
   - An Import Report window opens, showing the process status.
   - After the process is finished, click **Ok** in the window displaying the operation outcome.
   - At the end of the operation, a window displays, asking if the administrator wants to import another file. In the same window, click **Ok** to import a new file.
4. To export a report:
   - In the left pane, select the **Report** to be exported.
   - In the left pane, click **Export**.
   - A system-based window displays, prompting you to either open or save the file in XML format.
   - Click **Ok** in the window displaying the operation outcome.

The XML file name contains the report name, date, and hour.

Create a report

To create a report, proceed as follows:

1. From the **Reports** tab, click **Add** .
2. The **Details** tab opens. This is the starting point of the Report Configuration Wizard.

Configure a product report

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.
3. In the right pane the wizard opens by default. Follow the steps to configure the **Product Report**.

Copy a report

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.

3. Click **Copy**.
4. The **Details** tab opens by default. Insert the required information and follow the wizard to configure the report.

Note: This operation is recommended for changing configuration settings while still maintaining the joined report query values.

Report simulation

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.
3. Click **Test**.
4. The Report Simulation window opens.
5. Clicking **Ok**, the Report Simulation Wizard begins.
6. Choose the **Report format** (PDF, XLSX, CSV), then click **Next**, followed by **Execute**.
7. A system-based window displays prompting you to save the file in the chosen format.
8. Click **Ok** in the window showing the operation outcome.

The file name contains the report name, date, and hour.

Remove a report

Proceed as follows:

1. Perform a report search.
2. In the **Reports** tab, select the desired report.
3. Click **Remove**.
4. To confirm the operation, click **Ok** in the window that displays.
5. Click **Ok** in the window showing the operation outcome.

Dashboard

Create dashboards or configure dashboard items to be used on Dashboard home pages in Service Center.

Dashboard items are special types of reports. They are associated with a query, which produces the data to display. To be visible, dashboard items must be assigned to an Entitlement.

Users who have the Admin Role have the Entitlements that are assigned to the Admin Role. The corresponding dashboard items are included in the Dashboard home page Service Center. Users who are assigned to multiple Admin Roles see a **Dashboard** home page in Service Center. It consists of all the dashboard items from all of their Admin Roles.

You work with dashboard items in **Report Designer** > **Manage** > **Dashboard**.

- A list of dashboard items is shown in the left pane, **Dashboards**.
- Attributes are organized in tabs in the right pane. The tabs that are shown depend on the dashboard item you select.

The following controls are in the left pane:

- A list of dashboard items
- **Actions** - Click to select **Copy**, **Test**, **Remove**, or **Add from Query**.
- **Filter** - Filters are used to search the list.

In the list, you can see information in fields for each dashboard item, as listed in the following table.

Table 333. Dashboard item fields

Field	Description
Name	Dashboard item name. An icon shows the type of item: • Product item, which can be copied but not deleted. Only some attributes can be edited for a product item. • Custom item.
Status	• **New** - Not yet assigned to an entitlement • **Assigned** - The dashboard item is assigned to an Entitlement. • **Locked** - The dashboard item is locked and cannot be edited.
Article	Dashboard item type. It can be Product or Custom.

Dashboards for personas

See the following sections to see how the Dashboard home page can be configured for personas.

- Application Manager
- User Manager
- Employee

Tasks for working with dashboard items

You can do the following tasks for dashboard items.

- Search, by using filters
- Edit
- Test
- Copy
- Add from Query
- Remove
- Assign to an Entitlement

Note:

- You can create dashboard items from existing queries. As an alternative, you can copy a product dashboard item and edit it.

- You cannot remove product dashboard items. You can delete copies that you made.

Searching for a dashboard item

1. In the left pane, click **Filter**.
2. Enter the search criteria in the fields: **Name** or **Status**.
3. Click **Search**. The list is updated to show only dashboard items that meet the search criteria.

Click the **Dashboard** tab above the left pane to show the full list again.

Table 334. Dashboard item filters

Filter	Description
Name	Dashboard item name
Status	Dashboard item status values • **New** • **Assigned** • **Locked**

The attributes for filters appear in the **Details** tab for a dashboard item.

See "Available dashboard items" on page 604 for the full list of available dashboard items.

Editing a dashboard item

You can edit some information in a provided dashboard item. You can edit all information in a dashboard item that you copied.

1. In the left pane, select a dashboard item.
2. The **Details** tab opens in the right pane. You can move among the tabs in the following ways:
   - Click the tabs at the top of the right pane.
   - Use the wizard. Click **Next** and **Previous** to move through the tabs.
3. Click **Save** to save your changes.

Testing a dashboard item

You can test a dashboard item to display the effects of your changes.

1. In the left pane, select a dashboard item.
2. Click **Test** in the left pane. A sample of the dashboard item is shown.
3. Click **OK** when you are done.

Copying a dashboard item

As an alternative to creating a dashboard item directly, you can copy an existing product dashboard item and edit it.

1. In the left pane, select a dashboard item.
2. Select **Actions** > **Copy**.
3. Enter a name for the copy.
4. Click **Save**.

Creating a dashboard item

You can create a custom dashboard that is based on a defined query. You can use the properties of the query to set up the dashboard visibility and attributes.

Important: The options that follow depend on the properties of the query to which the dashboard is linked. You might not encounter some of these options all the time.

1. In the left pane, select **Actions** > **Add from Query**.
2. Select one of the queries that are listed in the Query window.
3. In the Details page in the right pane, enter a name and a description for the new dashboard. Select a chart type for the dashboard. Optionally, select **Show legend** to display the dashboard legend in Service Center. Click **Next**.
4. In the Application visibility page, define the visibility scope of the dashboard. The page is displayed only if the scope of the query is set to Application Scope. Click **Next**.
5. In the Organization Unit visibility page, define the visibility scope of the dashboard. The page is displayed only if the scope of the query is set to Organization Unit Scope. Click **Next**.
6. In the Layout page, select which query columns you want to display in the dashboard and how you want them to be labeled. Click **Next**.
7. In the Filters page, define how the query columns filter the data that is displayed in the dashboard. Click **Next**.
8. In the Localization page, configure globalized strings for labels in the dashboard.
9. Click **Save**. The new dashboard definition is added to the list in the left pane.

Follow the instructions in “Assigning a dashboard item to an entitlement” to make the dashboard available to a user with a particular entitlement.

Attention: Dashboards that are created in this way do not support the drill down action.

Removing a dashboard item

You cannot remove product dashboard items. You can remove copies that you made.

1. In the left pane, select a dashboard item.
2. Select **Actions** > **Remove**. This menu item is not active for product dashboard items.
3. Click **OK** to confirm.

Assigning a dashboard item to an entitlement

1. In **Report Designer**, click **Configure** > **Assignment**.
2. In the **Report/Dashboard > Entitlement** tab, click a dashboard item. The current assignments are shown in the right pane. You can also click the **Entitlement > Report/Dashboard** tab to see the list of entitlements and the reports that are assigned to them.
3. In the right pane, use the **Actions** menu to add or remove entitlements.

Details tab

Configure basic information about the dashboard item.

Table 335. Details tab fields

Field	Description
Query name	Read-only field. Click **Show Query** to go to the **Query** tab and view the query.
Description	Description of the dashboard item.
Name	Name of the dashboard item.
Status	• **New** - Not yet assigned to an entitlement • **Assigned** - Automatically set if the dashboard item is assigned to an entitlement. • **Locked** - The dashboard item cannot be assigned.
Chart layout	Choose one of the following chart types: Single value, Table, Pie, Line, Bar, Area, Scatter. Depending on the query, not all choices can be available.
Show legend	Check to show a legend for the chart.

Organization Unit visibility tab

Configure the scope of data that is available in the dashboard item. This tab is available only if the query scope is set for Organization Unit scope.

The following table lists the fields in the **Organization Unit visibility** tab.

Table 336. Organization Unit visibility tab fields

Field	Description
Name	Read only. The name of the Organization Unit scope.
Description	Read only. The description of the scope.
All entities of type Organization Unit with no selection	Choose to use all data from all entities of the Organization Unit.
Admin scope of Organization Unit with no selection	Choose to constrain the data for the dashboard item to the administrative scope of the Organization Unit. **Note:** An Admin Role that includes a dashboard item of this scope must have a scope of **Org Unit**. Set the Admin Role scope in **Access Governance Core** > **Configure** > **Admin Roles** in the **Scope** tab.

Application visibility tab

Configure the scope of data available in the dashboard item. This tab is available only if the query scope is set for Application scope.

Table 337. Application visibility tab fields

Field	Description
Name	Read only: the name of the Application scope.
Description	Read only: the description of the scope.
All entities of type Application with no selection	Choose to use all data from all entities of type Application.
Admin scope of Application with no selection	Choose to constrain the data for the dashboard item to the administrative scope of the Application. **Note:** An Admin Role that includes a dashboard item of this scope must also have a scope of **Application**. Set the Admin Role scope in **Access Governance Core** > **Configure** > **Admin Roles** in the **Scope** tab.

Layout tab

Configure how columns are available and labeled in the dashboard item. A list of the columns that are defined by the query is shown. Configure information for each column.

Table 338. Layout tab fields

Field	Description
Selected columns	Select to show the column. Clear to hide the column.
Name	Read only: the name of the column. It is read from the query.
Localization Code	The name of the localization code that corresponds to the column name. Click the information icon to the right to display the current list of localizations for the code. ℹ

Filters tab

Determine how filters are available in the dashboard item. A list of columns that are candidates for filters is shown.

Table 339. Filter tab fields

Field	Description
Visible	Check to allow the user to filter data by this column on the dashboard. The user sees **Filters** in the **Settings** menu for the dashboard item as it appears in the Service Center. Clear to disable filtering for this column
Mandatory	Read only. If checked, a filter must be set for this column.

Table 339. Filter tab fields (continued)

Field	Description
Order	Select a filter column, then click the arrows to position it in the list. The order determines the axis assignment for the columns.
Name	Read only: the column to filter.
Localization Code	The name of the localization code that corresponds to the column name.
Value	Enter a value to constrain the query. For example, if the query object is **Accounts expiring in the next x days**, then specify the number of days to use to constrain the query for the dashboard item.
Type	Select the data type to display.
Description	Enter a description for the filter.
Custom Filters	If you set **Type** to **Custom**, you can choose a custom filter from the list.

Localization

Configure localized strings for labels in the dashboard item. When you click **Localization** for a field, a window prompts you for the localized string to use for each language.

Table 340. Localization tab fields

Field	Description
Localization	The name of the dashboard item.
Columns localization	A line appears for each column. The localization code and text is shown.
Filters localization	A line appears for each filter. The localization code and text is shown.

Configure

Use the following functions for configuring the listed elements:

- Report Assignment
- Menu

Report assignment

From this section, you can move to the Report/Dashboard-Entitlement and Entitlement-Report/Dashboard tabs.

Report/Dashboard-Entitlement

The **Report/Dashboard** > **Entitlement** tab (left), contains the list of inventoried reports and filters for the Report search.

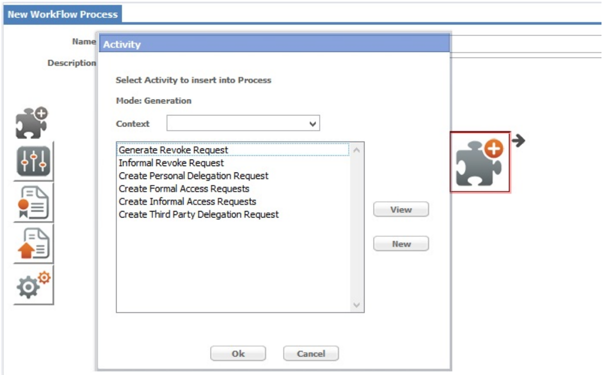
The table below summarizes the filters (clicking the **Filter/Hide Filter** button) available for the Report search:

Table 341. Report filters.

Filter	Description
Name	Name of the report.
Code	
Status	Available report status: • **Assigned** • **Locked** • **New**
Category	Category of the report.
Display Type	Display types of the report: • **Report** • **Dashboard**

The same frame lists the results according to the following attributes:

Table 342. Report attributes.

Name	Description
Name	Name of the report. An icon is present near the item name, depending on the type of item: • for a product item. •  New WorkFlow Process Name Description Activity Select Activity to insert into Process Mode: Generation Context Generate Revoke Request Informal Revoke Request Create Personal Delegation Request Create Formal Access Requests Create Informal Access Requests Create Third Party Delegation Request for a custom item.
Status	Available report status: • **Assigned** • **Locked** • **New**
Report Category	Category of the report

After creating a report, the administrator can assign it to a user.

The administrator can also assign reports to an application role (IT Role, Business Role) as permission-type entitlements. When a report is selected, the entitlements already assigned to that report are displayed in the **Assignment** tab.

If you click **Add** in the **Assignment** tab , the **Entitlements** panel is displayed and enables you to search (clicking **Filter**) and associate new entitlements with the report. The following table lists and describes the assignable entitlement filters.

Table 343. Assignable entitlement filters.

Filter	Description
Application	Application name: Entitlements filtered mainly according to the specified application.
Name	Name of assignable entitlement: matches with the application entitlements inventoried in the AG Core Module.
ID Code	
Type	Entitlement type: • **IT Role** • **Business Role**

Entitlement->Report/Dashboard

The **Entitlement** > **Report/Dashboard** tab (left) contains the list of entitlements and filters for the entitlement search.

The table below summarizes the available filters for the entitlements search:

Table 344. Entitlement filters.

Filter	Description
Application	Application name: Entitlements filtered mainly according to the specified application.
Name	Name of assignable entitlement: matches with the application entitlements inventoried in the AG Core Module.
ID Code	
Type	Entitlement type: • **IT Role** • **Business Role**

In the same tab are listed the results, according to the **Name** (Entitlement name) and **Application** (Application name) attributes. After selecting an entitlement from the list, the **Assignment** tab displays the reports that are already assigned to that entitlement.

If you click **Actions** > **Add** in the **Assignment** tab , the **Reports/Dashboard** panel is displayed and enables you to search (clicking **Filter**) and associate new reports to the entitlements. The following table lists and describes the assignable report filters:

Table 345. Assignable Reports filters.

Filter	Description
Name	Name of the report.
Code	

Table 345. Assignable Reports filters. (continued)

Filter	Description
Status	Available report status: - **Assigned** - **Locked** - **New**
Category	Category of the report.
Display Type	Display types of the report: - **Report** - **Dashboard**

Report-Entitlement tab

The **Report** > **Entitlement** tab (left), contains the list of inventoried reports and filters for the report search.

The table below summarizes the filters available for the Report search:

Table 346. Report filters

Filter	Description
Name	Name of the report.
Description	Brief description of the report.
Status	Available report status: - Assigned - Locked - New
Report Category	Category of the report.

The same frame lists the results according to the following attributes:

Table 347. Report attributes.

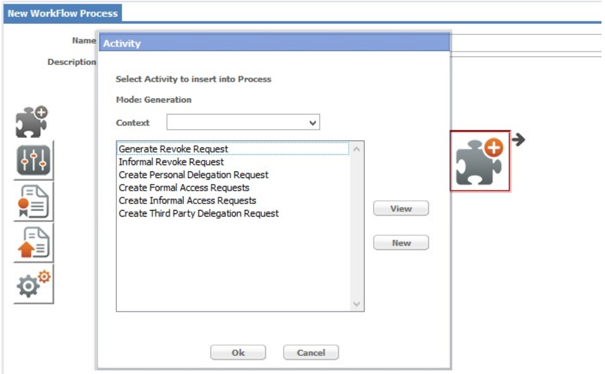
Name	Description
Name	Name of the report. An icon is present near the item name, depending on the type of item: - for a product item. -  New WorkFlow Process Name Description Activity Select Activity to insert into Process Mode: Generation Context View New Ok Cancel Generate Revoke Request Informal Revoke Request Create Personal Delegation Request Create Formal Access Requests Create Informal Access Requests Create Third Party Delegation Request for a custom item.

Table 347. Report attributes. (continued)

Name	Description
Status	Available report status: • Assigned • Locked • New
Report Category	Category of the report

After creating a report, the administrator can assign it to a user.

The administrator can also assign reports to an application role (IT Role, Business Role) as permission-type entitlements. After selecting a report from the list, the **Assignment** pane automatically displays the entitlements already assigned to that report.

Clicking **Add**, the **Entitlements** panel that displays, showing the list of the available entitlements and allowing the RD administrator to perform a search and aggregate new entitlements to the report. Each search produces a list of results. The following table describes the assignable entitlement filters:

Table 348. Assignable Entitlement filters.

Filter	Description
Application	Application name: Entitlements filtered mainly according to the specified application.
Name	Name of the assignable entitlement: Matches with the application entitlements inventoried in the AG Core Module.
Type	Entitlement type: • IT Role • Business Role

Report search

Proceed as follows:

1. In the **Report** > **Entitlement** tab, click **Filter/Hide Filter**.
2. Set the Report filters and click **Search**.
3. The results are displayed in the same pane.

Assigned entitlements search

Proceed as follows:

1. Perform a **Report Search**.
2. Choose the desired report from the list of results.
3. The **Assignment** tab lists all entitlements associated to the selected report.

Assign entitlement to a report

Proceed as follows:

1. Perform a **Report Search**.

2. Choose the desired report from the list of results.
3. Click **Add**, in the **Entitlements** window that opens, set the filters and click **Search**.
4. Select the desired entitlement from the results list and click **Ok**.

The **Assignment** tab displays the assigned entitlement.

Remove assigned entitlements

Proceed as follows:

1. Perform an **Assigned Entitlements Search**, then select the entitlement to remove (use the [Ctrl] or [Shift] keys for multiple selections).
2. Click **Remove**.
3. Click **Ok** to confirm.
4. Click **Ok** in the window displaying the operation outcome.

Note: After removing an entitlement, all users having that entitlement will no longer be able to use the report associated to that entitlement.

Entitlement-Report tab

The **Entitlement** > **Report** tab (left) contains a list of entitlements and filters for the entitlement search.

The table below summarizes the available filters for the Entitlements search:

Table 349. Entitlement filters.

Filter	Description
Application	Application name: Entitlements filtered mainly according to the specified application.
Name	Name of the assignable entitlement: matches with the application entitlements inventoried in the AG Core Module.
Type	Entitlement type: • IT Role • Business Role

The same frame lists the results, according to the **Name** (Entitlement name) and **Application** (Application name) attributes.

After selecting an entitlement from the list, the **Assignment** tab displays the reports that are already assigned to that entitlement.

Clicking **Add**, the **Reports** window that opens, displaying the list of available reports and allowing the RD Administrator to perform a search and associate a new report to the entitlements. Each search produces a list of results. The following table describes the assignable reports filters:

Table 350. Assignable reports filters.

Filter	Description
Name	Name of the report.
Description	Brief description of the report.

Table 350. Assignable reports filters. (continued)

Filter	Description
Status	Available report status: • Assigned • Locked • New
Report Category	Category of the report.

Entitlement search

Proceed as follows:

1. In the **Entitlement** > **Report** tab (left), click **Filter/Hide Filter**.
2. Set the Entitlement filters and then click **Search**.
3. The results are displayed in the same frame.

Assigned report search

Proceed as follows:

1. Perform an **Entitlement search**.
2. Choose the desired entitlement from the list of results.
3. The **Assignment** tab lists all reports associated to the selected entitlement.

Assign report to an entitlement

Proceed as follows:

1. Perform a **Report Search**.
2. Choose the desired Report from the list of results.
3. Click **Add**, in the **Reports** window that opens, set the filters and click **Search**.
4. Select the desired report from the results list and click **Ok**.

The **Assignment** tab displays the assigned report.

Remove assigned report

Proceed as follows:

1. Perform an **Assigned Report search**, then select the report to remove (use the [Ctrl] or [Shift] keys for multiple selections).
2. Click **Remove**.
3. Click **Ok** to confirm.
4. Click **Ok** in the window displaying the operation outcome.

Menu

In this section, the RD administrator can categorize reports into folders.

The administrator can only add to a folder reports with a specific status (see Assigned Status).

The **Reports** tab lists the available reports. If the reports have the icon ✓ , it means that the report has already been added to a folder.

In the **Folder Menu** tab, the RD administrator can modify the folder hierarchy and the report position.

The administrator must create and add the first folder to the root folder. The administrator can then create and add new folders below the first.

The RD administrator can:

- Only add a report to a folder, not to its sub-folders.
- Only add a report to a single folder.
- Always place a report as a hierarchy leaf.

You can use the following filters to search specific reports:

Table 351. Report filters.

Filter	Description
Name	Name of the report
Description	Brief description of the report
Status	Available report status: • Assigned • Locked • New

The report search produces results based on the following attributes:

Table 352. Report attribute.

Attribute	Description
Name	Name of the report. An icon is present near the item name, depending on the type of item: • for a product item. • for a custom item.

Table 352. Report attribute. (continued)

Attribute	Description
Status	Available report status: • Assigned • Locked • New
Menu	✓ Report is associated to a folder.

The RD administrator needs to locate newly created folders to find easier a desired report.

From the **Folder Menu** tab, the administrator can locate a folder using the **Localize** button.

The administrator needs to categorize all reports of an entitlement.

After creating a folder, it will have the following label: [dir.34908187xxxxxxxxExx]; where:

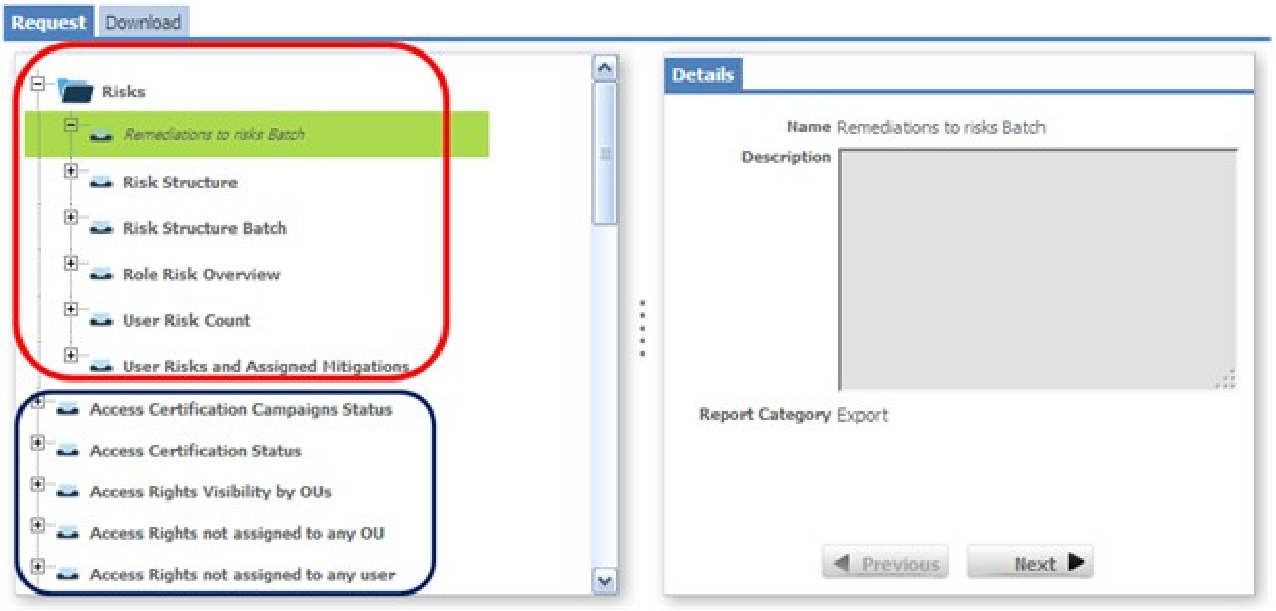
dir Is the directory.

code number
Is the number of directory.

The administrator could locate the folder with the name "Entitlement Reports." This feature is particularly useful when the data model elements do not have names easy to understand.

Note: The RD Administrator can select localization languages from the **Languages** button in the Edit Labels section.

When the administrator creates folders containing reports, the user requesting the reports will see the following:


Request
Download
Risks
Remediations to risks Batch
Risk Structure
Risk Structure Batch
Role Risk Overview
User Risk Count
User Risks and Assigned Mitigations
Access Certification Campaigns Status
Access Certification Status
Access Rights Visibility by OUs
Access Rights not assigned to any OU
Access Rights not assigned to any user
Details
Previous
Next

Name Remediations to risks Batch

Description

Report Category Export

Figure 132. Categorizing of reports into folders.

In the figure above:

- The blue rectangle contains reports that the user has requested, but because the reports are not in any folder yet, searching for a specific report is difficult.
- The red rectangle contains reports that the user has requested. In this case, though, the reports are in the **Risks** folder, which makes searching for a specific report much easier.

For example, to find reports regarding the User Risk Count, you can simply open the **Risks** folder and find easily the report "User Risk Count".

Report search

Proceed as follows:

1. In the **Reports** tab, click **Filter/Hide Filter**.
2. Set the Report filters and then click **Search**.
3. The results are displayed in the same pane.

Add directory (Create folder)

Proceed as follows:

1. From the **Folder Menu** tab, select the **Root** folder.
2. Click **Add dir**.

The new folder is automatically created and is associated to the Root folder.

After creating the first folder, the administrator can associate it to another folder, performing the same **Add dir** operation.

Locate folder

Proceed as follows:

1. Add a directory. Then, from the **Folder Menu** tab, select the desired folder.

2. In the same pane, click **Localize**.
3. In the window Localization that is displayed, enter the desired localization text.
4. Click **Ok** in the window showing the operation outcome.

Remove folder

Proceed as follows:

1. From the **Folder Menu** tab, select the desired folder.
2. In the same pane, click **Remove**.
3. In the Warning window that is displayed, click **Ok** to confirm the operation and close the window.

Note:

The RD administrator can only remove folders that do not contain nested directories.

If the administrator wants to remove a folder with nested directories, the nested directories must be deleted first.

Add report to a folder

Proceed as follows:

1. Perform a **Report Search**.
2. From the **Reports** tab, select the desired reports.
3. In the **Folder Menu** tab, select the target folder, then, in the **Reports** tab, click **Add**.

This automatically associates the report to the target folder.

Remove report from a folder

Proceed as follows:

1. From the **Folder Menu** tab, click on the desired folder to display the reports added to the folder.
2. Choose the report to remove, and click **Remove**.
3. Click **Ok** in the Warning window to confirm the operation.

This automatically removes the report from the folder.

Settings

The following functions are available for setting values of some elements of the module:

- Edit Labels
- System Entities
- Scopes
- “Custom filters” on page 634

Note:

Only an experienced administrator can perform the operations available in this section of the RD module.

Inappropriate changes to any configuration in this section can degrade the performance of the report designer module.

Edit labels tab

In this section, the RD administrator can associate a specific localization code to the messages available for all languages.

In the **Localization codes** tab, the localization codes registered by the system are listed.

The RD administrator can use the following filters to search for the localization codes:

Table 353. Localization Code filters.

Filter	Description
Code	Name of the localization code.
Message	Text contained in the "message" section.
Language	Localization code language.
No Localization	When selecting this check box, you can search for localization codes which is not localized.

In the right pane, there are some tabs that correspond to the languages available. When a localization code on the right is selected, the first tab that opens, represents the default language sets.

By default, the language tabs always display the **Code** and **Localized message** fields.

In the right pane, clicking **Languages** opens a window and allows the administrator to modify the default language used to load the label groups associated with the different application objects.

The Languages in use (Browser) text box displays the language that is currently set for the browser. The Default Language text box displays the language that is currently set.

To modify the language, proceed as follows:

1. Click **Change** near the Default Language text box.
2. Select one of the languages from the **Default Language** window that displays.
3. Click **Ok** to confirm the selected default language.

To add languages in the list of available languages (from right to left), proceed as follows:

1. Select the desired language from the available languages list box on the right.
2. Click ◀ **Add to Table on Left** to move the selected language into the languages in use list box on the left.

To remove a language from the list of languages in use (from left to right), proceed as follows:

1. Select the desired language from the languages in use list box on the left.
2. Click ▶ **Remove Languages** to move the selected language into the available languages list on the right.

Every operation described in this section is automatically saved.

Note:

Languages found in the Languages in Use list box match with those available in the Localization phase.

The settings described in this section are not related to the language settings of the browser.

The browser language settings affect the labels on the tab bar only.

To edit a localized message, proceed as follows:
1. In the **Localization codes** tab, select the desired code.
2. The tab on the right displays the **Code Name** and **Localized Message** in the default language chosen in the Language in Use window.
3. In the same pane, modify the localized message.
4. Click **Save**.

System entities

In this section, the RD administrator can manage the system entity keys used to write the query.

The RD administrator can use the following filters to search for entity keys (clicking **Filter**/**Hide Filter**):

Table 354. Entity Key Filters.

Filter	Description
Name	Name of the entity key.
Reference Entity	This field is fixed and cannot be modified. System is the only reference entity.

The table below describes the four message localization attributes in the **Entity Key Details** tab:

Table 355. Entity Key Details.

Attribute	Description
Reference Entity	System is the only reference entity.
Name	Name of the entity key.
Value	Name of one of the available realms to be deployed.
Description	Brief description of the entity key.

Edit entity keys

Proceed as follows:

1. In the **Entity Keys list** tab, select the desired key. The **Entity Key details** tab displays details of the selected entity key.
2. In the same tab, modify the entity key details.
3. Click **Save**.

Add an entity key

Proceed as follows:

1. In the **Entity Keys list** tab, click **Add**.
2. In the **Entity Key details** tab, insert the **Localized Message** details.
3. Click **Save**.

Remove an entity key

Proceed as follows:

1. In the **Entity Key list** tab, select the entity key to remove.
2. In the same pane, click **Remove**.
3. Click **Ok** to confirm the operation.

Scope

In this section, the RD administrator can create scopes.

The **Scope List** tab, contains scopes that the RD administrator can associate to queries.

The administrator can also perform scope searches using the filters **Name** and **Description** (click **Filter/Hide Filter**).

The same frame lists the results according to the following attributes:

Table 356. Scope search attributes.

Attribute	Description
Name	Scope name. An icon is present near the item name, depending on the type of item: • for a product item. • for a custom item.
Description	Brief scope description (maximum 256 characters).
Entity	Scope entity: • **Application** • **Entitlement** • **Org_Unit** • **PwdCfg** • **Resource** • **System** • **Task** • **User**

In the **Scope Details** tab, the RD Administrator can create the desired scope according to the following attributes:

Table 357. Scope Details

Detail	Description
Name	Scope name.
Description	Brief scope description (maximum 256 characters).
SQL Query	Query text.
Reference Entity	Scope entity: • **Application** • **Entitlement** • **Org_Unit** • **PwdCfg** • **Resource** • **System** • **Task** • **User**

Scope search

Proceed as follows:

1. In the **Scope List** tab, click **Filter/Hide Filter**.
2. Set the filter data (**Name**, **Description**), then click **Search**. The results are displayed in the same pane.

Create scope

Proceed as follows:

1. Perform the scope search.
2. In the **Scope List** tab, click **Actions > Add**.
3. In the **Scope Details** tab, set the scope attributes.
4. Click **Save** to save the scope and add it in the **Scope List** tab.

For help about the query processing, click **Help** in the **Scope Details** tab.

Modify scope

Proceed as follows:

1. Perform the scope search and select the scope to modify.
2. In the **Scope Details** tab, modify the scope.
3. Click **Save**.

Remove scope

Proceed as follows:

1. Perform the scope search.
2. In the **Scope List** tab, select the desired scope and click **Remove**.
3. A Warning window displays a message about the effects of the operation.

4. Click **Ok** to confirm the operation.

Note:

Removing a scope results in the loss of its visibility configuration. The tmp table is still part of the query but contains no data.

After removing a scope from the selected query, all aggregations with any other query are lost.

Custom filters

In this section, the RD administrator can customize filters.

The **Custom Filters** tab, contains the list of available custom filters that the RD administrator can associate to the report.

The administrator can also perform a custom filter search using the **Name** (filter name) and the **Description** (brief filter description) filters by clicking **Filter/Hide Filter**.

The same pane lists the results according to the following attributes:

Table 358. Custom Filter Attributes.

Name	Description
Name	Scope name. An icon is present near the item name, depending on the type of item: • ▣ for a product item. • 🖥 for a custom item.
Description	Brief scope description (maximum 256 characters).

In the **Filter details** tab, the RD Administrator can create the desired filters according to the following attributes:

Table 359. Filter details.

Name	Description
Name	Scope name.
Description	Brief scope description (maximum 256 characters).
SQL Query	Query text.

Create custom filters

Proceed as follows:

1. In the **Custom Filters** tab, click **Add**.
2. In the **Filter details** tab, set the filter detail attributes.
3. Click **Save** to save the filters in the **Custom Filters** tab.

For help about query processing, click Help in the same pane.

Modify custom filters

Proceed as follows:

1. In the **Custom Filters** tab, select the custom filter to modify.
2. In the **Filter details** tab, modify the filter detail attributes.
3. Click **Save**.

Remove custom filters

Proceed as follows:

1. In the **Custom Filters** tab, select the custom filter to remove.
2. Click **Remove**.
3. Click **Ok** to confirm the operation.

Note: The RD administrator cannot remove the product 🟩 custom filters.

Monitor

The functions that are available for monitoring some elements are contained in the following list.

Report queue

After the report is run, the RD administrator can check the report status and the report download.

The table below lists the different report execution statuses:

Table 360. Report execution statuses.

Execution status	Description
Pending	Report execution is pending.
Running	Report is in execution.
Download	Report is ready to be downloaded.
Error	Error during the report execution.

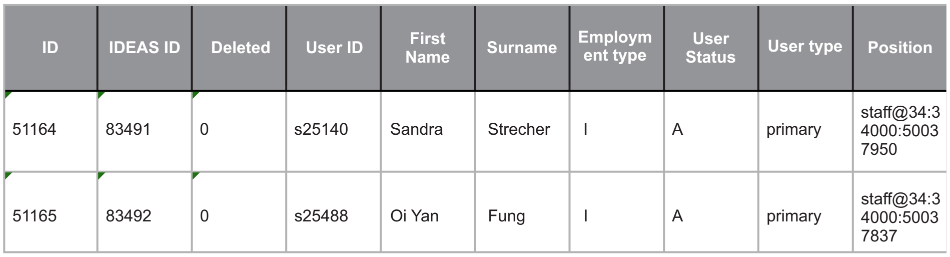
The **Report Property** pane (bottom) displays properties of the report, as described in the table below:

Table 361. Report properties.

Properties	Description
Name	Name of the key: • Report name • Application • Language • File format • User ID
Description	Description of the key.
Value	Value of the key.

Note: A Report with Download status is available for download until it is deleted.

The following figure shows a sample report in **XLSX** format (User imported report) :



ID	IDEAS ID	Deleted	User ID	First Name	Surname	Employment type	User Status	User type	Position
51164	83491	0	s25140	Sandra	Strecher	I	A	primary	staff@34:34000:50037950
51165	83492	0	s25488	Oi Yan	Fung	I	A	primary	staff@34:34000:50037837

Figure 133. Report sample: User removal.

Chapter 28. Introduction to Task Planner

Task Planner (TP) module is a scheduler that helps you manage asynchronous processes that can be performed at a future time.

An example of these types of processes is the production of a set of reports.

These processes usually involve massive interrogations of one or more databases and might require a relatively long time. They are therefore preferably run at night when the system is not used for ordinary operations.

The IBM Security Identity Governance and Intelligence Task Planner is based on the job concept. A job describes an executable function, such as a massive database update, and is distinguished by the following triad:

- Name
- Java class
- Set of parameters

A single-job-based approach does not usually allow for execution of complex functions. In some cases, it might be convenient to have a load-balancing mechanism to allocate parts of the processing operation to other machines.

The IBM Security Identity Governance and Intelligence Task Planner effectively provides for the following requirements:

- Simple single-job writing capabilities.
- Ability to describe even the most complex relations between different jobs.
- Transparency and flexibility in time-limited job scheduling.
- Load-balancing in the system running a job set.

Architecture and components

This section describes the main task planner components.

The IBM Security Identity Governance task planner consists of four components:

- Hibernate framework
- Scheduler engine
- EJB layer
- Application

Hibernate framework

Hibernate is an ORM (Object Relational Mapping) framework that manages information persistence in the database. ORM is a group of management methods and techniques that integrate an object-oriented paradigm into the relational paradigm of a relational database management system (RDBMS). The objective of ORM is to program the relational database interaction using a purely object-oriented paradigm, concealing a relational paradigm translation from the developer. For more information on Hibernate, see: http://www.hibernate.org

Scheduler engine

The scheduler engine is the core component of the system; it hosts the task planner basic framework, based on the Quartz library. This layer mainly provides all the internal services used by the EJB layer. Quartz is a full-featured, Open Source Job scheduling system that can be integrated with or used with any J2EE or J2SE application. From the smallest stand alone application to the largest system.

Quartz can be used to create simple or complex schedules, executing up to tens of thousands of jobs. The Quartz Scheduler includes many enterprise-class features, such as JTA transactions and clustering. For more information on Quartz, see: http://quartz-scheduler.org/

IBM Security Identity Governance Task Planner is perfectly compliant with Quartz Jobs. Default jobs (bundled with the IBM Security Identity Governance platform) as well as custom jobs can therefore be used with the Quartz interface.

EJB layer

The EJB layer hosts the task planner module basic components: job classes, jobs and tasks.

Application

This layer is mainly composed of a:

- Front end Administration Module (entirely documented in this manual).
- Back end IBM Security Identity Governance jobs set, which provides the task planner common functions based on the EJB layer.

Use the product jobs for managing the IBM Security Identity Governance platform common activities.

You can define third-party jobs.

Guide to task modeling

The IBM Security Identity Governance task planner distinguishes among three main concepts: job class, job and task.

The job class is a single unit of code (generally a Java class method) that must be run. Every operation executed by the scheduler must implement the job interface and the associated execute method, according to the Quartz library guidelines.

Each individual job can be defined by a set of job class parameters needed to perform that job. Therefore, every job is characterized by a set of job class attributes.

A task can be composed of a single job or a set of jobs.

The task structure

The task is the main unit managed by the IBM Security Identity Governance task planner.

A task can be built on:

- A single job (a tree with a single node).
- A list of jobs (a tree with a single level of nodes).
- A tree-hierarchy of jobs.

Running a task composed of a single job means running that job.

If a task is composed of a list of jobs, the task starts running when the first job in the list begins, and ends when the last job in the list terminates.

If a task is composed of a tree of jobs, it proceeds by running any job in the hierarchy according to the predefined order.

Generally, the execution of a child node begins when the execution of the parent node ends. After the jobs are added to a task, their execution type needs to be defined, for example the job behavior.

You can choose between the following:
- Start if parent OK: Job starts if parent completed successfully.
- Start if parent KO: Job starts if parent failed.

Task status

Three different status characterize a task:
- **Start** (Active)
- **Inconsistent**
- **Stop** (Inactive)

Start (Active) status

If the task is running (for example, the task is active), the associated jobs are enqueued and will be run according to the task time planning attributes. The set of jobs associated with a task can be structured as follows:
- A single job.
- A list of jobs.
- A hierarchy of jobs.

The time planning attributes are applied to the first job of the task.

If the first job is structured as a job list, the time planning attributes are associated with the first job of the list. The other jobs are subsequently scheduled as indicated in the list.

For example, Job K begins running only after Job K-1 has finished.

If the task is structured as a composite set of Jobs, executing any level of nodes depends on the execution type of the parent job.

Inconsistent status

A task is characterized as ! inconsistent when a misalignment between the task planner module and the scheduler engine occurs. This misalignment might be caused by unpredictable external problems. A task can be restored to its original condition using the synchronization process, which synchronizes all tasks aggregated to a scheduler.

It primarily reactivates tasks that were ✓ active before the misalignment, where no action is taken for the tasks that were ✗ inactive.

Stop (Inactive) status

After entering the stop state, a scheduler will try to stop all currently running jobs. Any job queued after that time will be discarded. Other jobs cannot be queued until the scheduler reenters the Start state.

How to implement a new job

This section provides the basic elements needed to understand how to implement and deploy a new job.

Any job to be used in the IBM Security Identity Governance task planner must be structured according to the Quartz guidelines (http://quartz-scheduler.org/).

General job structure

The following example shows the general structure of a job:

```
public class Test extends ACrossJob {

@Override

public List<WorkPropBean> getInitPropertyList() {

// TODO Auto-generated method stub

return null;

}

@Override

public boolean execute(Properties workProperties, StopProcess stopObject) throws Exception {

// TODO Auto-generated method stub

return false;

}

@Override

public void interrupt() throws Exception {

// TODO Auto-generated method stub

}
}
```

Parameters list of a job

Job parameters can be specified through the method List<WorkPropBean> getInitPropertyList():

```
public List<WorkPropBean> getInitPropertyList() {

List<WorkPropBean> result = new ArrayList<WorkPropBean>();

WorkPropBean message = new WorkPropBean();

message.setType(WorkPropType.STRING.getValue());

message.setRequired(false);

message.setName("Message");

message.setValue("Hello World!");

message.setDescription("System out message");

result.add(message);

WorkPropBean exception = new WorkPropBean();

exception.setType(WorkPropType.INT.getValue());

exception.setRequired(false);

exception.setName("Exception");

exception.setValue("0");

exception.setDescription("set value 1 if you want an exception ");

result.add(exception);

WorkPropBean wait = new WorkPropBean();

wait.setType(WorkPropType.INT.getValue());

wait.setRequired(false);

wait.setName("Wait");

wait.setValue("0");

wait.setDescription("Time wait before continue");

result.add(wait);

return result;

}
```

Parameters specified here are configured using the Task Planner web interface.

Three parameters are specified in this example: message, exception and wait.

Five elements of information must be specified for every parameter:

- Type (setType)
- Specifies if the parameter is mandatory (setRequired, where the value *false* means that it is not mandatory to set this parameter and a default value is provided)
- Name (setName)
- Value (setValue)
- Description (setDescription).

Managing job execution

Job execution is managed using the method public boolean **execute (Properties** inputParameters **,** StopProcess stopProcess):

```
public boolean execute(Properties inputParameters, StopProcess stopProcess)
throws Exception {

Integer wait = (Integer) inputParameters.get("Wait");

if (wait != null && wait > 0) {

try {

Thread.sleep(wait);

} catch (InterruptedException e) {

e.printStackTrace();

}

}

// you can use this mode to check if the process is stopped:

stopProcess.throwExceptionifStopped();

// or this other one:

if (!run) {

throw new Exception("Interrupted Process!!!");

}

Integer ex = (Integer) inputParameters.get("Exception");

if (ex == null || ex == 0) {

System.out.println("[SystemOUTJob] message: " + inputParameters.get("Message"));
} else {

throw new Exception("Test exception");

}

return false;

}
```

The parameters indicated in getInitPropertyList () are provided with inputParameters.

The stopProcess parameter takes care of terminating execution.

If the return value is true , the job is automatically restarted after the current execution terminates. This behavior might be useful when you need to loop a job, but this requires a dedicated subset of code lines to manage the job behavior.

If the return value is false, the job is terminated.

Job interruption

In order for the Task Planner to interrupt a job execution, the method public void interrupt () must be used:

```
boolean run = true;

public void interrupt() throws Exception {

// You can use StopProcess Object in the execute method instead of this...

run = false;

}
```

A set of code lines can be specified in the body of the method to manage interruptions.

How to deploy the new job

When the new job is ready, it takes the form of a JAR named `MyCustomJob.jar`.

To deploy this new job, perform the following steps using the Task Planner web interface:

1. Stop the Application Server
2. Save `MyCustomJob.jar` in the directory:
   ```
   /opt/IBM Security Identity Governance/jboss-6.1.0.Final/IBM Security
   Identity GovernancePlatformEnvCustom/lib
   ```
3. Start the Application Server

How to configure the new job

After the deployment, use the Task Planner web interface to:

- Add the new job class and define the job parameters.

- Build a task using the newly added job.
- Schedule the task.

Manage

The following functions for managing the main entities of this module are available:

- Jobs
- Tasks

Jobs

In this section, the administrator can add jobs and configure job class attributes.

The **Jobs** tab displays the jobs listed in the system. You can search for specific jobs using the filters described below (click **Filter/Hide Filter** and click **Search**):

Table 362. Job filters.

Filter	Description
Name	Name of the job.
Job classes	Name of the job class.
Context	Task group.

The job pane lists the results according to the following attributes:

Table 363. Job attributes.

Attribute	Description
Used	Job status: ✓ : Job assigned to one or more tasks ✗: Job not assigned to any task
Name	Name of the job.
Job classes	Name of the job class.

In the **Actions** menu, all available buttons for managing jobs are listed below:

- **Add**: Allows you to add a job.
- **Remove**: Allows you to delete a job.

The contents of the right pane changes depending on the tab selected in the upper side of the pane. The **Details** tab is active by default:

Table 364. Job details.

Detail	Description
Name	Name of the job.
Job class	Name of the job class .
Context	Task group.
Description	Brief job description (maximum 256 characters).

Note: For a **Used Job**(✓) the Remove button is disabled. To remove it, the job must first be removed from all tasks. A Used Job cannot be modified unless it is first removed from all tasks.

In the **Details** tab, you can edit a job and configure the following job class parameters:

Table 365. Job class parameters.

Parameter	Description
Mandatory	This field is distinguished by: ✓ : a parameter value is mandatory. ✗ : a parameter value is not mandatory.
Name	Name of the job class attribute.
Type	Type of the job class attribute.
Value	Value of the job class attribute.
Mode	Status of the value: • Modifiable : Value modifiable in tab **Manage** > **Task** > **Jobs**. • Not Modifiable : Value not modifiable.
Description	Brief name/value description (maximum 256 characters).

The list below shows the main job-related operations:

- Tasks
- History

Tasks

From the **Jobs** web interface, select a ✓ Used Job and click on the **Task** tab to view the task associated to the job. The following filters are used to perform a task search (click **Filter**/**Hide Filter**):

Table 366. Task filters.

Filter	Description
Name	Name of the task.
Context	Task groups.
Scheduler	Scheduler that executes the task.

Select the desired task and, from the **Actions** menu, click **Task**. This enables the **Manage** > **Tasks** tab. The desired task can be quickly configured.

History

From the **Jobs** web interface, select a ✓ Used Job and click on the **History** tab to view the scheduling results of a job assigned to a specific type of task. This is only possible for the ✓ Active Task , whose scheduling has already begun and ended. The following filters are used to perform a task search (click **Filter/Hide Filter**):

Table 367. History filters.

Filter	Description
Scheduler	Scheduler that executes the task.
Task	Scheduled task.
Start date from	Start date of the task from a specific date.
Start date to	Start date of the task to a specific date.
Results	Tasks results: • Completed: search only successfully completed tasks. • Error: search only tasks that have generated errors.

In the **Actions** menu, all available buttons for managing the jobs history are listed below:

- **Task**: allows you to go to the **Manage** > **Tasks** tab quickly.
- **Remove**: allows you to remove one or more history results.
- **Clear All**: allows you to clear all history results.

From the **Actions** menu, clicking **Task** enables the **Manage** > **Tasks** tab.

Task Planner: jobs, parameters, and schedules

In the Task Planner module, the administrator can manage the configuration of tasks, or a list of jobs to be executed, by creating and configuring them, defining job class parameters, and configuring scheduling.

Note: The Task Planner module is configured out of the box. If you edit this configuration, live operations might be delayed.

The following sections cover:

- Task searches
- Task actions
- Task details
- Task-oriented operations, which include the following topics:
  - **Jobs**
  - **Scheduling**
  - **History**

Task searches

The administrator can manage tasks. You can search specific tasks by clicking **Filter/Hide Filter** and by clicking **Search**. The following table lists the filters that help you refine the search.

Table 368. Task filters

Filter	Description
Name	Search for tasks by their names. You can use wildcards to modify the search criteria. For more information about wildcards, see Chapter 3, "Identity Governance and Intelligence modules," on page 55.
Context	Define task groups.
Scheduler	Specify how many and which tasks are performed by the scheduler.

The **Task** search tab lists results according to the following attributes:

Table 369. Task attributes

Attribute	Description
Active	The following icons represent the various task statuses: ✓ **Active task** ✗ **Inactive Task** ! **Inconsistent Task**
Name	Search for tasks by their names. You can use wildcards to modify the search criteria. For more information about wildcards, see Chapter 3, "Identity Governance and Intelligence modules," on page 55.
Context	Define the task group.
Scheduler	Specify how many and which tasks are performed by the scheduler.

Task Actions

You can complete the following tasks that are related to task management from the **Actions** menu:

Monitor

Monitors the selected task scheduling for ✓ **Active Tasks**. Each time a job is performed, an entry in monitoring is written giving information on the dates and status. An entry will be created even if an error occurs during the execution. Enable monitoring by enabling the history. Specify the following fields:

- **Final Fire Date**
- **Previous Fire Date**
- **End Date**
- **Status**
- **Start Date**
- **Next Fire Date**

Start/Stop

Starts or stops a task. After IBM Security Identity Governance and Intelligence is configured, preconfigured tasks are active.

Add Create a new task instance:

1. Log into the IBM Security Identity Governance and Intelligence virtual appliance or the local management interface.
2. Select **Administration Console**, and authenticate.
3. Click **Task Planner**
4. Click **Manage**.
5. Under the **Task** tab, select **Actions** > **Add**.
6. Specify the details of the task beneath the **Details** tab.
7. Specify additional settings in the **Jobs** and **Scheduling** tabs.
8. Save the task upon completion.

Note: When you add a task, you must specify the **Name** and **Scheduler** fields.

Remove

Deletes ✗ **Inactive Task**.

Task details

In the **Details** tab, you can edit the following task details:

Table 370. Task details

Detail	Description
Name	Name the task.
Scheduler	Specify how many and which tasks are performed by the scheduler.
Context	Define the task groups.
Enable history	If this check box is selected, the scheduling history is available.
Description	Define a task description.

Note:

For an ✓ **Active Task**, the **Remove** button is disabled. To remove it, the task must first be stopped.

An ✓ **Active Task** cannot be partially modified unless it is first stopped. After you stop the task, you can modify the following details:

- Name
- Context
- Description

Jobs

In the **Task** web interface, select a task and click the **Jobs** tab to view the task structure and the job components.

You can modify a task that is already built by selecting one of the items in the **Actions** menu:

Move Up
Moves a job up in the list.

Move Down
Moves a job down in the list.

Note: The jobs are processed in the order that they appear in the hierarchy.

Add Adds a new job to the list and associates it with a task:

Remove
Removes a job.

All of the following operations are only available for the ✗ **Inactive Tasks**.

After you configure the task, you can define the **Job class** attribute values for any job associated with the task.

1. Select a job from the tree structure.
2. In the adjoining pane, specify the following attributes:

Table 371. Job attributes

Attribute	Description
Name	Name the task.
Job class	Specify the job class.
Identifier	Specify the job identifier.
Execution type	In this field, select the job behavior: **Start if parent OK** Job starts if the parent completed successfully. **Start if parent KO** Job starts if the parent failed. These selections are also available for all child nodes.

3. Edit a set of parameters from the following table for any job class:

Table 372. Job class parameters

Parameter	Description
Mandatory	✓ You must define a parameter value. ✗ You do not have to define a parameter value.
Name	Name the job class attribute.
Type	Choose a format of the job class attribute: • Long • String
Value	Define the value of the job class attribute.
Description	Provide a brief name or value description.

Editing the `cacheTimeMinute` parameter

The platform configuration sets the `cacheTimeMinute` parameter of the **SystemRuleEngine** job to `120` as a default value. If you set the value to `0`, no cache exits. When you set the platform to production, you can ensure that the Rule Engine runs more efficiently by setting high values for the `cacheTimeMinute` parameter:

1. Select **Manage** > **Tasks**.
2. In the **Task** tab, select the Rule Engine item.
3. Select the **Jobs** tab and double-click **SystemRuleEngine** job.
4. Set the `cacheTimeMinute` to a value that is greater than 0. A value of 600 minutes is recommended.

Note:

Increasing the value of the `cacheTimeMinute` parameter increases the number of minutes the rules will be retained before they are refreshed. When you create or change a rule, remember to wait for the entire specified duration of the `cacheTimeMinute` parameter to ensure that the rule will be saved.

Scheduling

In the **Task** web interface, select a task, and click the **Scheduling** tab to view the task scheduling. Two options are available:

- Simple Execution
- Advanced Execution

Note: When you try to modify the scheduling of an ✓ **Active Task**, a warning message displays: `The Scheduling of an active Task cannot be modified`.

Table 373. Simple Execution attributes

Attribute	Description
Scheduling	**Recurring** If this check box is selected, the task is run recursively. **Iterations** If the check box **Recurring** is selected, this text area is disabled. If the check box **Recurring** is not selected, you can define the number of repetitions. **Frequency** Use this option to specify how often you want to run the task.

Table 373. Simple Execution attributes (continued)

Attribute	Description
Start Date and Time	**Date** Use this option to specify the date in the *dd/mm/yyyy* format on which you want the task to run. **Hours and Minutes** Use this option to specify the desired duration of the task execution in the *hh:mm* format.

Table 374. Advanced Execution attributes

Attribute	Description
Scheduling	**Recurring** If this check box is selected, the task is run recursively. **Iterations** If the **Recurring** check box is selected, this text area is disabled. If the **Recurring** check box is not selected, you can define the number of repetitions. **At the hour** Set the hour when the task executes. **At the minute** Set the minute when the task executes.
Calendar scheme	**Week days** Select this button to specify the day of the week on which you want the task to start. **Month days** Select this button to specify the day of the month on which you want the task to start. You have the following options: • You can choose specific days for the task to run during the month or on the last day of the month.. • **Clear All** clears the choices, and the task never runs. • **Select All** runs the task every day. • **Last day of the month** runs the task on the last day of the month.

Table 374. Advanced Execution attributes (continued)

Attribute	Description
Start Date and Time	**Date** Use this option to specify the future task execution date in the *dd/mm/yyyy* format on which you want the task to run. **Hours and Minutes** Use this option to specify the desired duration of the future task execution in the *hh:mm* format.

History

You can view the results of the task scheduling for an ✓ active task for which the scheduling is terminated:

1. Navigate to the **Task** web interface.
2. Select a task.
3. Select the **History** tab.
4. Toggle **Filter/Hide Filter** to display the following filters to perform a task search:

Table 375. History filters

Filter	Description
Job	Specify the name of the job. Click ⋯ **Search Jobs** to choose a specific job.
Start date from	Specify the start date of the task from a specific date.
Start date to	Specify the start date of the task to a specific date.
Results	Task results include the following options: • **Completed**: Search successfully completed tasks only. • **Error**: Search the tasks that only generated errors.

The following table summarizes the attributes of the task results:

Table 376. Task attributes

Attribute	Description
Name	Name the task.
Scheduler	Specify the scheduler type.
Start Date and Time	Choose a scheduling start date.
Elapsed Time	Specify the duration of the scheduling (starting from **Start Date and Time**).
Message	This field is populated only when an error message displays.
Instance	This indicates the name of the host that performs the job available when an error occurs.

5. From the **Actions** menu, manage the jobs history with the following buttons:
   - **Job** takes you to the **Manage** > **Jobs** tab.
   - **Clear All** clears all history results.
   - **Remove** deletes one or more history results.
6. In the **History** tab, click **Jobs** to enable **Manage** > **Jobs**. See “Jobs” on page 644.

Monitor

This section displays all task histories.

The **History** search tab displays all tasks listed in the system. You can search for a specific task using the filters displayed below by clicking **Filter** /**Hide Filter**:

Table 377. History filters.

Name	Description
Scheduler	Search by scheduler name.
Task	Search by task name.
Job	Search by job name.
Start date from	Start date of the task from a specific date.
Start date to	Start date of the task to a specific date.
Results	Tasks results: • Completed: search successfully completed tasks only. • Error: search tasks that have generated errors only.

In the **Actions** menu, all available buttons for managing jobs are listed below:

- **Job<**: allows you to go to **Manage>Jobs** tab quickly.
- **Task<**: allows you to go to **Manage>Tasks** tab quickly.
- **Clear All**: allows you to clear all history results.
- **Remove**: allows you to remove one or more history results.

In the same tab, selecting a 📁 **Task**:

- Enables the >**Task** button in the **Actions** menu. Click it to enable the **Manage** > **Tasks** tab.
- Opens the task tree-structure, displaying the associated 📁 / 📁 jobs. Selecting a specific job enables the >**Job** button, in the **Actions** menu, which enables the **Manage** > **Jobs** tab.

Settings

The following functions are available for setting values of some elements of the module:

- Scheduler
- Context

Scheduler

In this section, the administrator can view the scheduler details and perform a scheduler synchronization.

The **Scheduler** search tab displays all schedulers listed in the system.

You can use the **Name** filter to perform a scheduler search by clicking **Filter/Hide Filter**.

In the **Actions** menu, all available buttons for managing jobs are described below:

- **Task**: allows you to go to the **Manage** > **Task** tab quickly.
- **Synchr.**: allows you to synchronize all tasks to the selected scheduler.

In the same tab, selecting a scheduler:

- Enables the **Task** button in the **Actions** menu. Click it to enable the **Manage** > **Tasks** tab and view the task associated to the selected scheduler.
- Enables the **Synchr.** button in the **Actions** menu. Click it for synchronizing all tasks associated to the selected scheduler.

The **Synchr.** button primarily reactivates tasks that were ✓ active before the misalignment. No action is taken for tasks that were ✗ inactive.

Synchronization reactivates ! inconsistent tasks. Only active tasks can become inconsistent.

The **Details** tab shows information (**Name** and **Description**) about the selected scheduler. The five available schedulers are described in the table below:

Table 378. Scheduler Set.

Name	Description
System	This scheduler contains all system tasks critical to core system operations. This scheduler should be stopped only if strictly necessary.
Reports	This scheduler is intended to run the report task only. This task might be critical, affecting overall system performance. Reports can be launched without the possibility for checking the amount of data to be involved.
Connectors	This scheduler is intended to run connector tasks only. Connector tasks poll the connector worktable to find work items to be executed. Single connectors are scheduled in the connector configuration.
Singleton	This scheduler is intended to use one thread only. Use this scheduler for tasks to be run sequentially only.
Custom tables	This scheduler runs custom tasks that are developed to address very specific customer needs. Custom tasks are not controlled tasks and can therefore impact system performance.

The **Details** tab also displays the scheduler attributes. Information fields for each attribute are described in the table below:

Table 379. Scheduler attributes.

Name	Description
Name	Name of the scheduler attribute

Table 379. Scheduler attributes. (continued)

Name	Description
Value	Attribute value
Description	Brief attribute description

The **History** tab displays the history of the selected scheduler.

The following filters are used to perform a task search by clicking **Filter/Hide Filter**:

Table 380. History filters.

Filter	Description
Task	Name of the task. Click ... Search Tasks to choose a specific task.
Job	Name of the job. Click ... Search Jobs to choose a specific job.
Start date from	Start date of the task from a specific date.
Start date to	Start date of the task to a specific date.
Results	Task results: • Completed: search successfully completed tasks only. • Error: search tasks that have generated errors only.

In the **Actions** menu, all available buttons for managing the history results are described below:

- >**Job**: allows you to go to the **Manage** > **Jobs** tab quickly.
- >**Task**: allows you to go to the **Manage** > **Tasks** tab quickly.
- **Remove**: allows you to remove one or more history results.
- **Clear All**: allows you to clear all history results.

From the **Actions** menu:

- By selecting a task, the >**Task** button is enabled. Click it to enable the **Manage** > **Tasks** tab and view the task associated to the selected scheduler.
- By selecting a job, the >**Job** button is enabled. Click it to enable the **Manage** > **Jobs** tab and view the job associated to the selected task.

Context

You can group tasks under a certain context.

This feature is useful when data model elements do not have names easy to understand.

The **Context search** tab displays all contexts that are listed in the system. You can search specific context by clicking **Filter/Hide Filter**.

Through **Actions** menu, you can:

- **Show Task** to go to the **Manage** > **Tasks** tab quickly and view the tasks that are associated to the selected context.
- **Add** adds a context.

- **Remove** removes a context. All tasks that are associated to a removed context are available in the system again but are no longer grouped under that context.

In **Context Details** tab, you can modify the **Name** and **Description** of a context.

Chapter 29. Request

The Reports frame on the left contains the assigned reports.

The Report Designer (RD) administrator can classify the available reports into a hierarchy of folders, labeled with specific names. Every folder can contain a specific set of reports (leaves of the hierarchy) or other folders.

For each folder, it is possible to repeat recursively this structure..

When the authorized user plans a report, they can configure some settings, organized into a Wizard composed of several steps. The available settings are provided according to the design outlined by the Administrator of the RD Module.

After the Report is configured, as the last step of the Wizard, click the **Execute** button. A complete overview of the configuration actions is shown below.

How to configure a report

The configuration of a report is managed through an interactive utility that guides users through a multi-step process.

In every step it is possible to configure a specific Tab, dedicated to a limited subset of information.

The Administrator can easily go back and forward through the sequence of steps of the wizard.

The sequence of steps of the configuration is shown in the table below:

Table 381. Configuration steps.

Step (tab)	Description	Always/Optional
Details	Shows the description of the Report (read only).	Always present
Users	Lets you choose which Users will be considered in the Report generation.	Optional
Application	Lets you choose which Application will be considered in the Report generation.	Optional
Entitlements	Lets you choose which Entitlements will be considered in the Report generation.	Optional
Organization Units	Lets you choose which Organization Units will be considered in the Report generation.	Optional
Activities	Lets you choose which Activities will be considered in the Report generation.	Optional

Table 381. Configuration steps. (continued)

Step (tab)	Description	Always/Optional
Configurations	Lets you choose which type of Account Configurations will be considered in the Report generation.	Optional
Filters	Lets you specify which type of Filters will be used for the Report generation.	Always present
Processing Policy	Lets you specify the scheduling parameters for the Report run.	Always present

Details tab

The **Details** tab is the first tab present in all reports.

The tab includes the following data:
- **Name**: the name of the report
- **Code**: univocal identifier of the report
- **Description**: brief read-only description of the report
- **Report Category**: indication of the report classification group

Visibility – Users tab

In this tab you can select the users that will be involved in the report.

The complete list of available users can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the user (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more users from the set shown in this last tab, you can be select them and click the **Actions** > **Remove** button.

When the configuration activity in this tab is finished, click the **Next** button.

Visibility – Applications tab

In this tab you can select the applications that will be involved in the report.

The complete list of available applications can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the application (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the Report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more applications from the set shown in this last tab, select them and click the button.

When the configuration activity in this tab is finished, click the **Next** button.

Visibility – Entitlements tab

In this tab you can select the entitlements that will be involved in the report.

The complete list of available entitlements can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the Entitlement (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the Report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more entitlements from the set shown in this last tab, select them and click the **Actions** > **Remove** button.

When the configuration activity in this Tab is finished, click on **Next** button.

Visibility – Organization Units tab

In this tab you can select the organization units that will be involved in the report.

The complete list of available organization units can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the OU (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the Report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more organization units from the set shown in this last tab, select them and click the **Actions** > **Remove**button.

When the configuration activity in this Tab is finished, click the **Next** button.

Visibility – Activities tab

In this tab you can select the activities that will be involved in the report.

The complete list of available activities can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the activity (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more activities from the set shown in this last tab, select them and click the button.

When the configuration activity in this tab is finished, click the **Next** button.

Visibility – Configurations tab

In this tab you can select the configurations that will be involved in the report.

The complete list of available configurations can be found in the Assignable pane (**Actions** > **Add** button).

From the list displayed in the Assignable pane, select the configuration (using the [Ctrl] or [Shift] keys for multiple selection) to aggregate to the report.

After the selection, click the **Ok** button and the selected items will be automatically added into the Assigned tab.

If you need to remove one or more configurations from the set shown in this last tab, select them and click the **Actions** > **Remove**button.

When the configuration activity in this Tab is finished, click the **Next** button.

Filters tab

In this tab you can:
- Set the filters for the report
- Choose the output format that will be generated by selecting the related radio button.

Under the **Filters** tab you can find a **Filter** box in which to configure additional filters that can refine the result of the report.

The following output formats for the report are available:
- XLSX
- RTF
- PDF
- HTML
- DOCX
- CSV

Typically, for every report, only a subset of these six formats can be chosen.

The first format type of the list is selected by default.

Schedule Tab

The **Schedule** tab provides the configuration of scheduling rules for the production of the report.

The available options are:
- **Frequency**: From this combobox you can set the Connector frequency start from once to 12 Hours.
- **Immediately**: Selecting this radio button the Connector starts immediately.
- **Date**: You can set the date (dd/mm/yyyy) and the hour (hh:mm) of the Connector start.

To complete the configuration of the report, click the **Execute** button. A diagnostic message will advise you that a report has been scheduled and will be processed. A complete list of scheduled reports is shown in the section Download.

Chapter 30. Download

You can follow the status of a report and download it.

The following table shows a list of the possible report execution statuses:

Table 382. Report execution Status.

Execution Status	Description
Pending	The Report is waiting to run.
Running	The Report is running.
Download	The Report is ready to be downloaded by the user.
Error	An error occurred during the report execution.

Note: When the report is in Download status, you can download it as often as you want until it is deleted by the administrator.

Chapter 31. IBM Security Identity Governance and Intelligence documentation

After you log in, you can access the following interfaces:

IBM Security Identity Governance and Intelligence Chapter 1, "Administration Console," on page 3

Central Administration is the administration dashboard that provides control over the various management features of the IBM Security Identity Governance and Intelligence platform.

IBM Security Identity Governance and Intelligence Chapter 32, "Service Center," on page 669

The Service Center contains the applications that are available to the user.

For complete documentation, see the IBM Security Identity Governance and Intelligence Knowledge Center at http://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.2.

Part 2. Managers

Managers are defined in the *Regular Users schema* and can perform tasks in the Service Center. Examples of managers are application managers, user managers, department managers, role managers, and risk managers.

For more information about the tasks that user managers can do, see Personas and use cases.

Chapter 32. Service Center

Service Center shows a dashboard and provides access to Identity Governance and Intelligence applications according to roles assigned to you.

Logging in to the Service Center

To log in to Service Center, enter a valid user name and password in the Login window and click **Login**.

Home - Dashboard

When you log in, you see your **Dashboard** home page. It is a dashboard populated with instruments (dashboard items) that report on various aspects of your roles in the system. A dashboard item is configured to be one of the following types:

- Single value, a number with a title.
- Table, with information arranged in rows and columns.
- Graphic chart, one of pie, line, bar, area, or heat map,

Application menu and top bar

To see the application menu, click the application menu icon ≡ . The application menu is available from any application or pane in the system. Your menu choices can be constrained by your role in the system. Some choices that are shown in the following list might not be available to your role.

- **Home** - Your home **Dashboard**
- **Access Certifier** - See Chapter 35, “Introduction to Access Certifier,” on page 679.
- **Access Requests** - See Chapter 37, “Introduction to Access Requests,” on page 741.
- **Reports** - See Chapter 39, “Introduction to Report Client,” on page 889.
- **User-Account Matching** - See Chapter 36, “Introduction to User-account matching,” on page 737.
- **Business Activity Mapping** - See Chapter 38, “Introduction to Business Activity Mapping,” on page 885.
- **Logout** - Logs you out of the system
- **Act as delegate for...** - Click to select a user. You must be configured as a delegate for that user.
- **Terms of Use** - Displays the terms of use for the system.
- **Current Realm: (Realm)** - Read only. The realm that you are working in
- **Last login: (Month) (day), (year) (timestamp)** - Read only. The date and time you last logged in

The top bar also shows the following items:

- Identity Governance and Intelligence
- **(Realm)/(User)** - The realm and login name you are using

- **Help** - Help in the IBM Knowledge Center for your current location in the system.

Dashboard item controls

Table 383. Dashboard items controls

Icon	Label	Description
⤢	**Maximize**	Click to enlarge the dashboard item. Click again to return to normal size.
⟳	**Refresh**	Click to refresh the dashboard item. If the underlying data changed, the refresh shows the changes.
⚙ ⌄	**Settings**	Click and choose **Configure** to configure the following settings: • **Chart Type** - Click to choose a chart type from the menu. The chart types available depend on the query for the dashboard item and the configuration of the dashboard item. • **Legend** - Click to display a dialog for choosing the position of the legend.
▼	**Filter**	Click and enter filter criteria in the dialog. Filter fields depend on the dashboard item configuration.
≡	None. Columns table control	Show or hide columns. Appears only for tables, in the upper right of the table dashboard item. Click to choose which columns to hide or show. The columns available depend on the dashboard item configuration.

Table 383. Dashboard items controls (continued)

Icon	Label	Description
Drill down	None. Cursor changes from arrow to select when you move it over an item where you can drill down.	Click to access to additional information that is typically in another application. Depending on the configuration of the dashboard item, you might drill down on the following items: • Single-value dashboard item • Graphic chart part - a pie slice, bar section, or line. • Table row **Attention:** This control does not work for custom dashboards that are created with the **Add from Query** action in Report Designer.
No data available		Read-only message that appears instead of a table or graphic chart if no data returns from the query.

Chapter 33. Password management

Managers and help desk personnel can manage passwords in the Service Center for yourself or for others, depending how the system is configured.

Password management tasks

You can use the Self Care application to change your own password or reset your password. You can use the Access Request application to change or reset the password for other users.

Use the Service Center to do these tasks:

Table 384. Password management tasks

Task	Refer to
Reset your own password if you have forgotten it.	"Resetting my forgotten password"
Change or reset the account password of other users.	"Resetting account passwords for other users" on page 674

For information about password-related tasks that administrators can do in the Administration Console, see Chapter 13, "Password administration," on page 109.

Resetting my forgotten password

If you forgot your Service Center password, you can either specify a new password or have the system generate new password.

Before you begin

The administrator must configure the forgotten password service in the Administration Console. Otherwise, the **Forgot your password?** link does not display on the Service Center Login page. For more information, see "Configuring password services" on page 110.

Your security questions must already be set up. For more information, see Chapter 44, "Updating my security questions," on page 903.

About this task

When you forget your password, you must answer the security questions correctly to reset your password. The new password replaces the old password for your Service Center account. Depending on how your system is configured, you can either specify a new password or use a system-generated password. The new password is sent to the email address that is specified in your personal profile.

If no email address is defined in your personal profile, the system-generated password cannot be sent. Contact the help desk or administrator to add an email address to your profile.

Procedure

1. From the Service Center Login page, type your user ID, and then click **Forgot your password?**
2. On the Forgot Your Password page, answer the security questions, and then click **Continue**. The following scenarios are possible, depending on how a system administrator configured the system:

Option	Description
The questions are answered correctly, and your system is configured for you to specify a new password.	Type your new password in the **New Password** field, and then type your new password again in the **Confirm Password** field. Then, click **Change Password**. When you see a message that indicates a successful password change, click **OK**.
The questions are answered correctly, and your system is configured to generate a new password and send the password to a predefined email address.	A new system-generated password is automatically sent to the email that is defined in your personal profile. You must use this new password on your next login, and then you can change your password on your next login. Click **Return to Login**.
The questions are answered correctly, and your system is configured to generate a new password and prompts you to type an email address.	Type the email address where you want the new system-generated password to be sent. You must use this new password on your next login, and then you must change your password on your next login. Click **Continue**. When you see a message that indicates a successful operation, click **Return to Login**.
The questions are answered correctly, and your system is configured to generate a new password. However, an email address is not defined in your personal profile.	Contact the help desk or administrator to add your email address to your personal profile. Click **Return to Login**. After the email address is added to your profile, you can follow the **Forgot your password?** link again from the Service Center Login page to receive the system-generated password in your email address.
The questions are not answered correctly, and an error message is displayed. Depending on how your system is configured, you might have more attempts to correctly answer the questions.	You cannot access the system unless you remember your password or answer the questions correctly. If you exceed the maximum number of attempts to verify your identity, your Service Center account is locked. Contact your help desk or administrator to unlock your Service Center account or reset your Service Center password.

Related reference:

Chapter 34, “Forgot Your Password,” on page 677
If you forgot your Service Center password, you can reset it.

Resetting account passwords for other users

If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

Before you begin

You must be entitled with a role (for example, `User Manager` or `Application Manager`) that has the permission to reset the account passwords of other users.

About this task

Depending on how a system administrator configured the system, you can change or reset the passwords of other users in the Access Requests application of Service Center.

Procedure

1. Log in to the Service Center.
2. On the Service Center home page, select **Access Requests**. The Access Requests page is displayed.
3. Select the role that is entitled to reset passwords for others, such as **User Manager** or **Application Manager**.
4. Select the tab that is associated with the password reset task, such as **ManagerPasswordResetGEN** or **HelpDeskPasswordResetGEN**. The first page of a wizard displays the list of users whose password you are entitled to reset. The wizard leads you through the completion of your task.
5. Select a user in the list and click **Next**. Depending on the process that is defined for your role, the next window displays the security questions that verify the identity of the user or the names of the accounts for which the password you are about to reset grants access.
6. If the Security Questions window is displayed, enter the answers to the security questions with the help of the user. The answers must match the answers that were first entered by the user on the first login. The **Identified by other means** check might be available. You can skip the security questions and select this box as an alternative. Click **Next** to proceed to the Accounts window.
7. The Accounts window lists all the accounts that the user is entitled to access. The `Ideas` account is associated with the Service Center. Select the accounts and click **Next** to proceed to the Account Password Management window where you enter the password or generate the password.
8. The items featured in this window depend on the setup that was done by the administrator. Complete the following items when they are available:
   a. In the **Applicant** box, enter your own password.
   b. In the **Beneficiary** box, either type the new password or select **Generate** to have the password created automatically.

      If the **Generate** button is available, select it to create the password automatically.

      If there is no **Generate** button, type the new password in the **New password** field and the **Confirm password** field. A **Show password characters** check box might be displayed. Select it to see the characters you type. As you type, a list of password requirements on the right shows if you are complying with standards.
   c. The **New password will be sent to this email address** field displays the email address of the user. Based on the configuration, you might be able to edit it. If the field is not displayed, you must communicate the new password to the user by other means.
9. Click **Submit** to complete the request.

Results

The password is created and emailed to the beneficiary. The request is marked as completed. Depending on the configuration of the process, the request might be listed with other requests in a report or in another tab available to an `Operator` or similar role.

Related information:

"Entering the new password in a new request to make account changes" on page 748
This final step of the wizard guides you to reset the password.

Chapter 34. Forgot Your Password

If you forgot your Service Center password, you can reset it.

When you forget your password, you must answer the security questions correctly and change your password. The new password replaces the old password for your Service Center account.

You can reset your password only if you previously set up security questions for the Service Center.

Depending on how a system administrator configured the system, these scenarios are possible:

- You can change your password immediately.
- The system generates a new password and sends it to your email address that is specified in your personal profile.
- The system generates a new password and prompts you to enter an email address to send it to.

If no email address is defined in your personal profile, the new system-generated password cannot be sent. Contact the help desk or administrator to add an email address to your profile.

You cannot access the system unless you remember your password or answer the questions correctly. If you exceed the maximum number of attempts to verify your identity, your Service Center account is locked. Contact your help desk or administrator to unlock your Service Center account or reset your Service Center password.

Related tasks:

"Resetting my forgotten password" on page 673
If you forgot your Service Center password, you can either specify a new password or have the system generate new password.

Chapter 35. Introduction to Access Certifier

The Access Certifier (AC) is the module dedicated to implementing certification for an organization.

The Access Certifier module provides a complete and flexible workflow for certifying permissions that are aggregated to a user through a specific role, according to the RBAC standard and `segregation of duty` policies that are enforced by the IBM Security Identity Governance and Intelligence platform.

For example, adding a set of permissions (entitlements) to a role structure might require certification. Mixing old and new entitlements can originate new permissions to be reviewed by an administrator.

Consider the example of fusing two different organization units (OUs) to form a new one: this new situation requires the review of roles that are already aggregated to the old OUs.

The Access Certifier module assists administrators during the role certification workflow by assigning different scopes and responsibilities to several specific certification functions.

User - Assignment Reviewer
: To monitor permissions that are joined to a user.

OU - Entitlement Reviewer
: To monitor entitlement joined to the OUs.

Entitlement Reviewer
: To monitor the structure of a generic entitlement.

Risk Reviewer
: To monitor mitigation controls that are joined to the users risks.

Supervisors
: To monitor the activities of the reviewers.

ℹ	**Note:** The Access Governance Core administrator defines the campaign contents. Access Certifier users can approve or revoke these contents.

Campaign Management

The following functions for managing the main entities of this module are available:

Summary of available campaigns

In the **Summary** tab, you can view the list of available campaigns.

The following table lists the **Summary** attributes:

Table 385. Summary Attributes

Attribute	Description
Type	Types of campaigns for common reviewers: • User • OU • Risk • Entitlements • Accounts When a supervisor approves: • User • OU • Risk • Entitlements • Accounts
Campaign Name	Name of the campaign.
End Date	End date of the campaign.
Status	Status of the campaign. ⊘ **Stopped** shows closed campaigns. If this icon is not present, campaigns are open.
Supervisor	Name of the supervisor of the campaign.
Requested by	Name of the applicant of the campaign.
% Completion	Percentage of the entities that are certified.

The **Details** tab is activated only after the campaign is selected.

- User - Assignment (Reviewer)
- OU - Entitlement (Reviewer)
- Risk Violation Mitigation (Reviewer)
- Entitlements (Reviewer)
- Account (Reviewer)
- User - Assignment (Supervisor)
- OU - Entitlement (Supervisor)

- Risk Violation Mitigation (Supervisor)
- Entitlements (Supervisor)
- Account (Supervisor)

Table 386. Details tab note

ℹ	**Note:** The Access Governance Core administrator defines the campaign contents and settings. Access Certifier reviewers can have different sets of functional buttons, icons, or tabs available, depending on the configuration of the campaign.

Details - OU Entitlement Review

After you select the campaign, the **Details** tab shows the list of the entities to be certified.

To search a specific entity, set the filters that are shown in the following table by clicking **Filter**/**Hide Filter**:

Table 387. Filters

Filter	Description
Org Unit	Click … **OU** to enter an OU.
Hierarchy	If this check box is ticked, the search activity is on all the hierarchy. It starts from the root OU indicated in **Org Unit**.
Activity	Click… **Browse** to choose the Activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.
Status	Indicates the status of the certification. • **Complete** • **Pending**
Owner	Indicates the owner of the certification activity. • **Assigned to me** • **Redirect by me** • **Redirect to me** • **Returned**
Only Entity with Violation	If this check box is ticked, the search activity is on the entity with Visibility Violation.

When you click the link **Campaign:** *Campaign Name* in the upper right part of the page, the Campaign Info window displays the information in the following table:

Table 388. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.

Table 388. Campaign Info window (continued)

Field	Description
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: **Automatic** The approval or revocation is immediately signed off. **By User** The user decides when to sign off on the approval or revocation. **End Review** The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, the **Details** tab structure can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 389. Details tab buttons and icons

Button/Icon	Description
Inspect	Inspect the entities of the campaign.
Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
30 **History**	In the Note History window, **History** displays the information about the previous campaigns in which the entity was involved. When you select a listed item, **Note** opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
Notes	Click to insert a note about the entity.
Notes	Click to read a note that was previously inserted through .
Redirect	Redirect to another reviewer to be approved or revoked. In the field **Redirect to** you must set the name of the reviewer.
Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using **Return**.
Return	Return the information to the sender reviewer.
Redirect	Received by a reviewer after the checking (see **Return**).

Table 389. Details tab buttons and icons (continued)

Button/Icon	Description
Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
Sign off	The certifier can decide when to sign off on the approval or revocation.
Show UME	Identifies the master UME, and you can group UME.
Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
🔵 / 🟠 / 🔴	Click the colored dot to open a window that displays the following activities: • The risk activities tree (related to a specific user) into the **Risk Info** tab • The activities that are involved in a specific risk into the **Risk Activity** tab
Certifying: ***EntityName***	Click **Certifying**: ***EntityName*** in the upper-right part of the page to display information about the entity.
Approve **Revoke** **Redirect** **Escalate** **Sign-off**	In the upper-right side of the page, which is aligned with **Filter/Hide Filter** and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Entitlement/OU Visibility Details		
Type of Campaign	**Detail**	**Description**
Entitlement/OU Visibility	**Action**	Allows the inspection of the entities of the campaign.
	Code	Univocal identifier of the OU.
	Name	Name of the OU.
	% Entity Completion	Percentage of the entities that are certified.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

When you click the ⓘ **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 390. Entity information

Tab	Attributes	Description
User Details	**OU**	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip/Postal code	Zip/Postal code of the User.
	Country	Country of the User.
	Phone	Phone number of the User.
Entitlement Details	**Type**	Type of the Entitlement: • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab **Org. Units**.
	Users	List of Users that are associated to the Entitlement.

Table 390. Entity information (continued)

Tab	Attributes	Description
OU Details	**Type**	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click **Actions** > **Users** for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

Details - Entitlement/User

After the selection of the campaign, the **Details** tab opens and shows specialized views.

Detailsincludes the following specialized views:

- Details - Entitlement View
- Details - User View

This view option and the contents of the views, can be changed by the administrator.

Note: The Access Governance Core administrator defines the campaign contents and settings. Access Certifier reviewers can have different sets of functional buttons, icons, or tabs available, depending on the configuration of the campaign.

Details - Entitlement View

After the selection of the Campaign, the Details tab shows the list of the entities to be certified. To search a specific *Entity*, set the filters in the following table by clicking **Filter**/**Hide Filter**:

Table 391. Entitlement View filters.

Context	Filter	Description
User	**Org Unit**	Click ⋯ **OU** to enter an OU.
	Hierarchy	If this check box is ticked, the search activity is on all the hierarchy. It starts from the root OU indicated in **Org Unit**.
	Identity	This field can host the name, the surname, or the User ID of the user.
	UME	UME is a digital identity (User) that can have more than one account on the same Target System. If this check box is ticked, the search activity is on all the UME in the Campaign.
	Activity	Click ⋯ **Browse** to choose the Activity associated with the users through the permission associated with the users.
	Hierarchy	If this check box is flagged, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.
	Only Users with Violations	If this check box is ticked, the search activity applies only to users with outstanding violations.
Entitlement	**Application**	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	Status	Indicates the status of the certification. • **Complete** • **Pending**
	Type	Indicate the entitlement type. • **Permission** • **IT Role** • **Business Role** • **External Role**
	Only with Visibility Violations	If this check box is ticked, the search activity applies to the entitlements in role alignment violation. That is, entitlements are assigned to a user, but they do not belong to the OU of the user.
	Reviewed	Was the user reviewed? • **Formerly** indicates that the user was reviewed at least one time. • **Never** indicates that the user was not reviewed.
	Owner	Indicates the owner of the certification activity. • **Assigned to me** • **Redirected by me** • **Redirected to me** • **Returned**
	User Hierarchy	Indicates the group hierarchy for filtering entitlements to be certified.

Clicking the link **Campaign *Campaign Name*** in the upper right part of the frame displays the information summarized in the following table in the Campaign Info window:

Table 392. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: **Automatic** The approval or revocation is immediately signed off. **By User** The user decides when to sign off on the approval or revocation. **End Review** The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Details can show different sets of attributes or different sets of icons and buttons. They are based on the type of the campaign you selected.

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 393. Details tab buttons and icons

Button/Icon	Description
🔍 **Inspect**	Inspect the entities of the campaign.
ⓘ **Entity info**	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
📅 **History**	In the Note History window, **History** displays the information about the previous campaigns in which the entity was involved. When you select a listed item, **Note** opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
📝 **Notes**	Click to insert a note about the entity.
📝 **Notes**	Click to read a note that was previously inserted through 📝.

Table 393. Details tab buttons and icons (continued)

Button/Icon	Description
Redirect	Redirect to another reviewer to be approved or revoked. In the field **Redirect to** you must set the name of the reviewer.
Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using **Return**.
Return	Return the information to the sender reviewer.
Redirect	Received by a reviewer after the checking (see **Return**).
Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
Sign off	The certifier can decide when to sign off on the approval or revocation.
Show UME	Identifies the master UME, and you can group UME.
Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
🔵 / 🟠 / 🔴	Click the colored dot to open a window that displays the following activities: • The risk activities tree (related to a specific user) into the **Risk Info** tab • The activities that are involved in a specific risk into the **Risk Activity** tab
Certifying: ***EntityName***	Click **Certifying**: *EntityName* in the upper-right part of the page to display information about the entity.
Approve **Revoke** **Redirect** **Escalate** **Sign-off**	In the upper-right side of the page, which is aligned with **Filter/Hide Filter** and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table shows the entire superset of configurable columns for the details of the campaign:

Table 394. Columns for Entitlement View

Column	Description
Attestation buttons	Makes actions visible. • **Approve** • **Revoke** • **Sign Off** • **Notes** • **Redirect** • **Redirect to Supervisors**
Master UID	UID of the user.
User First Name	Given name of the user.

Table 394. Columns for Entitlement View (continued)

Column	Description
User Last Name	Surname of the user.
User info buttons	Makes user information visible. • **Details** • **Entitlements** • **External Data** • **Accounts** • **Activities** • **Rights**
OU Name - Code	Name and code of the organizational unit (OU).
OU Owner	Owner of the organizational unit, according to the setting in AGC.
OU Description	Short description of the organizational unit.
Application Name	Name of the application, with the information available about the application.
Application Owner	Owner of the application, according to the setting in AGC.
Application Description	Short description about the application.
Entitlement Name	Name of the entitlement. If the **Entitlement Localization** option is active, the entitlement is shown as a localized name.
Entitlement ID Code	ID code of the entitlement.
Entitlement Description	Short description of the entitlement.
Entitlement info button	Makes entitlement information visible. • **Details** • **Structure** • **Activities** • **Rights**
VV	Role Alignment Violation property, which is related to an entitlement assigned to a user but not joined to the organizational unit of the user.
User Type Name	Type of user, according to AGC settings.
Group Name [Code]	The IGI Administrator can configure several types of hierarchies that are based on user attributes. Every hierarchy can be made by several groups. A group is an element (a node) of the hierarchy, identifies by a name and a specific code. Every group can be associate to a set of entitlements.
Hierarchy Name	Identifier of the hierarchy. The base hierarchy is ORGANIZATIONAL_UNIT hierarchy.

Every row of the campaign host an entitlement to be certified.

You must consider every row as a node of a tree.

You must select and work only one node at the time.

The type of entitlement might be
- **Permission**
- **IT Role**

- **Business Role**
- **External Role**

Click the little dark row, on the left of the selected entitlements, for expanding a possible set of subrows that are present if the entitlement is associated to a set of rights.

Note: If the entitlement contains all rights with empty values, it's not possible to expand the structure clicking the dark row.

Note: It's not possible to associate rights to an **External Role**.

If you are considering a permission, the rights that are associated are listed under the permission node.

If you are considering another type of entitlement, the hierarchy of nodes is expanded up to list all permissions and rights that are involved.

If you have a single value right that is associated to a permission, you have only one subrow to manage.

If you have a multi-value right that is associated to a permission, you can have several subrows to manage, in a flat view.

On a row that is related to the value of a right, you can make the following operations:

- **Revoke** deletes the value of a right (the button turns red, like the name of the right).
- **Edit** changes the value of a right (the button turns orange, like the name of the right).

Every value that is not edited keeps its value.

The previous operations are effective and are propagated to the DB of Access Governance Core only if you confirm them, through the button **Approve** related to the selected node.

To click **Approve** is needed for triggering the sign-off action that is configured for the campaign.

It is possible to have several types of sign-off:

- Automatic (after you click **Approve** or **Revoke** for the selected node).
- Manual (after you click **Approve** or **Revoke** for the selected node, the button ✎ **Sign off** is enabled).
- At the end of the campaign, automatically.

After the sign-off, you can click 📅 **History** in the row of a specific right, for getting a pop-up with a list of all operations performed.

For required permission with N>1 rights, it is possible to revoke N-1 rights, preserving at least one right (on the last right, the **Revoke** button is disabled).

The **Revoke** button is disabled also for a required permission that has just one right available.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can be no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

Note: In some views, only a subset of the data that is indicated might be shown.

When you click the ⓘ **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 395. Entity information

Tab	Attributes	Description
User Details	**OU**	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip/Postal code	Zip/Postal code of the User.
	Country	Country of the User.
	Phone	Phone number of the User.

Table 395. Entity information (continued)

Tab	Attributes	Description
Entitlement Details	**Type**	Type of the Entitlement: • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab **Org. Units**.
	Users	List of Users that are associated to the Entitlement.
OU Details	**Type**	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click **Actions** > **Users** for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	

Table 395. Entity information (continued)

Tab	Attributes	Description
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

Details - User View

The **User View** tab shows the list of the users to be certified. To search a specific user, set the filters in the following table by clicking **Filter**/**Hide Filter**:

Table 396. Filters

Filter	Description
Org Unit	Click ⋯ **OU** to enter an OU.
Hierarchy	If this check box is ticked, the search activity is on all the hierarchy. It starts from the root OU indicated in **Org Unit**.
Identity	This field can host the name, the surname, or the ID of the user.
UME	UME is a digital identity (User) that can have more than one account on the same Target System. If this check box is ticked, the search activity is on all the UME in the Campaign.
Activity	Click⋯ **Browse** to choose the Activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.
Status	Indicates the status of the certification. • **Complete** • **Pending**
Owner	Indicates the owner of the certification activity. • **Assigned to me** • **Redirect by me** • **Redirect to me** • **Returned**
Only Users with Violation	If this check box is ticked, the search activity is on the entity with Visibility Violation.

Clicking **Campaign :*Campaign Name*** in the upper right part of the frame displays the information summarized in the following table in the Campaign Info window:

Table 397. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.

Table 397. Campaign Info window (continued)

Field	Description
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: **Automatic** The approval or revocation is immediately signed off. **By User** The user decides when to sign off on the approval or revocation. **End Review** The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Details shows a list of rows.

Every row is composed of a different set of attributes and a different set of icons and buttons.

Note: The Access Governance Core administrator defines the campaign contents and settings. Access Certifier reviewers can have different sets of functional buttons, icons, or tabs available, depending on the configuration of the campaign.

The following table shows the entire superset of buttons and icons for the **Details** tab:

Table 398. Details tab buttons and icons

Button/Icon	Description
Inspect	Inspect the entities of the campaign.
Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
History	In the Note History window, **History** displays the information about the previous campaigns in which the entity was involved. When you select a listed item, **Note** opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
Notes	Click to insert a note about the entity.
Notes	Click to read a note that was previously inserted through .
Redirect	Redirect to another reviewer to be approved or revoked. In the field **Redirect to** you must set the name of the reviewer.
Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using **Return**.
Return	Return the information to the sender reviewer.

Table 398. Details tab buttons and icons (continued)

Button/Icon	Description
Redirect	Received by a reviewer after the checking (see **Return**).
Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
Sign off	The certifier can decide when to sign off on the approval or revocation.
Show UME	Identifies the master UME, and you can group UME.
Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
🔵 / 🟠 / 🔴	Click the colored dot to open a window that displays the following activities: • The risk activities tree (related to a specific user) into the **Risk Info** tab • The activities that are involved in a specific risk into the **Risk Activity** tab
Certifying: ***EntityName***	Click **Certifying**: ***EntityName*** in the upper-right part of the page to display information about the entity.
Approve **Revoke** **Redirect** **Escalate** **Sign-off**	In the upper-right side of the page, which is aligned with **Filter/Hide Filter** and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

Selecting one item, related to a specific user, and clicking on 🔍 **Inspect** you can get a table of entitlements related to the selected item.

Every row of the campaign host an entitlement to be certified.

You must consider every row as a node of a tree.

You must select and work only one node at the time.

The type of entitlement might be
- **Permission**
- **IT Role**
- **Business Role**
- **External Role**

Click the little dark row, on the left of the selected entitlements, for expanding a possible set of subrows that are present if the entitlement is associated to a set of rights.

Note: If the entitlement contains all rights with empty values, it's not possible to expand the structure clicking the dark row.

Note: It's not possible to associate rights to an **External Role**.

If you are considering a permission, the rights that are associated are listed under the permission node.

If you are considering another type of entitlement, the hierarchy of nodes is expanded up to list all permissions and rights that are involved.

If you have a single value right that is associated to a permission, you have only one subrow to manage.

If you have a multi-value right that is associated to a permission, you can have several subrows to manage, in a flat view.

On a row that is related to the value of a right, you can make the following operations:

- **Revoke** deletes the value of a right (the button turns red, like the name of the right).
- **Edit** changes the value of a right (the button turns orange, like the name of the right).

Every value that is not edited keeps its value.

The previous operations are effective and are propagated to the DB of Access Governance Core only if you confirm them, through the button **Approve** related to the selected node.

To click **Approve** is needed for triggering the sign-off action that is configured for the campaign.

It is possible to have several types of sign-off:

- Automatic (after you click **Approve** or **Revoke** for the selected node).
- Manual (after you click **Approve** or **Revoke** for the selected node, the button ✎ **Sign off** is enabled).
- At the end of the campaign, automatically.

After the sign-off, you can click 📅 **History** in the row of a specific right, for getting a pop-up with a list of all operations performed.

For required permission with N>1 rights, it is possible to revoke N-1 rights, preserving at least one right (on the last right, the **Revoke** button is disabled).

The **Revoke** button is disabled also for a required permission that has just one right available.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can be no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

Note: In some views, only a subset of the data that is indicated might be shown.

The following table shows the entire superset of configurable columns for the details of the campaign:

Table 399. Configurable columns for the details of the campaign

Column	Description
Attestation buttons	Makes for attestations actions available: **Approve** - **Revoke** - **Sign Off** - **Notes** - **Redirect** - **Escalate to Supervisors**, or other. See the entire set.
Master UID	Unique identifier of the user.
Type	Indicates the type of user, according to configurations.
User First Name	Name of the user.
User Last Name	Surname of the user.
User info buttons	Click to see a set of information tabs related to the user: **Details** - **Entitlements** - **External Data** - **Accounts** - **Activities** - **Rights**.
OU Name - Code	Name of the OU and the unique identifier of the OU.
% Entitlement Completion	A progressive bar indicates the % of certified entitlements of the user.

Every row in the **Details** tab is characterized by the **% Entity Completion** progress bar, indicating the percentage of the Entities certified.

When you click the ⓘ **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 400. Entity information

Tab	Attributes	Description
User Details	**OU**	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip/Postal code	Zip/Postal code of the User.
	Country	Country of the User.
	Phone	Phone number of the User.

Table 400. Entity information (continued)

Tab	Attributes	Description
Entitlement Details	**Type**	Type of the Entitlement: • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab **Org. Units**.
	Users	List of Users that are associated to the Entitlement.
OU Details	**Type**	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click **Actions** > **Users** for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	

Table 400. Entity information (continued)

Tab	Attributes	Description
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

Details - User Remediation Review

After you select the campaign, the **Details** tab shows the list of the entities to be certified.

To search a specific entity, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 401. Filters

Filter	Description
Org Unit	Click ⋯ **OU** to enter an OU.
Hierarchy	If this check box is ticked, the search activity is on all the hierarchy. It starts from the root OU indicated in **Org Unit**.
Identity	This field can host the name, the surname, or the ID of the user.
UME	UME is a digital identity (User) that can have more than one account on the same Target System. If this check box is ticked, the search activity is on all the UME in the Campaign.
Activity	Click⋯ **Browse** to choose the Activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.
Status	Indicates the status of the certification. • **Complete** • **Pending**
Owner	Indicates the owner of the certification activity. • **Assigned to me** • **Redirect by me** • **Redirect to me** • **Returned**
Only Users with Violation	If this check box is ticked, the search activity is on the entity with Visibility Violation.

When you click the link **Campaign:** *Campaign Name* in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Table 402. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.

Table 402. Campaign Info window (continued)

Field	Description
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: **Automatic** The approval or revocation is immediately signed off. **By User** The user decides when to sign off on the approval or revocation. **End Review** The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, **Details** can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 403. Details tab buttons and icons

Button/Icon	Description
Inspect	Inspect the entities of the campaign.
Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
History	In the Note History window, **History** displays the information about the previous campaigns in which the entity was involved. When you select a listed item, **Note** opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
Notes	Click to insert a note about the entity.
Notes	Click to read a note that was previously inserted through 📝.
Redirect	Redirect to another reviewer to be approved or revoked. In the field **Redirect to** you must set the name of the reviewer.
Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using **Return**.
Return	Return the information to the sender reviewer.

Table 403. Details tab buttons and icons (continued)

Button/Icon	Description
Redirect	Received by a reviewer after the checking (see **Return**).
Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
Sign off	The certifier can decide when to sign off on the approval or revocation.
Show UME	Identifies the master UME, and you can group UME.
Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
🔵 / 🟠 / 🔴	Click the colored dot to open a window that displays the following activities: • The risk activities tree (related to a specific user) into the **Risk Info** tab • The activities that are involved in a specific risk into the **Risk Activity** tab
Certifying: ***EntityName***	Click **Certifying**: ***EntityName*** in the upper-right part of the page to display information about the entity.
Approve **Revoke** **Redirect** **Escalate** **Sign-off**	In the upper-right side of the page, which is aligned with **Filter/Hide Filter** and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Table 404. Risk Violation Mitigation Details

Type of Campaign	Detail	Description
Risk Violation Mitigation	**Action**	Allows the inspection of the entities of the campaign.
	Violation	Risk level: 🔵 : **Low level** 🟠 : **Medium level** 🔴 : **High level** When you click a colored dot, the Risk Info window opens.
	Master UID	Univocal identifier of the user.
	User Type	Indicates the type associated with the user.
	Name	Name of the user.
	Last Name	Surname of the user.
	OU Name [Code]	Name of the OU [Univocal identifier of the OU].
	% Entity Completion	Percentage of the entities that are certified.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can be no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

When you click the ⓘ **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 405. Entity information

Tab	Attributes	Description
User Details	**OU**	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip/Postal code	Zip/Postal code of the User.
	Country	Country of the User.
	Phone	Phone number of the User.
Entitlement Details	**Type**	Type of the Entitlement: • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab **Org. Units**.
	Users	List of Users that are associated to the Entitlement.

Table 405. Entity information (continued)

Tab	Attributes	Description
OU Details	**Type**	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click **Actions** > **Users** for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

Details - Entitlement Review

After you select the campaign, **Details** shows the list of the entities to be certified.

To search a specific entity, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 406. Entitlement View filters.

Context	Filter	Description
User	**Org Unit**	Click ... **OU** to enter an OU.
	Hierarchy	If this check box is ticked, the search activity is on all the hierarchy. It starts from the root OU indicated in **Org Unit**.
	Identity	This field can host the name, the surname, or the User ID of the user.
	UME	UME is a digital identity (User) that can have more than one account on the same Target System. If this check box is ticked, the search activity is on all the UME in the Campaign.
	Activity	Click ... **Browse** to choose the Activity associated with the users through the permission associated with the users.
	Hierarchy	If this check box is flagged, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.
	Only Users with Violations	If this check box is ticked, the search activity applies only to users with outstanding violations.
Entitlement	**Application**	Name of the application.
	Search Entitlement (Name or Code)	Name or code of the entitlement.
	Status	Indicates the status of the certification. • **Complete** • **Pending**
	Type	Indicate the entitlement type. • **Permission** • **IT Role** • **Business Role** • **External Role**
	Only with Visibility Violations	If this check box is ticked, the search activity applies to the entitlements in role alignment violation. That is, entitlements are assigned to a user, but they do not belong to the OU of the user.
	Reviewed	Was the user reviewed? • **Formerly** indicates that the user was reviewed at least one time. • **Never** indicates that the user was not reviewed.
	Owner	Indicates the owner of the certification activity. • **Assigned to me** • **Redirected by me** • **Redirected to me** • **Returned**
	User Hierarchy	Indicates the group hierarchy for filtering entitlements to be certified.

Table 407. Note about the UME check box

ℹ	**Note:** When the check box **UME** is selected, results show only the UME in the campaign. When you click **Master UME**, it displays all of the UME of the selected master.

When you click the link **Campaign:** *Campaign Name* in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Table 408. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: **Automatic** The approval or revocation is immediately signed off. **By User** The user decides when to sign off on the approval or revocation. **End Review** The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, **Details** can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons of the **Details** tab:

Table 409. Details tab buttons and icons

Button/Icon	Description
Inspect	Inspect the entities of the campaign.
Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.

Table 409. Details tab buttons and icons (continued)

Button/Icon	Description
History	In the Note History window, **History** displays the information about the previous campaigns in which the entity was involved. When you select a listed item, **Note** opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.
Notes	Click to insert a note about the entity.
Notes	Click to read a note that was previously inserted through .
Redirect	Redirect to another reviewer to be approved or revoked. In the field **Redirect to** you must set the name of the reviewer.
Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using **Return**.
Return	Return the information to the sender reviewer.
Redirect	Received by a reviewer after the checking (see **Return**).
Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
Sign off	The certifier can decide when to sign off on the approval or revocation.
Show UME	Identifies the master UME, and you can group UME.
Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
🔵 / 🟠 / 🔴	Click the colored dot to open a window that displays the following activities: • The risk activities tree (related to a specific user) into the **Risk Info** tab • The activities that are involved in a specific risk into the **Risk Activity** tab
Certifying: ***EntityName***	Click **Certifying**: ***EntityName*** in the upper-right part of the page to display information about the entity.
Approve **Revoke** **Redirect** **Escalate** **Sign-off**	In the upper-right side of the page, which is aligned with **Filter/Hide Filter** and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Table 410. Entitlement details

Type of Campaign	Detail	Description
Entitlement	**Action**	Allows the inspection of the entities of the campaign.
	Entitlement	Type and name of the entitlement.
	SoD/SA	Click a colored dot to display the following information: • The risk activities tree (related to a specific user) in **Risk Info**. • The activities that are involved in a specific risk in **Risk Activity**.
	Description	Brief description of the entitlement.
	Application	Name of the entitlement application.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

When you click the ⓘ **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 411. Entity information

Tab	Attributes	Description
User Details	**OU**	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip/Postal code	Zip/Postal code of the User.
	Country	Country of the User.
	Phone	Phone number of the User.

Table 411. Entity information (continued)

Tab	Attributes	Description
Entitlement Details	**Type**	Type of the Entitlement: • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab **Org. Units**.
	Users	List of Users that are associated to the Entitlement.
OU Details	**Type**	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click **Actions** > **Users** for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	

Table 411. Entity information (continued)

Tab	Attributes	Description
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

Details - Account Review

After you select the campaign, the **Details** tab shows the list of the entities to be certified.

To search a specific entity, set the filters in the following table by clicking **Filter/Hide Filter**:

Table 412. Details Filters

Filter	Description
Org Unit	Click ... **OU** to enter an organizational unit (OU).
Hierarchy	If this check box is selected, the search activity applies to all the hierarchy, starting from the root OU that is indicated in **Org Unit**.
Identity	This field can host the name, the surname, or the ID of the user.
UME	UME is a digital identity (user) that can have more than one account on the same target system. If this check box is selected, the search activity applies to all the UME in the campaign.
Activity	Click... **Browse** to choose the activity associated with the users through the permission associated with the users.
Hierarchy	If this check box is flagged, the search starts from the root that is selected in the **Activity** field and runs on the hierarchy.
Only Users with Violations	If this check box is ticked, the search activity is on the entity with Visibility Violation.
Status	The following list shows the status of the certification: • **Complete** • **Pending**
Reviewed	The user can have one of the following review statuses: • **Formerly** indicates that the user was reviewed at least one time. • **Never** indicates that the user was not reviewed.
Account	The identifier of an account.
Owner	The following list shows activity for the owner of the certification: • **Assigned to me** • **Redirect by me** • **Redirect to me** • **Returned**
Application	The identifier of an application.
Account Status	• **Suspend** indicates that the account is suspended. • **Restore** indicates that the account is restored.
Configuration Name	Name of the configuration joined to the account.

Note: When you select **UME**, it shows only the UME in the campaign. When you click **Master UME**, it displays all of the UME of the selected master.

When you click **Campaign:** *Campaign Name* in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Table 413. Campaign Info window

Field	Description
Campaign Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Name of the supervisor.
Campaign Type	Type of the campaign.
Allow Redirection	If this check box is selected, the reviewer can redirect to other reviewer entities to be approved or revoked.
Escalation to Supervisor	If this check box is selected, the reviewer can redirect to the supervisor entities to be approved or revoked.
Notes Revocation (Mandatory)	If this check box is selected, inserting a note is mandatory for an entity revocation.
Sign Off	The method in which the approval or revocation is validated: **Automatic** The approval or revocation is immediately signed off. **By User** The user decides when to sign off on the approval or revocation. **End Review** The approval or revocation is signed off at the end of the campaign.
Start/End Date	Start/end date of the campaign, according to the format established by the administrator.

Depending on the type of the campaign that is selected, the **Details** tab can show:

- Different set of attributes
- Different set of icons and buttons

The following table shows the entire superset of buttons and icons for the **Details** tab:

Table 414. Details tab buttons and icons

Button/Icon	Description
Inspect	Inspect the entities of the campaign.
Entity info	Provides information about the entity in the campaign, such as user, OU, entitlement, and risk.
History	In the Note History window, **History** displays the information about the previous campaigns in which the entity was involved. When you select a listed item, **Note** opens automatically, displaying the note for the selected item.
Approve/Revoke	Approve/revoke associations between entities.

Table 414. Details tab buttons and icons (continued)

Button/Icon	Description
Notes	Click to insert a note about the entity.
Notes	Click to read a note that was previously inserted through .
Redirect	Redirect to another reviewer to be approved or revoked. In the field **Redirect to** you must set the name of the reviewer.
Escalation	Escalate to the supervisor to be approved or revoked. The Supervisor can send back the information using **Return**.
Return	Return the information to the sender reviewer.
Redirect	Received by a reviewer after the checking (see **Return**).
Supervisors	This icon indicates that different supervisors are configured for the selected certification. Click this icon to see the entire list of supervisors.
Sign off	The certifier can decide when to sign off on the approval or revocation.
Show UME	Identifies the master UME, and you can group UME.
Stats	Allows the supervisor to monitor by two types of pie charts, the status of the campaign completion.
🔵 / 🟠 / 🔴	Click the colored dot to open a window that displays the following activities: • The risk activities tree (related to a specific user) into the **Risk Info** tab • The activities that are involved in a specific risk into the **Risk Activity** tab
Certifying: ***EntityName***	Click **Certifying**: ***EntityName*** in the upper-right part of the page to display information about the entity.
Approve **Revoke** **Redirect** **Escalate** **Sign-off**	In the upper-right side of the page, which is aligned with **Filter/Hide Filter** and depending on the previous selection, up to four bulk operations are available. Activate these operations by selecting the check boxes that are associated with each item. You can select all items by clicking the check box on the left side of the upper blue bar.

The following table includes the details of this campaign:

Table 415. Account details

Type of Campaign	Detail	Description
Account	**Application Name**	A list of applications joined to the specific account.
	Account setting	The entire set of data that determines the policy of management of the account.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can be no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

When you click the ⓘ **Info** icon, you get a set of information related to the data model entity that you are considering:

Table 416. Entity information

Tab	Attributes	Description
User Details	**OU**	The type that is associated to the Organizational Unit.
	First Name	Name of the User.
	Last Name	Surname of the User.
	Master UID	Unique identifier of the User.
	User Type	The type that is associated to the User.
	Address	Address of the User.
	City	City of the User.
	Email	Email of the User.
	State	Nation of the User.
	Zip/Postal code	Zip/Postal code of the User.
	Country	Country of the User.
	Phone	Phone number of the User.
Entitlement Details	**Type**	Type of the Entitlement: • Business Role • External Role • IT Role • Permission
	Code	Unique identifier of the Entitlement
	Name	Name of the Entitlement
	Description	Short description that is associated to the Entitlement.
	Owner	Owner of the Entitlement.
	Last Reviewed Date	The date of the last certification of the Entitlement.
	Expiration Date	After this date, the Entitlement is not longer active for the User
	Org. Units	Number of Organizational Units where this Entitlement is present. Click the number for opening the tab **Org. Units**.
	Users	List of Users that are associated to the Entitlement.

Table 416. Entity information (continued)

Tab	Attributes	Description
OU Details	**Type**	The administrator can set specific values for defining types of OU. For example, a Marketing type can be associated to all Organizational Units involved in marketing.
	Name	Name of the Organizational Unit
	Code	Unique identifier of the Organizational Unit
	Owner	Owner of the Organizational Unit
	Description	Short description that is associated to the Organizational Unit.
Structure	The hierarchical tree view of the selected Entitlement.	
Org. Units	A list of all OU related to the selected Entitlement.	
Activities	A list of all activities that are related to the selected User. If you select an activity, click **Actions** > **Users** for getting all the users that are associated to the selected activity.	
Accounts	A list of all accounts that are related to the selected User.	
Rights	A list of all permissions that holds rights and that are related to the selected User.	
Risks	A list of all risks that are related to the selected User.	
Applications	A list of all applications that are related to the selected User.	

Depending on the data model entity, some tabs might not be present.

Details for Supervisor - OU Entitlement

After you select the campaign, the **Details** tab shows information about the selected campaign. Information about the activities of the reviewers of the campaign is also displayed.

In the upper part of the page, information about the campaign is available. It is summarized in the following table:

Supervisor Campaign	
Detail	**Description**
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign in the `dd/mm/yyyy` format.

Supervisor Campaign	
Detail	**Description**
Sign Off	Validation mode for approval or revocation actions: • **Automatic**: The approval or revocation is immediately signed off. • **By User**: The user decides when to sign off on the approval or revocation. • **End Campaign**: The approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign in the `dd/mm/yyyy` format.
% Completion	Percentage of the entities certified.

When you click the link **Campaign:** *Campaign Name* in the upper right part of the page, the Campaign Info window displays the information summarized in the following table:

Campaign Detail	**Description**
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. • Automatic • Completed By User • End campaign

Campaign Detail	Description
Activity Details	Attributes for an active campaign. • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • *Entity* User Signed Off / Total *Entity H/M* Users • Working Progress J/TOT-M – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 417. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	**User Hierarchy** If enabled, shows the available user hierarchy scope. It is always available for organizational units. **Entity** If enabled, shows the entity scope.
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use**Add** and **Remove** to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set `Grace period=0`. Campaigns on Account have the following options: • `Delete the Account` • `Lock the Account`
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of *name Process - name Activity*.
Custom Behaviour	The management of the fulfillment involves a set of rules.

Table 418. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	**Start date** If checked, enables the workflow processes to define the frequency and length of the campaign. **Duration** The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)
Execution Frequency	The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time The set of values is bounded according to the **`Duration`** parameter. If `Duration=Continuous`, you cannot set values for this parameter.
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.

Notification Type	Description
Campaign Started for Reviewer	If **Enable** is set, the reviewer receives an email when the campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information about the campaign.
Activity Reminder for Reviewer	If **Enable** is set, the reviewer receives an email at the following times. • *K* days before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. • When the percentage of activity that is already managed is greater than X%. Determined by **Activity percentage** The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Reviewer	If **Enable** is set, the reviewer receives an email *K days* before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

Notification Type	Description
Campaign Reminder for Supervisor	If **Enable** is set, the supervisor receives an email *K days* before the end of the campaign. Determined by **Days before end date**, *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Continuous Review for Reviewer	If **Enable** is set, the reviewer receives an email when a continuous campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Redirect	If **Enable** is set, the reviewer or supervisor receives an email in response to any action of redirection. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

To search a specific reviewer, set the filters shown in the following table by clicking **Filter/Hide Filter**:

Reviewer filters	
Filter	**Description**
Identity	This field can host the **Name**, the **Surname**, or the **User ID** of the user.
Org Unit	Use ⋯ **OU** on the right side of the attribute's box to enter an OU.
Hierarchy	If this box is ticked, the search activity is on all the hierarchy. It starts from the root OU that is indicated in **Org Unit**.

Results are displayed in the same frame according to the following attributes:

Reviewer details	
Detail	**Description**
Action	◔ **Stats** monitors the status of the campaign completion. 🔍 **Inspect** inspects the entities of the campaign.
User ID	Univocal identifier of the reviewer.
Name	Name of the reviewer.
Surname	Surname of the reviewer.
OU Name [Code]	Name of the organizational unit of the reviewer.

Reviewer details	
Detail	**Description**
% Entity Completion	Percentage of the entities certified.

Clicking **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor the campaign completion status.

If **Sign off** is set to **By User or Automatic**, the `No data to display` message is under **Signed Off**.

By clicking **Inspect**, the Supervisor can view the approved or removed campaigns.

Details for Supervisor - User Entitlement

After the selection of the campaign, the Details tab displays information about the selected campaign and about the activities of the reviewers in the campaign.

The upper part of the frame displays the information about the campaign. It is summarized in the following table:

Supervisor Campaign	
Detail	**Description**
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign.
Sign Off	Validation mode for approval or revocation actions: • **Automatic**: the approval or revocation is immediately signed off. • **By User**: the user decides when to sign off the approval or revocation. • **End Campaign**: the approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign.
% Completion	Percentage of the entities certified.

Clicking **Campaign:** ***Campaign Name*** in the upper right part of the frame displays the information summarized in the following tab in the Campaign Info window:

Campaign Detail	**Description**
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).

Campaign Detail	Description
Campaign Type	Type of campaign. • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • *Entity* User Signed Off / Total *Entity H/M* Users • Working Progress J/TOT-M – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 419. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	**User Hierarchy** If enabled, shows the available user hierarchy scope. It is always available for organizational units. **Entity** If enabled, shows the entity scope.
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use**Add** and **Remove** to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set `Grace period=0`. Campaigns on Account have the following options: • `Delete the Account` • `Lock the Account`
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of *name Process - name Activity*.
Custom Behaviour	The management of the fulfillment involves a set of rules.

Table 420. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	**Start date** If checked, enables the workflow processes to define the frequency and length of the campaign. **Duration** The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)
Execution Frequency	The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time The set of values is bounded according to the **`Duration`** parameter. If `Duration=Continuous`, you cannot set values for this parameter.
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.

Notification Type	Description
Campaign Started for Reviewer	If **Enable** is set, the reviewer receives an email when the campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information about the campaign.

Notification Type	**Description**
Activity Reminder for Reviewer	If **Enable** is set, the reviewer receives an email at the following times. • *K* days before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. • When the percentage of activity that is already managed is greater than X%. Determined by **Activity percentage** The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Reviewer	If **Enable** is set, the reviewer receives an email *K days* before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Supervisor	If **Enable** is set, the supervisor receives an email *K days* before the end of the campaign. Determined by **Days before end date**, *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Continuous Review for Reviewer	If **Enable** is set, the reviewer receives an email when a continuous campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Redirect	If **Enable** is set, the reviewer or supervisor receives an email in response to any action of redirection. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

To search a specific reviewer, set the filters in the following table by clicking **Filter/Hide Filter**:

Reviewer filters	
Filter	**Description**
Identity	This field can host the name, surname, or user ID of the user.
Org Unit	Use ⋯ **OU** on the right side of the attribute to enter an organizational unit.
Hierarchy	If this box is selected, the search activity is on all the hierarchy. It starts from the root OU in **Org Unit**.

Results are displayed in the same frame by the following the attributes:

Reviewer details	
Detail	**Description**
Action	**Stats** monitors the status of the campaign completion. **Inspect** inspects the entities of the campaign.
Master UID	Univocal identifier of the reviewer.
Name	Name of the reviewer
Last Name	Surname of the reviewer.
OU Name [Code]	Name of the organizational unit of the reviewer.
% Entity Completion	Percentage of the entities certified.

Clicking **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor the status of the Campaign completion.

If the campaign sign-off is in **By User** or **Automatic** mode, the `No data to display` message is under **Signed Off Items**.

By clicking **Inspect**, the supervisor can view the approved or removed campaigns.

Details for Supervisor - User Remediation

After the selection of the campaign, the **Details** tab displays information about the selected campaign and about activities of the reviewers in the campaign.

The upper part of the frame displays information about the campaign. It is summarized in the following table:

Supervisor Campaign	
Detail	**Description**
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign in the `dd/mm/yyyy` format.
Sign Off	Validation mode for approval or revocation actions: • **Automatic**: the approval or revocation is immediately signed off • **By User**: the user decides when to sign off the approval or revocation • **End Campaign**: the approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign in the `dd/mm/yyyy` format.

Supervisor Campaign	
Detail	**Description**
% Completion	Percentage of the entities certified.

Clicking **Campaign:** ***Campaign Name*** in the upper right part of the frame displays the information summarized in following tabs in the Campaign Info window

Campaign Detail	Description
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • *Entity* User Signed Off / Total *Entity H/M* Users • Working Progress J/TOT-M – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 421. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	**User Hierarchy** If enabled, shows the available user hierarchy scope. It is always available for organizational units. **Entity** If enabled, shows the entity scope.
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use**Add** and **Remove** to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set `Grace period=0`. Campaigns on Account have the following options: • `Delete the Account` • `Lock the Account`
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of *name Process - name Activity*.
Custom Behaviour	The management of the fulfillment involves a set of rules.

Table 422. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	**Start date** If checked, enables the workflow processes to define the frequency and length of the campaign. **Duration** The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)

Table 422. Cert_Campaign_Scheduling_Tab (continued)

Scheduling Detail	Description
Execution Frequency	The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time The set of values is bounded according to the **`Duration`** parameter. If `Duration=Continuous`, you cannot set values for this parameter.
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.

Notification Type	Description
Campaign Started for Reviewer	If **Enable** is set, the reviewer receives an email when the campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information about the campaign.
Activity Reminder for Reviewer	If **Enable** is set, the reviewer receives an email at the following times. • *K* days before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. • When the percentage of activity that is already managed is greater than X%. Determined by **Activity percentage** The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Reviewer	If **Enable** is set, the reviewer receives an email *K days* before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Supervisor	If **Enable** is set, the supervisor receives an email *K days* before the end of the campaign. Determined by **Days before end date**, *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Continuous Review for Reviewer	If **Enable** is set, the reviewer receives an email when a continuous campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

Notification Type	Description
Redirect	If **Enable** is set, the reviewer or supervisor receives an email in response to any action of redirection. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

To search a specific *Reviewer*, set the filters in the following table by clicking **Filter/Hide Filter**:

Reviewer filters	
Filter	**Description**
Identity	This field can host the name, the surname, or the user ID of the user.
Org Unit	Use ⋯ **OU** on the right side of the attribute to enter an OU.
Hierarchy	If this box is selected, the search activity is on all the hierarchy. It starts from the root OU in **Org Unit**.

Results are displayed in the same frame by the following attributes:

Reviewer details	
Detail	**Description**
Action	◔ **Stats** monitors the status of the campaign completion. 🔍 **Inspect** inspects the entities of the campaign.
User ID	Univocal identifier of the reviewer.
Name	Name of the reviewer
Surname	Surname of the reviewer.
OU Name [Code]	Name of the Org. Unit the Reviewer belongs to.
% Entity Completion	Percentage of the Entities certified.

Clicking ◔ **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor campaign completion status.

If the campaign sign-off is **By User** or **Automatic** mode, the `No data to display` message is under **Signed Off Items**.

By clicking 🔍 **Inspect**, the supervisor can view the approved or removed campaigns.

Details for Supervisor - Entitlement

After you select the campaign, the **Details** tab displays information about it and about the activities of the reviewers in the campaign.

In the upper part of the frame, the information about the campaign is available. It is summarized in the following table:

Supervisor Campaign	
Details	**Description**
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign.
Sign Off	Validation mode for approval or revocation actions: • **Automatic**: the approval or revocation is immediately signed off • **By User**: the user decides when to sign off the approval or revocation • **End Campaign**: the approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of the campaign.
End Date	End date of the campaign.
% Completion	Percentage of the entities certified.

Clicking **Campaign:** ***Campaign Name*** in the upper right part of the frame displays the following information in Campaign Info:

Campaign Detail	**Description**
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.

Campaign Detail	Description
Sign Off	Type of sign-off. • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • *Entity* User Signed Off / Total *Entity H/M* Users • Working Progress J/TOT-M – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 423. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	**User Hierarchy** If enabled, shows the available user hierarchy scope. It is always available for organizational units. **Entity** If enabled, shows the entity scope.
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use**Add** and **Remove** to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.
Physical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set `Grace period=0`. Campaigns on Account have the following options: • `Delete the Account` • `Lock the Account`
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of *name Process - name Activity*.
Custom Behaviour	The management of the fulfillment involves a set of rules.

Table 424. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	**Start date** If checked, enables the workflow processes to define the frequency and length of the campaign. **Duration** The following values are available: - 1, 2, or 3 weeks - 1, 2, 4, 6, or 9 months - 1 year - Continuous (never closed)
Execution Frequency	The following values are available: - 1, 2, or 3 weeks - 1, 2, 4, 6, or 9 months - 1 year - One time The set of values is bounded according to the **`Duration`** parameter. If `Duration=Continuous`, you cannot set values for this parameter.
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.

Notification Type	Description
Campaign Started for Reviewer	If **Enable** is set, the reviewer receives an email when the campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information about the campaign.
Activity Reminder for Reviewer	If **Enable** is set, the reviewer receives an email at the following times. - *K* days before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. - When the percentage of activity that is already managed is greater than X%. Determined by **Activity percentage** The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Reviewer	If **Enable** is set, the reviewer receives an email *K days* before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

Notification Type	Description
Campaign Reminder for Supervisor	If **Enable** is set, the supervisor receives an email *K days* before the end of the campaign. Determined by **Days before end date**, *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Continuous Review for Reviewer	If **Enable** is set, the reviewer receives an email when a continuous campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Redirect	If **Enable** is set, the reviewer or supervisor receives an email in response to any action of redirection. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

To search a specific reviewer, set the filters from the following table by clicking **Filter/Hide Filter**:

Reviewer filters	
Filter	**Description**
Identity	This field can host the **Name**, the **Surname**, or the **User ID** of the user.
Org Unit	Use ··· **OU** on the right side of the attribute's box to enter an OU.
Hierarchy	If this check box is ticked, the search activity is for all the hierarchy. It starts from root OU that is indicated **Org Unit** .

Results are displayed in the same frame according to the following attributes:

Reviewer details	
Detail	**Description**
Action	◔ **Stats** monitors the status of the campaign completion. 🔍 **Inspect** inspects the entities of the campaign.
Master UID	Univocal identifier of the reviewer.
Name	Name of the reviewer.
Last Name	Surname of the reviewer.
OU Name [Code]	Name of the reviewers organizational unit.
% Entity Completion	Percentage of the Entities certified.

Clicking **Stats** displays the **Total items** and **Signed Off items** pie charts in the Stats window so you can monitor the campaign completion status.

If **Sign off** is set to **By User or Automatic**, the `No data to display` message is under **Signed Off**.

By clicking **Inspect**, the Supervisor can view approved or removed *Entities*.

Details for Supervisor - Accounts

Details provides information about the selected campaign and its activities.

The upper part of the frame provides information about the campaign, which is summarized in the following table:

Supervisor Campaign	
Details	**Description**
Campaign Name (link)	Name of the campaign.
Start Date	Start date of the campaign.
Sign Off	Validation mode for approval or revocation: **Automatic** The approval or revocation is immediately signed off. **By User** The user decides when to sign off the approval or revocation. **End Campaign** The approval or revocation is signed off at the end of the campaign.
Campaign Type	Type of campaign.
End Date	End date of the campaign.
% Completion	Percentage of certified entities.

Clicking **Campaign:** ***Campaign Name*** in the upper right part of the frame displays the Campaign Info window. The information is summarized in following tabs:

Campaign Detail	**Description**
Name	Name of the campaign.
Description	Brief description of the campaign.
Supervisor	Supervisors of the campaign (at least 1 supervisor).
Campaign Type	Type of campaign. • Entitlement • User assignment • Entitlement/OU visibility • Risk violation mitigation
Certification Dataset	Name of the data set that is built to feed or to start the campaign.

Campaign Detail	Description
Exclude Reviewed Since	If this check box is selected, the entities that were reviewed during the specified time are excluded by revision activity: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year
Notes Revocation (Mandatory)	If this check box is selected, the reviewer is required to specify notes for any revocation.
Allow Bulk Operations	If this check box is selected, the reviewer can use special commands for bulk approval/revocation actions.
Sign Off	Type of sign-off. • Automatic • Completed By User • End campaign
Activity Details	Attributes for an active campaign. • Start Date • End Date • Reviewers Signed Off/Total Reviewers K/N • *Entity* User Signed Off / Total *Entity H/M* Users • Working Progress J/TOT-M – N is the maximum number of reviewers – M is the maximum number of entities – TOT is the total number of pairs OU-Entitlement or User-Entitlement or User-Risk, depending on the campaign type

Table 425. Cert_Campaign_Reviewer_Tab

Reviewer Detail	Description
Scope	**User Hierarchy** If enabled, shows the available user hierarchy scope. It is always available for organizational units. **Entity** If enabled, shows the entity scope.
Default Reviewer	The default reviewer for the campaign.
Allow Redirection	If checked, approvals and revocations can be redirected to another reviewer
Escalation to Supervisor	If checked, approvals and revocations can be escalated to the supervisor of the campaign.
Exclusion list	Defines a list of reviewers that are excluded from the campaign. If enabled, you can use**Add** and **Remove** to define the reviewer list.

Fulfillment Detail	Description
Logical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are deleted but only logically.

Fulfillment Detail	Description
Physical deletion	If this option is selected, the entities-joins, for example, User-Role, in the fulfillment process are physically deleted, after a grace period if provided. Before the end of this period, data is available for any usage. For an immediate deletion, set `Grace period=0`. Campaigns on Account have the following options: • `Delete the Account` • `Lock the Account`
Physical deletion after workflow	If this option is selected, the entities-joins are deleted after a specified workflow, which is identified through the setting of *name Process - name Activity*.
Custom Behaviour	The management of the fulfillment involves a set of rules.

Table 426. Cert_Campaign_Scheduling_Tab

Scheduling Detail	Description
Activate On	**Start date** If checked, enables the workflow processes to define the frequency and length of the campaign. **Duration** The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • Continuous (never closed)
Execution Frequency	The following values are available: • 1, 2, or 3 weeks • 1, 2, 4, 6, or 9 months • 1 year • One time The set of values is bounded according to the **`Duration`** parameter. If `Duration=Continuous`, you cannot set values for this parameter.
Time Kept In History (Days)	Number of days to maintain the campaign data in the history.

Notification Type	Description
Campaign Started for Reviewer	If **Enable** is set, the reviewer receives an email when the campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information about the campaign.

Notification Type	Description
Activity Reminder for Reviewer	If **Enable** is set, the reviewer receives an email at the following times. • *K* days before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. • When the percentage of activity that is already managed is greater than X%. Determined by **Activity percentage** The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Reviewer	If **Enable** is set, the reviewer receives an email *K days* before the end of the campaign. Determined by **Days before end date**, where *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Campaign Reminder for Supervisor	If **Enable** is set, the supervisor receives an email *K days* before the end of the campaign. Determined by **Days before end date**, *K* is a value 0 - 32. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Continuous Review for Reviewer	If **Enable** is set, the reviewer receives an email when a continuous campaign begins. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.
Redirect	If **Enable** is set, the reviewer or supervisor receives an email in response to any action of redirection. The email is constructed according to **Email template**. If **Include campaign details** is set, the mail includes additional information on the campaign.

To search a specific Reviewer, set the filters shown in the following table by clicking **Filter/Hide Filter**:

Reviewer filters	
Filter	**Description**
Identity	Shows the **Name**, the **Surname** , or the **User ID** of the user.
Org Unit	Use ⋯ **OU** on the right side of the attribute to enter an OU.
Hierarchy	If selected, the search activity is on the hierarchy, which starts from root OU in **Org Unit** .

Results are displayed in the same frame by the following attributes:

Reviewer details	
Detail	**Description**
Action	**Stats** monitors the status of the campaign completion. **Inspect** inspects the entities of the campaign.
Master UID	Univocal identifier of the Reviewer.
Name	Name of the reviewer.
Last Name	Surname of the reviewer.
OU Name [Code]	Name of the organizational unit of the reviewer
% Entity Completion	Percentage of the Entities certified.

Clicking **Stats** displays the Stats window with the **Total items** and **Signed Off items** pie charts for campaign completion status monitoring:

If **Sign off** is set to **By User or Automatic**, `No data to display` is under **Signed Off items**.

By clicking **Inspect**, the Supervisor can view approved or removed entities.

Chapter 36. Introduction to User-account matching

User-account matching is the module that is dedicated to managing orphan accounts that are currently not matched with company policies.

The User-account matching user can do the following tasks:

- Join orphan accounts with users
- Decouple users and accounts

Dashboard

You can browse a number of Matching Dashboards, one for every target (application or external system) engaged.

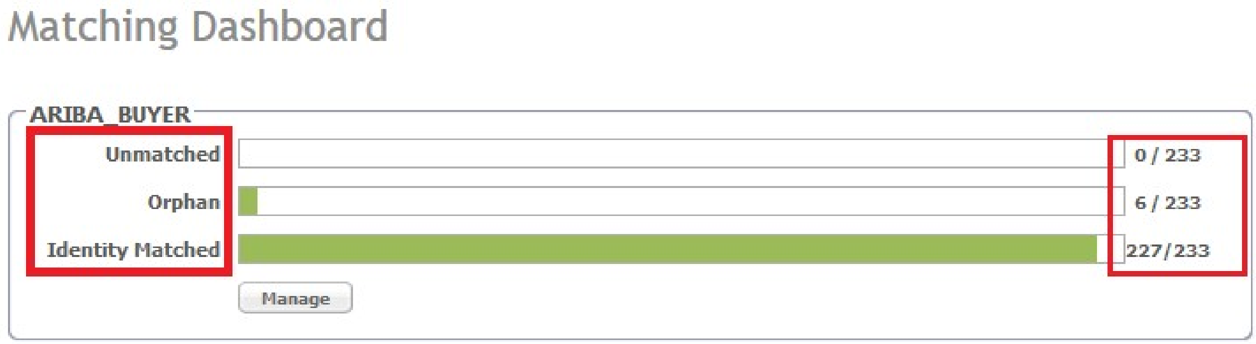


Figure 134. Application Accounts: Matching Dashboard

Every Matching Dashboard shows

Unmatched
The number of accounts that after the synchronization with the target system, are found not to match with company policies.

Orphan
The number of accounts that are not assigned to any user.

Identity Matched
The number of accounts that were assigned to a user by the action of the logged-in user.

Each of these numbers is shown over the total number of accounts that retrieved from the target.

To browse the details of the accounts, click **Manage** in the Dashboard you are viewing.

You can use the following filters to search for specific accounts (click **Filter**).

Table 427. User filters

Filter	Description
Application UID	The unique identifier of the application.

Table 427. User filters (continued)

Filter	Description
Status	The status of the account. • Unmatched • Orphan • Identity Matched
Master UID	The unique identifier of the user to whom the account is assigned.
Organization Unit	The organizational unit that is associated with the account. Click ··· **OU** to enter an OU.
Hierarchy	Flag this check-box to specify that the search is to be made on the entire organizational hierarchy that starts from the root OU specified in the **OU** field.

Note: The filters **Master UID** - **Organization Unit** - **Hierarchy** are enabled ONLY IF the filter **Status** is set to the value `Identity Matched`

The following details are displayed.

Table 428. User/Account attributes

Attribute	Description
Account details	Click ⓘ **Account details** for getting all the details that are related to the account.
Application UID	The unique identifier of the application.
Status	The status of the account. • Unmatched • Orphan • Identity Matched
Master UID	The unique identifier of the user to whom the account is assigned.
Name	The name of the user to whom the account is assigned.
Surname	
Email	The email address of the user to whom the account is assigned.
Distinguished Name	The Distinguished Name of the user to whom the account is assigned.
Display Name	Personal data of the user referred by **Master UID**.
Identity UID	Data incoming by a Target system and associated to the user referred by **Master UID** .

The **Actions** menu includes the following actions on an account that is selected from the list:

Permissions
Shows a list of permissions that are related to the account. If the target is

an external system, it displays a list of the last operations/events involving permissions on the target. This action is not available for matched accounts.

Orphan
Switches a matched account to the **Orphan** status. In other words, removes the association between the account and the user.

Match
Switches an **Orphan** or **Unmatched** account to the **Identity Matched** status. It displays the Match User window where you can select a user from the associated OU.

If the user you select has already an account on the application, another window asks if you want to create a secondary account (UME).

Details
Displays the User Details window with system and personal data of the user that is associated with the account. This action is not available for unmatched accounts.

Click the **Dashboard** tab to return from the detailed view of an application to the general view.

Chapter 37. Introduction to Access Requests

Access Requests (AR) is the module dedicated to running authorization processes.

In the Process Designer (PD) module, the IBM Security Identity Governance and Intelligence administrator defines workflows that implement customized sequences of activities that build authorization flows.

These authorization flows are then managed with Access Requests to assign operating permissions, such as business roles/IT roles/permissions/rights) to the users registered on the system.

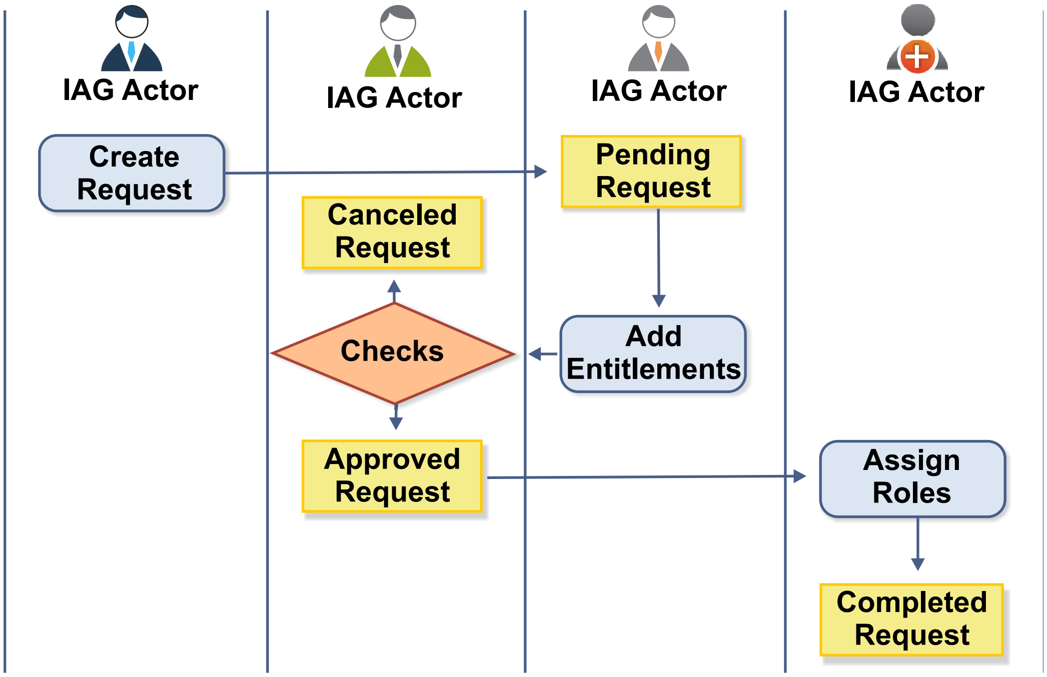


Figure 135. Example of authorization workflow

Access Requests directly communicates with Access Governance Core to execute the assignment/revocation of roles and the propagation of permissions on the target systems.

Access Requests provides the following functions:

- Create user entities
- Manage user accounts (Suspend/Restore account and reset password)
- Assign permissions to users
- Manage the assignment of administration roles
- Manage role delegation

ARM Requests Status

The requests that are generated during the authorization workflow activities can be characterized by various statuses.

They are summarized in the following table:

Table 429. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

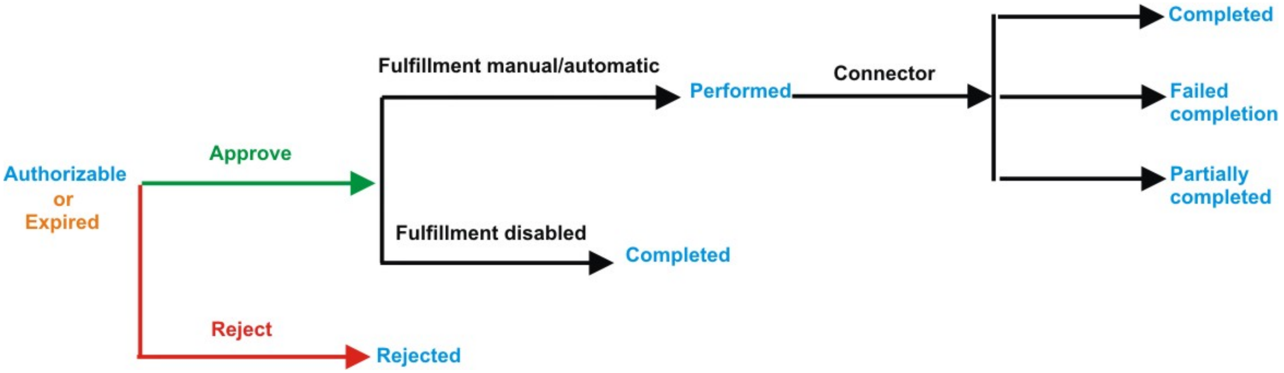


Figure 136. Subrequest status

Table 430. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

AR functions

Access Requests Manager provides several functions.

This module provides the following set of functions:
- “Selecting the user in a new request to make account changes” on page 744
- “Authorizing an account change request” on page 749
- “Executing a request for account change” on page 757
- “Selecting users in a new request to assign entitlements and roles” on page 762
- “Authorizing a request to assign entitlements and roles” on page 769
- “Executing a request to assign entitlements and roles” on page 777
- “Generating a request to delegate administrative roles” on page 783
- “Authorizing a request to delegate administrative roles” on page 783
- “Executing a request to delegate administrative roles” on page 783
- “Viewing requests in your Daily Work scope” on page 783

- “Viewing the requests present in the system” on page 842
- “Generating a request to delegate entitlements” on page 790
- “Authorizing a Delegation request” on page 795
- “Executing a Delegation request” on page 803
- “Insert/Update entitlement: generating a request” on page 813
- “Insert/Update entitlement: processing a request” on page 828
- “Insert/Updates entitlements: executing a request” on page 836
- “User access: generating a request” on page 849
- “User access: processing a request” on page 860
- “User access: executing a request” on page 868
- “Create/Update user: generating a request” on page 874
- “Insert/Update user: processing a request” on page 876
- “Insert/Update user: executing a request” on page 884
- “Authorize escalation” on page 809

Selecting the user in a new request to make account changes

Use this tab to generate a request to reset a user password or to suspend or restore a user account.

This tab starts a wizard that leads you through the steps of a work flow to generate the following types of requests:

- Reset the password of users who forgot their password and are unable to change it. Pre-configured wizards for the User manager and Help Desk administrative roles help you with the process.
- Suspend or restore the account of a selected user.

The Identity Governance and Intelligence Administrator can create similar work flows that respond to other business requirements.

The **User** tab is the first step of the wizard. You select the user on whose password or account you are about to act. You can use filters to search for specific users. The following filters are available:

Table 431. User filters

Filter	Description
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
First Name/Last Name/Master UID	The name or surname or the unique identifier of the user
Enabled	The user is enabled to be assigned entitlements
Activity	The business activity that the user is involved with. After the selection of the activity, you can flag **Hierarchy** to search also all the activities that are defined from this point down in the hierarchical structure.

Users are displayed in a table that shows the following attributes:

Table 432. Attributes in the Users list

Attribute	Description
Info	Click ⓘ **Info** to open the User details window. This window shows several user details like external data, assigned entitlements, assigned accounts, and rights.
First Name	The name of the user
Last Name	The surname of the user
User ID	The Unique identifier of the user
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
Group [Code]	The Organization Unit [Univocal identifier of the OU] to which the user belongs

To select a user, click a row.

Click ⓘ **Info** to show the Details window. The window includes several tabs. Some of the tabs might not be present depending on the properties that were defined for the user:

Table 433. User Information tabs

Tab	Description
Details	User information, including ID, type, organization, name, and address. This tab is always present.
External Data	Information that is taken from the User Virtual Attributes that are mapped from external databases in Access Governance Core.
Entitlements	A list of the entitlements that are assigned to this user. Click ⓘ **Info** for more information on an entitlement, its structure, the permissions that compose it, and the list of users and groups that are entitled to it.
Accounts	The list of accounts that this user can access. This tab is always present. Every user that is defined in Identity Governance and Intelligence must have access to at least the Ideas account.
Activities	Activities for the user. Activity access is based on assigned rights and entitlements. Click an activity to display a tree view of the hierarchical sequence.
Rights	A list of the rights that are assigned to this user.

After you select a user, click **Next**. Depending on the configuration of the work flow, this action displays the Security Questions window or the Accounts window.

Related tasks:

"Resetting account passwords for other users" on page 674
If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

Setting security questions in a new request to make account changes

Use this step in the wizard to verify the identity of the user who requested a password reset.

This window displays security questions to use to verify the identity of the beneficiary of the password reset. The items available depend on the choices for questions that were made by the Identity Governance and Intelligence administrator.

The window displays a number of security questions. A number specifies how many attempts the beneficiary is allowed to make before the account is locked.

A typical scenario for this work flow is one in which you get the answers from the beneficiary and enter them in this window in the user's place.

If the work flow configuration allows, you can also select the **Identified by other means** check box.

Click **Next** to proceed to the Accounts window.

Related tasks:

"Resetting account passwords for other users" on page 674
If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

Selecting accounts in a new request to make account changes

This step in the wizard is where you select the accounts to work on.

You can do one of the following actions:

Suspend or restore access of the beneficiary to one or more accounts

The upper part of the window summarizes information on the selected user and provides an entry field for adding request notes.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

The rest of the window lists the accounts that the user is entitled to access. Each row corresponds to an account. The 🔓 icon means that this account is unlocked. The 🔒 icon means that this account is locked.

You can click ⓘ to view the list of applications that are associated with the account and the details that are related to the account:

Table 434. Account details.

Detail	Description
Applications	Applications that are associated with the account configuration
Master UID	Identifies the user on the AG Core module
Account Expiration Date	After the expiration date, the policies that are configured for the account expiration are enabled (see **Manage** > **Account**). These policies are applied for all the users that are associated to the account that expired.
Last Login	Date of the last login
Last Login Error	Date of the last login error

Table 434. Account details. (continued)

Detail	Description
Number of Login Errors	Number of consecutive login errors. This value is reset to zero when a correct login is made.
Last Password Change	Date of the last password change
First Name	User name
Last Name	User surname
Email	Email address of the user. This information is used also from the policies that are related to account expiration.
DN	Distinguished Name of the user
Display Name	Personal data of the user as referred by **Master UID** .
Identity UID	Data incoming from a Target system and associated to the user who is referred by **Master UID** .
Account Attributes	A variable subset of account attributes. This subset is configured in **Manage** > **Accounts** > **Account Attributes**.

Note: In some views, only a subset of the data that is indicated could be shown.

Click **Close** to return to the account summary row.

Every account summary row includes a number of check boxes that describe a reason for suspending the access of this user to the account. If the account is unlocked, the check boxes are clear. If the account is locked, one or more check boxes are selected. The check boxes are:

Tech. Suspend
Access that is suspended for technical reasons.

Sec. Suspend
Access that is suspended for security reasons.

Terminated
Access that is suspended permanently.

Auth. Suspend
Access that is suspended because of authorization conflicts.

Expired
The expiration date that is defined for user was reached.

Maint. Suspend
Access is suspended because the account is under maintenance.

After you select the entire account, you can act on the account.

- Select one or more of the check boxes to suspend the user's access to the account or applications selected
- Clear the flagged check boxes to restore the user's access to the account or applications selected

Click **Submit** at the bottom to complete your account suspension/ restoration request for the beneficiary.

Provide a new password for the beneficiary to access one or more accounts

The upper part of the window provides information on the user you selected as the beneficiary of your password reset action.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

The rest of the window lists the accounts that the user is entitled to access. Each row corresponds to an account.

The 🔓 symbol means that this account is unlocked.

The 🔒 symbol means that this account is locked.

Select the check box in the title bar to select all the accounts that are listed or select the check box in account summary rows to select specific accounts. When you reset the password in the next step, the new password takes effect.

Click **Next** to proceed to the next step.

Related tasks:

"Resetting account passwords for other users" on page 674
If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

Entering the new password in a new request to make account changes

This final step of the wizard guides you to reset the password.

You are now in the Account Password Management window where you add the new password for the beneficiary. This step follows the steps where you selected the user for this action, verified the user's identity, and selected the accounts to which the new password is to grant access,

The appearance of the left portion of this window changes based on the configuration options that were chosen by the Identity Governance and Intelligence administrator for this type of request. This part of this window features the following items:

- **Applicant** section that includes the **Your Password** field, where you are prompted to enter your own password. This box is present if the Administrator configured the request so that your own identity is verified.
- **Beneficiary** section that includes the following items:
  - **New Password** and **Confirm Password** fields.

    You might see a **Generate** pushbutton on the right side of these fields. Select it to generate the password automatically. If **Generate** is not present, you are required to enter the new password. The password characters that you type are hidden. A **Show password characters** check box might be provided to help you view the password that you are typing.
  - A **New password will be sent to this email address** field. This field is not shown if the new password is to be communicated to the beneficiary by other means.

    If the field is present, you might enter or update the beneficiary's email address.

The right pane shows a checklist of syntax requirements for the new password. If you are entering the password manually, you see green check marks in the list become ⊗ if the requirements are ignored.

Click **Submit** to complete the request process.

The work flows that are provided with the product for password reset complete here. Click the **Request Report** tab to view information about your request, including type of request, the names of the applicant and of the beneficiary, and other information. The status of the request is declared to be completed.

If the work flow is configured to require authorization and other steps, the request is completed after those steps are carried out.

Related tasks:

"Resetting account passwords for other users" on page 674
If you are a manager, or someone entitled with a role that includes this activity, you can change the account passwords for users in the Service Center.

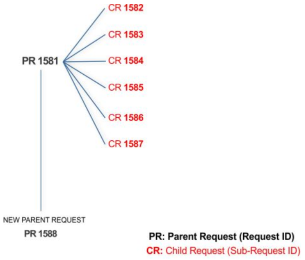
Authorizing an account change request

Authorizing an account change request.

You can view a summary of the generated requests. You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Requests**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the REQUEST REPORT EXE activity.

However, when you are logged-in as authorizator, some of the request (and sub-request) listed through the REQUEST REPORT EXE might not be visible because out of the scope defined for the authorizator.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 435. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

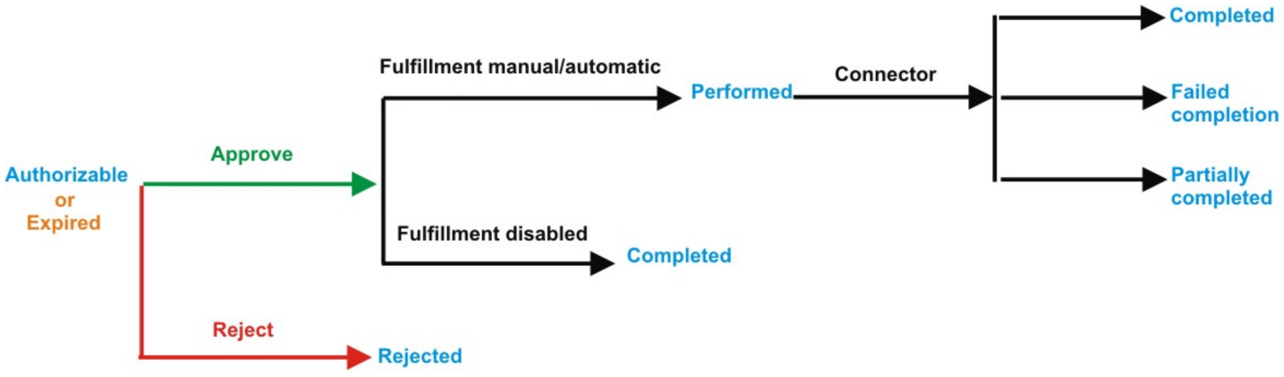


Figure 137. Subrequest status

Table 436. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization

Table 436. Subrequest status (continued)

Status	**Description**
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 437. Filters

Filter	**Description**
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	**Description**
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.

Requests attributes	
Attribute	**Description**
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.
Priority	The priority assigned to the request

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 438. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 439. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.

Table 439. Details of a request - upper section (continued)

Box	Details
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

Click the ⓘ **Info** icon to open the User details window and show the information in a set of tabs:

Table 440. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 441. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 442. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 443. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 444. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows the following information about the requests:

Table 445. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user

Table 445. Request attributes (continued)

Attribute	Description
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 446. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission
It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)
A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role
A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

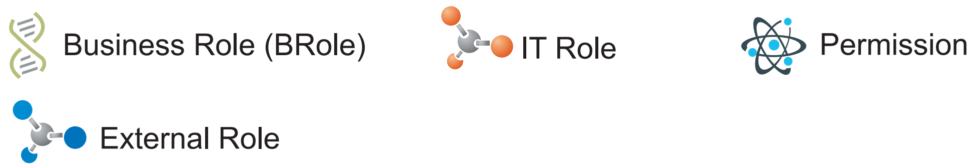
- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role
Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Executing a request for account change

You might get requests to reset a password for a user, to suspend or restore an account, or other actions.

Account Change requests might include an execution step. Based on the process setup, this step might be executed:

- Automatically through a connector
- Manually

Every request in the list displays two identification numbers:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, in black, is the parent request. Parent requests can have one or more **Sub-Requests** in red.

Depending on how the Account Change process is configured, a request has a Request Status from the following list:

Table 447. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific for requests with filters. Click **Filter/Hide Filter** and click **Search**.

Table 448. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

Requests are displayed with the following attributes:

Table 449. Request attributes

Attribute	Description
Request ID	Univocal identifier of the parent request
Sub-Request ID	Univocal identifier of the child request
Type	Type of request
Applicant	Name of the applicant of the request
Beneficiary	Name of the beneficiary of the request
Created on	Date (`dd/mm/yyyy`) and time (`hh:mm`) the request was created
Status	Request Status
Priority	The priority that is assigned to the request

Click **Applicant** or **Beneficiary** to open the User details window.

Table 450. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 450. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows information about the Request Actors:

Table 451. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The Request Notes are not mandatory. If no notes are present in the request, the fields of the Request Notes are blank.

Click the ⓘ **Info** icon to open the User details window.

Table 452. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 453. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 454. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 455. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 456. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows more request attributes.

Table 457. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to view the details of an entitlement. Information is displayed in a set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 458. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement

Table 458. Entitlement info - Structure (continued)

Detail	Description
Family	Family of the selected entitlement

If notes about the considered entitlement are in the request, the **Note** icon is available. Click it to open the Notes window.

When you finished processing a request, click the request and click **Execute** to mark the request as completed.

Selecting users in a new request to assign entitlements and roles

Use this type of requests to assign entitlements and roles to users.

The **Users** tab is the first step of the wizard. You can search and select users with the following filters. Click the **Filter**, enter one or more values, and then click **Search**.

Table 459. User filters

Filter	Description
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
First Name/Last Name/Master UID	The name or surname or the unique identifier of the user
Enabled	The user is enabled to be assigned entitlements
Activity	The business activity that the user is involved with. After the selection of the activity, you can flag **Hierarchy** to search also all the activities that are defined from this point down in the hierarchical structure.

Users are listed in a table that shows a number of attributes.

Table 460. Attributes in the Users list

Attribute	Description
Info	Click **Info** to open the User details window. This window shows several user details like external data, assigned entitlements, assigned accounts, and rights.
First Name	The name of the user
Last Name	The surname of the user
User ID	The Unique identifier of the user
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
Group [Code]	The Organization Unit [Univocal identifier of the OU] to which the user belongs

To select all the listed users, flag the check box in the attributes row. To select particular users, select the corresponding check boxes in the user rows.

Select ⓘ **Info** to display the User details window. This window shows additional information about the user in a number of tabs.

Table 461. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 462. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 463. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 464. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.

Table 464. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

Table 465. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Click the ⓘ **Info** icon to open the Entitlement information window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 466. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

Click **Next** to open the Catalog tab.

This tab is the second step of the wizard.

Selecting roles in a new request to assign entitlements and roles

The Catalog tab is the second step of the wizard.

In the **Catalog** page, you can choose the entitlements and roles for the users that you selected in the Users step of the wizard.

The upper part of the page summarizes the information about the selected users:

User data	
Data	**Description**
ⓘ Info	Click the **Info** icon to open the **Entitlement info** window.
First Name	Name of the user.
Last Name	Surname of the user.
User ID	Univocal identifier of the user.
Org. Unit [Code]	Name of the organizational unit and [Univocal identifier of the OU].
User Type	Type of user.
Risk Status 🔵 / 🟠 / 🔴	Click the colored dot to open a window that displays the following items: • The Risk Activities Tree (related to a specific user) in the **Risk Info** tab • The Activities that are involved in a specific risk, in the **Mitigations** tab

Click **Refresh** to update the risk situation of the user.

The lower part of the page shows a set of tabs:

- **Current Entitlements**
- **Business Roles**
- **Application Roles**
- **Permissions**

Depending on the configuration of the Activity, some of these tabs might not be present.

Current Entitlements tab

The **Current Entitlements** tab lists the entitlements that are assigned to the user. You can search (click **Filter/Hide Filter** and click **Search**) a specific entitlement with the filters that are shown next:

Table 467. Current Entitlement filters.

Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

You can run the following actions on the entitlements that are listed:

- **Remove** (Entitlement)
- **Validity** (End date of validity)

To remove an entitlement, click **Remove**.

To enter or change the validity of an entitlement, select **Validity**. In the Date Selection window, click **Calendar** to enter the end date, and click **OK** to confirm. The **Validity** pushbutton is highlighted in orange. To remove the end date, click **Validity**.

Next, select **Business Roles** to assign business roles, or **Next** to move to the Shopping Cart tab to process the request.

Business Roles tab

The **Business Roles** tab shows a list of available Business Roles for the selected user. Select **Filter**/**Hide Filter**, and click **Search**, to find specific business roles with any of the following filters:

Table 468. Business Role filters.

Filter	Description
Name	Name of the Entitlement.
Family	Family of the Entitlement.
Description	Brief description of the Entitlement.

Select **Add** to assign any of the listed business roles to the user. The **Add** pushbutton is highlighted in green.

If the added business roles have dependencies, the **Dependencies** pushbutton is displayed. Select it to open the Dependencies window, where you can add more dependencies.

To add dependencies, select **To Cart**, which is highlighted in green. Then, click **Ok** to confirm.

Dependencies can be defined and associated with roles. Dependencies are permissions or roles that are necessary, or useful, to other roles.

For example, a role that is named `TECHComm`, with all the specific permissions for this position, is being defined for an employee who is to take a position as technical writer.

The technical writer reviews the draft documents that are produced by the Product Managers. They are shared in a company repository that is named `DraftsOnProducts`, which is a dedicated database, linked to a permission named `DraftsOnProdcuts_Reader`.

The `DraftsOnProdcuts_Reader` permission can be considered as a dependency of `TECHComm`.

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

Next, select **Application Roles** to assign applications roles, or **Next** to move to the Shopping Cart tab to process the request.

Application Roles tab

You can assign application roles to the user in the Application Roles section. Application roles are also known as IT roles.

In the **Application Roles** tab, the Applications window opens by default. Select an application from the list to display a list of application roles in the **Applications Roles** tab. Close the Applications window to exit from it.

You can also select **Filter/ Hide Filter** and use any of the following filters to search for specific application roles:

Table 469. Application Role filters.

Filter	Description
Application	Name of the Application.
Family	Family of the Entitlement.
Name	Name of the Entitlement.
Description	Brief description of the Entitlement.

Click **Add** next to the application roles that you want to assign to the user. The **Add** pushbutton is highlighted in green.

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

Next, select **Permissions** to assign permissions, or **Next** to move to the Shopping Cart tab to process the request.

Permissions tab

You can assign permissions to the user in the Permissions section.

In the **Permissions** tab, the Applications window opens by default. Select an application from the list to display a list of permissions in the **Permissions** tab. Close the Applications window to exit from it.

You can also select **Filter/ Hide Filter** and use any of the following filters to search for specific permissions:

Table 470. Permission filters.

Filter	Description
Application	Name of the Application.
Permission Type	Type of Permission.
Name	Name of the Entitlement.
Description	Brief description of the Entitlement.

Click **Add** next to the permissions that you want to assign to the user. The **Add** pushbutton is highlighted in green.

The **Actions** menu includes the following items:

- **All Roles** Click to choose from the full set of available roles to assign to a selected user.
- **Like Mike** Click to assign to a selected User the same roles of another user that you choose from the full set of users.

Select **Next** to move to the Shopping Cart tab to process the request.

Reviewing your new request to assign entitlements and roles

The **Shopping Cart** page displays a summary tree structure of the new request.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

The **Operation** column lists the operations that you specified in the previous page. They can be one of the following operations:

- **Add**
- **Remove**
- **Change** (refers to the **Validity** change in the Current Entitlements tab)

If you click ⊗ **Clear**, the operation is revoked and is excluded from the request.

The **Name** column lists the entitlements that are impacted by the operations.

If the entitlement is a **Permission**, it can have one or more associated ⚙ **Rights**. You can assign a **Value** to each right.

A Right is defined by two attributes: Key and Value.

The Key attribute is an identifying name, while the Value attribute can be defined each time. A configurable default value can be provided for the Value attribute.

Rights can be of the following type:

- Single-value
- Single-value with lookup
- Multi-value
- Multi-value with lookup

With a single-value Right with lookup, you can choose a single value Vx from a set of several values (V1,V2, ... VN)

With a multi-value Right with lookup, you can choose a subset of values (Vx,Vy,Vz,...) from a larger set of values (V1,V2, ... VN).

When a Right is with Lookup, a ... **Browse** pushbutton is available nearby. Click it to display the **Rights** window, where you can select values.

The **Application** column lists the name of the applications to which the entitlements belong.

The presence of the **Visibility Violation** icon in the **VV** column, denotes an entitlement in Visibility Violation.

An entitlement is in VV when it is not associated to the OU, but is assigned to a single user of that OU. The entitlement is not available to the other users of the OU.

The following pushbuttons might be enabled for each entitlement. They are displayed next to the VV column.

Table 471. Pushbuttons and Icons in the Shopping Cart page.

Button/Icon	Description
Notes	Opens the Notes window, where you can write remarks for the operation.
Validity	Opens the Date Selection window, where you can enter the **Start Date** and the **End Date** of the role assignment.
Pushbuttons and Icons available only for the Admin Access Request	
Application resources	Opens the Resource Assign window, where you can select one or more **Applications** for assignment.
OU resources	Opens the Resource Assign window, where you can select one or more **Organization Units** for assignment.
BRole resources	Opens the Resource Assign window, you can select one or more **Business Roles** for assignment.
Risk resources	Opens the Resource Assign window, where you can select one or more **Risks** for assignment.
Attribute Hierarchy resources	Opens the Resource Assign window, where you can select an **Attribute Hierarchy** for assignment.

The **New Start Date** and **New End Date** columns list the dates that are defined with **Validity**.

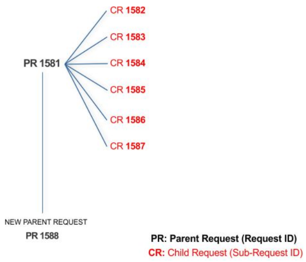
Authorizing a request to assign entitlements and roles

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the example, **Request ID 1581** generates the six **Sub-Request ID**s that range from 1582 to1587.

You can view all the requests that are registered by the Request Report activity. When you are logged-in as approver, some of the requests and subrequests might not be visible because they are out of the scope that was defined for an approver.

The submitted requests are listed in one of the following statuses:

Table 472. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

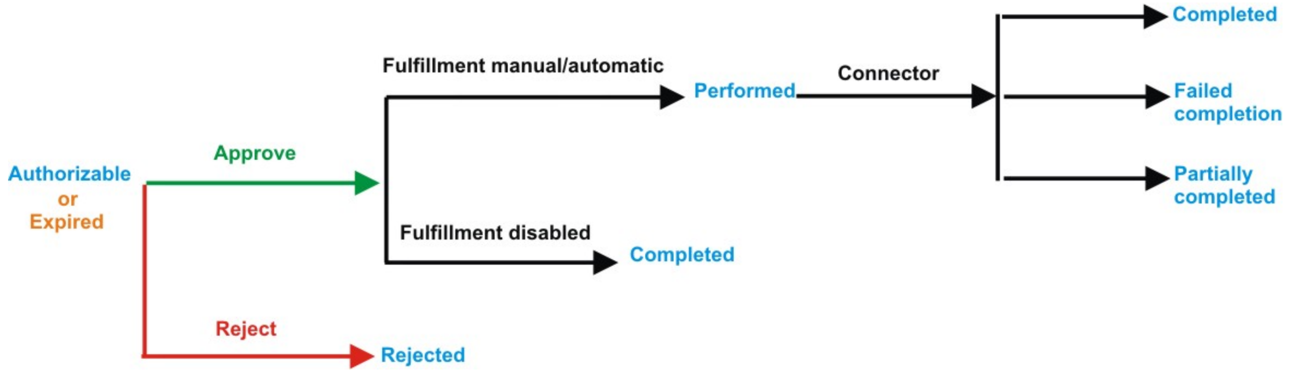


Figure 138. Subrequest status

Table 473. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 474. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest

Table 474. Filters (continued)

Filter	Description
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

Requests are displayed with the following details:

Table 475. Request details.

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and view the following information:

Table 476. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the page shows the following information about the **Actors of the Request**:

Table 477. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The request notes are not mandatory. If no notes are in the request, the fields in **Request Notes** are blank.

Click the ⓘ **Info** icon to open the User details window and view the information in a set of tabs:

Table 478. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user

Table 478. User Details - Details tab (continued)

Detail	Description
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 479. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 480. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 481. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 482. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.

Table 482. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the page shows the following information about the requests:

Table 483. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement information window and view the information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 484. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:

Business Role (BRole)
IT Role
Permission
External Role

If an entitlement has request notes, the **Notes** icon is available. Click it to open the Notes window and show the contents of the note.

In the center of the page, you find:

- Elements that are related with the request that needs to be authorized.
- Elements that are related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve

Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Executing a request to assign entitlements and roles

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.

The requests that were submitted in the system are listed in one of the following statuses:

Table 485. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress

Table 485. Request Status (continued)

Status	Description
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 486. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

Requests are displayed with the following details:

Table 487. Requests attributes.

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and view the following information:

Table 488. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the page shows the following information about the **Actors of the Request**:

Table 489. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.

Table 489. Details of a request - upper section (continued)

Box	Details
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The request notes are not mandatory. If no notes are in the request, the fields in **Request Notes** are blank.

Click the ⓘ **Info** icon to open the User details window and view the information in a set of tabs:

Table 490. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 491. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user

Table 491. User Details - Entitlements tab (continued)

Details	Description
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 492. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 493. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 494. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the page shows the following information about the requests:

Table 495. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement information window and view the summarized information in the following set of tabs:

- **Details**

- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 496. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

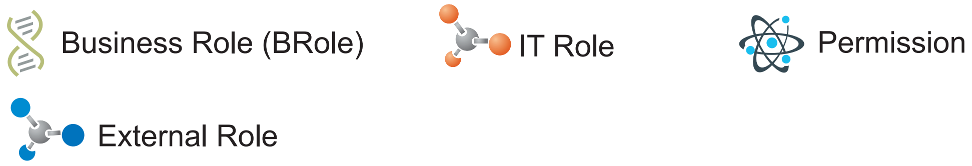
Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)

- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the **Notes** icon is available. Click it to open the Notes window and show the contents of the note.

Generating a request to delegate administrative roles

You can submit a request of delegation only for Administrative Roles.

The scope of this activity is limited to Administrative Roles. The procedure that you follow is similar to the one that you follow for delegating common roles.

The activity follows three steps:

- Select the user who delegates (Delegator)
- Select the users who are delegated (New Delegation)
- Select the administrative role to delegate (Catalog)

Authorizing a request to delegate administrative roles

You can view a summary of the requests to delegate an administrative role that were submitted. From this list, you can act on the ones that await your approval.

The scope of this activity is limited to Administrative Roles. The procedure that you follow is similar to the one that you follow for delegating common roles. See Authorizing a Delegation request.

Executing a request to delegate administrative roles

You can view a summary of the requests to delegate an administrative role that were submitted. From this list, you can operate on the ones that await your action.

The scope of this activity is limited to Administrative Roles. The procedure that you follow is similar to the one that you follow for delegating common roles. See Executing a Delegation request.

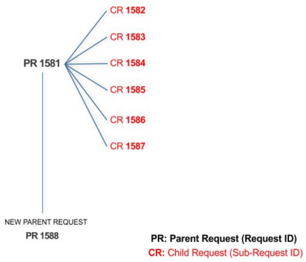
Viewing requests in your Daily Work scope

You can view a summary of generated requests that are in your scope.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are in red.



In the example, **Request ID 1581** generates the six **Sub-Request ID**s that range from 1582 to1587.

You can view all the requests that are registered by the Request Report activity. When you are logged-in as approver, some of the requests and subrequests might not be visible because they are out of the scope that was defined for an approver.

The requests that were submitted are listed in their status. A request can be in one of the statuses that are described in the following table:

Table 497. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

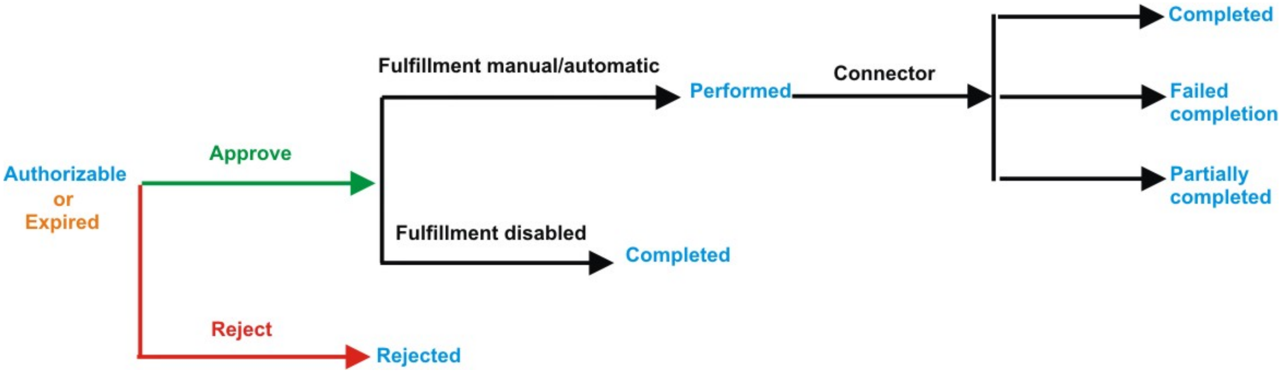


Figure 139. Subrequest status

Table 498. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 499. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest

Table 499. Filters (continued)

Filter	Description
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

Requests are displayed in the same page and include the following attributes:

Table 500. Request attributes.

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and view the following information:

Table 501. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the page shows the following information about the **Actors of the Request**:

Table 502. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The request notes are not mandatory. If no notes are in the request, the fields in **Request Notes** are blank.

Click the ⓘ **Info** icon to open the User details window that shows information in a set of tabs:

Table 503. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user

Table 503. User Details - Details tab (continued)

Detail	Description
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 504. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ! icon denotes an entitlement in Role Alignment Violation

Table 505. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 506. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 507. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.

Table 507. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the page shows the following information about the requests:

Table 508. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement information window and view the information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 509. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

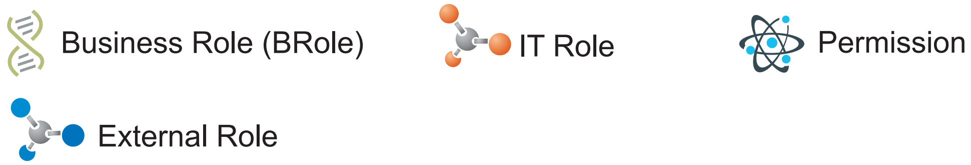
Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the **Notes** icon is available. Click it to open the Notes window and show the contents of the note.

Generating a request to delegate entitlements

You can generate a request to delegate an entitlement to a user. Then, you submit the request to the user who authorizes it.

The **Delegator** tab is the first step of the wizard, where you select the user whose entitlements must be temporarily delegated to someone else.

Note: Use the **Delegator** tab only for the complete activity of delegation (delegation of entitlements of a User A to a User B). The "personal delegation" activity, consisting in the action of delegating one's entitlements to another user, starts from the Delegate tab.

You can search and select users by clicking **Filter/Hide Filter** and then **Search**. The following filters are available:

Table 510. User filters

Filter	Description
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
First Name/Last Name/Master UID	The name or surname or the unique identifier of the user
Enabled	The user is enabled to be assigned entitlements
Activity	The business activity that the user is involved with. After the selection of the activity, you can flag **Hierarchy** to search also all the activities that are defined from this point down in the hierarchical structure.

The delegators are displayed with the following attributes:

Table 511. Attributes in the Users list

Attribute	Description
Info	Click ⓘ **Info** to open the User details window. This window shows several user details like external data, assigned entitlements, assigned accounts, and rights.
First Name	The name of the user
Last Name	The surname of the user
User ID	The Unique identifier of the user
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
Group [Code]	The Organization Unit [Univocal identifier of the OU] to which the user belongs

To select the entire list of users, select the check box on the attributes row, otherwise select the check box that corresponds to the user row.

Click ⓘ **Info** to display a user's Details window, which displays the following information in a set of tabs:

Table 512. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user

Table 512. User Details - Details tab (continued)

Detail	Description
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 513. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 514. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 515. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

Table 516. User Details - Activities tab

Detail	Description
Name	Name of the activity

Table 516. User Details - Activities tab (continued)

Detail	Description
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Click ⓘ **Info** in the **Entitlement** tab to display the Entitlement information window, which displays the information summarized in the **Structure** tab:

Table 517. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:

Business Role (BRole) IT Role Permission

External Role

Click **Next** to display the Delegate pane.

This tab is the second step of the wizard, where you select the users for the delegator's entitlements.

Selecting delegates for a delegator's entitlements

The **Delegate** tab is the second step of the Delegation wizard.

Use the Delegate pane to select the users to whom the delegator's entitlements are to be temporarily assigned.

The upper part of the pane displays information about the delegator user or about the user who is logged in for personal delegation.

The lower part of the pane displays a list of the users from which you can select the delegates. Select **Filter** to narrow the search to specific users.

To select the entire list of users, select the check box on the attributes row, otherwise check the one in the row of a particular user.

Click **Next** to move to the Catalog pane.

This tab is the third step of the wizard, where you select the entitlements to delegate and submit the request to a user who has the authority to accept it.

Selecting entitlements in the Catalog tab

The **Catalog** tab is the third step of the wizard.

In the Catalog page, you choose the entitlements of the Delegator user that you want to delegate to the users that you selected in the Delegate step.

The upper part of the page summarizes the information about the delegator and the delegates. The section that provides the delegate information shows also the level of incompatibility that is involved in selecting the users that are listed:

✓ The user is free of risk.

🔵 The level of risk that is attributed to the user is low.

🟠 The level of risk that is attributed to the user is medium.

🔴 The level of risk that is attributed to the user is high.

The lower part of the page includes the following tabs:

Select Roles for Delegation
A list where you select the Delegator's entitlements that you want to assign to the delegates. Click **Filter** to search for specific entitlements.

Delegated Roles
A list that includes any entitlements that the Delegator and the Delegates already share.

The page includes also:

- The **Priority** field, where you can set a priority level for the request. This field might not be enabled, based on the setup of this type of requests.
- A **Request Notes** field for optional remarks.

When you are ready to generate the request, click **Submit**. Then, click **Ok** on the confirmation window that follows. The new request is displayed in the Service Center session of the assignee of the administrative role that authorizes Delegation requests.

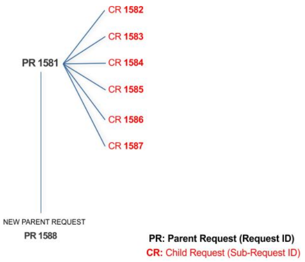
Authorizing a Delegation request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the example, **Request ID 1581** generates the six **Sub-Request ID**s that range from 1582 to1587.

You can view all the requests that are registered by the Request Report activity. When you are logged-in as approver, some of the requests and subrequests might not be visible because they are out of the scope that was defined for an approver.

The requests that were submitted are listed in their status. A request can be in one of the statuses that are described in the following table:

Table 518. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization

Table 518. Request Status (continued)

Status	Description
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

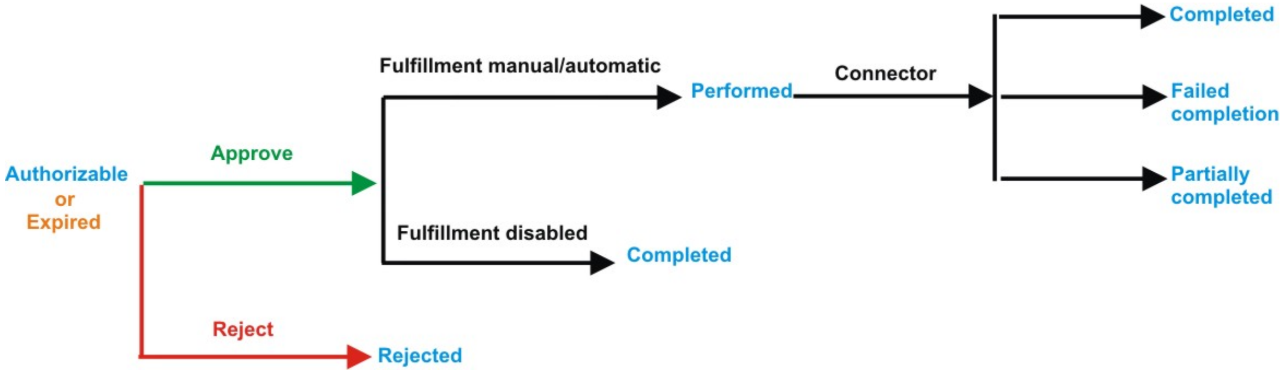


Figure 140. Subrequest status

Table 519. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization

Table 519. Subrequest status (continued)

Status	Description
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 520. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

Requests are displayed in the same page and include the following attributes:

Table 521. Request attributes.

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.

Table 521. Request attributes. (continued)

Attribute	Description
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.
Priority	The priority that is assigned to the request

Click **Applicant** and **Beneficiary** to open the User details window and view the following information:

Table 522. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the page shows the following information about the **Actors of the Request**:

Table 523. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.

Table 523. Details of a request - upper section (continued)

Box	Details
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The request notes are not mandatory. If no notes are in the request, the fields in **Request Notes** are blank.

Click the **Info** icon to open the User details window that shows information in a set of tabs:

Table 524. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 525. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 526. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 527. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 528. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the page shows the following information about the requests:

Table 529. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user

Table 529. Request attributes (continued)

Attribute	Description
VV	The ! icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement information window and view the information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 530. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

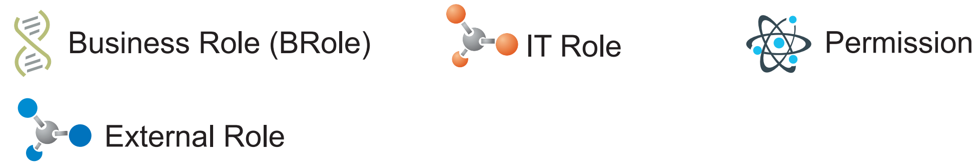
- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role
Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the **Notes** icon is available. Click it to open the Notes window and show the contents of the note.

In the center of the page, you find:

- Elements that are related with the request that needs to be authorized.
- Elements that are related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Executing a Delegation request

You can view a summary of the authorized requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.

The requests that were submitted are listed in their status. A request can be in one of the statuses that are described in the following table:

Table 531. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter**, enter your data, and click **Search**.

Table 532. Filters

Filter	Description
Request ID	The Unique identifier of the request

Table 532. Filters (continued)

Filter	Description
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

Requests are displayed in the same page and include the following attributes:

Table 533. Request attributes.

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.
Priority	The priority that is assigned to the request

Click **Applicant** and **Beneficiary** to open the User details window and view the following information:

Table 534. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 534. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the page shows the following information about the **Actors of the Request**:

Table 535. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The request notes are not mandatory. If no notes are in the request, the fields in **Request Notes** are blank.

Click the ⓘ **Info** icon to open the User details window and show the information in a set of tabs:

Table 536. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 537. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 538. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 539. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree

Table 539. User Details - Activities tab (continued)

Detail	Description
Description	Brief description of the activity

Table 540. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the page shows the following information about the requests:

Table 541. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement information window and view the information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement in the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 542. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement

Table 542. Entitlement info - Structure (continued)

Detail	Description
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission
It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)
A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role
A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

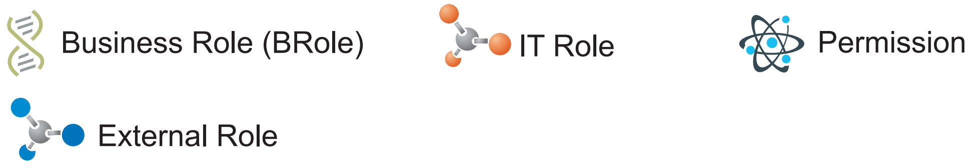
- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role
Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If an entitlement has request notes, the 📄 **Notes** icon is available. Click it to open the Notes window and show the contents of the note.

Authorize escalation

The Risk Manager provides several operations for user risks.

After you make a request, the Risk Manager processes the user risk that is generated by a request.

In the **Authorize Escalation** tab, you can view a summary of the generated risk requests.

You can search specific requests with the following filters. Click **Filter**, enter your search data in the filter fields, and click **Search**.

Table 543. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

Requests are displayed with the following details:

Table 544. Request details.

Attribute	**Description**
Request ID	Univocal identifier of the parent request
Applicant	Name of the applicant of the request
Beneficiary	Name of the beneficiary of the request
Type	Request type
Created on	Day (`dd/mm/yyyy`) and time (`hh:mm`) when the request was submitted
Priority	Priority that is assigned to the request

Click **Applicant** and **Beneficiary** to open the User details window and view the following information:

Table 545. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** to view the details.

The upper part of the frame displays the following information about the **Actors of the Request**:

Request Actors		
Actor	**Detail**	**Description**
Request	**Request ID**	Univocal identifier of the Request
	Status	the request is in `Escalation` status
	Priority	Priority that is assigned to the request
	Created on	Date (`dd/mm/yyyy`) and time (`hh:mm`) when the request was submitted
	Type	Type of request
	Risk Status	The risk status of the request. The level of risk is indicated by one of the following colored dots: 🔵 Low 🟠 Medium 🔴 High Click the colored dot to open a window that displays the following items: • The Risk Activities Tree (related to a specific user) in the **Risk Info** tab • The Activities that are involved in a specific risk, in the **Mitigations** tab
Applicant/ **Beneficiary/** **Delegator**	**Group**	Organization Unit (OU) of the **Applicant**, **Beneficiary**, or **Delegator**.
	First Name	Given name of the **Applicant**, **Beneficiary**, or **Delegator**.
	Last Name	Surname of the **Applicant**, **Beneficiary**, or **Delegator**
	User ID	Univocal identifier of the **Applicant**, **Beneficiary**, or **Delegator**. Click the ⓘ **Info** icon to view user details, and lists of entitlements, accounts, business activities, and rights assigned to the user.
Additional Notes	A space for more notes about the request.	

Click ⓘ **Info** in the Request box in the upper part of the page to display the Incompatibility Info window. It has the following tabs:

- **Risk Info**
- **Mitigation**

The **Mitigation** tab in the lower part of the page shows the mitigations that are already assigned to the user.

- At the first level, there is a set of risks.
- At the second level for every risk, there is the set of At-Risk Activities in which the user is involved; it might also display aggregated mitigations.

For information related to the Service Center mitigation configuration user interface, see “How to read the tree of the risks of a user” on page 36.

The lower left part of the page displays the following information:

Table 546. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ! icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Select the ⓘ **Info** icon to open the Entitlement info window, where the following tabs provide more information:

- **Structure**
- **Dependencies**
- **Activity**
- **Rights**

The **Structure** tab is always available. It shows the structure of the Entitlement of the Request. The other tabs are available only when the Entitlement is characterized by **Dependencies**, **Activities**, or **Rights**.

If notes about entitlements are in the request, the **Note** icon is available. Click it to open the **Notes** window and read the note.

The lower right part of the page shows information about the mitigations that are assigned to the user by the Risk Manager. **Control Name** is the name of the mitigation; **Description** is brief description of the mitigation.

Select one of the following actions:

- **Back** returns to the summary of the generated Risk Requests.
- **Approve** approves a request.
- **Reject** rejects a request.
- **Viol. Info** displays the Risk tree, and you can assign the appropriate mitigation to the risk.

After the appropriate mitigation is assigned to the user risk, it is visible in the lower right part of the frame.

Insert/Update entitlement: generating a request

You can insert a new user or update information for a registered user.

- Insert Entitlement
- Update Entitlement

Insert entitlements: generating a request

Use this workflow to create roles.

From the **Create Role** tab, you can select two more tabs:

Role Mining
Use it to discover roles

Data Exploration
Use it to collect information on the current status of User-Entitlements associations

If you first select **Data Exploration**, you are then lead to select the **Role Mining** tab.

In the **Role Mining** tab, every role mining analysis is described by fields arranged in a row.

Click **Filter** and use the items described in the next table to find one or more analyses:

Table 547. Analysis filters.

Filter	Description
Analysis Description	A descriptive text of the analysis.
Organization Unit	Click … **Browse** to choose the OU in the analysis.
Application	Click … **Browse** to choose the Application in the analysis.
Entitlement Type	Indicates the entitlement types. • Permission • IT Role • Business Role • External Role

Table 547. Analysis filters. (continued)

Filter	Description
Status	Indicates the status of the analysis. • ✓ Indicates in progress. • ✓ Indicates complete. • ✗ Indicates an error. • ! Indicates invalidated due to a new bulk load.
User/Entitlement Attributes	If present, according to the current configuration.

The details provided in each row of data belonging to an analysis are the totality of the ones described in the preceding table, with two important additions.

Click ⓘ **Info** to get the complete set of analysis information.

Use the **Actions** menu to run the following actions in this context:

Add To define a role mining analysis.

Remove
To delete a selected role mining analysis row.

Follow these steps to create a role after selecting an analysis:

1. Click **Next** to access the next wizard step in the **Candidate Roles** pane.

   The left frame includes the following tabs:

   - Roles
   - Entitlements
   - Users
   - Statistics tab

   The selection of one of these tabs displays in turn another set of tabs in the right frame.

   The main task that you can run in this step is to choose a candidate role of preference.
2. Click **Next** to gain access to the next wizard step in the **Impact Analysis** pane.

   The main functionality (**Structure - Permission - Users - Risk Info** tabs) available in the **Impact Analysis** pane allows you to:

   - Modify the selected candidate role to match OU needs
   - Simulate the effect of a candidate role after being imported into an organization.
3.

   Click **Next** to gain access to the next wizard step in the **Entitlements Details** pane.
4. Finally, select **Summary** to display the candidate role that you can submit to the authorization process by clicking the **Submit** button.

In this pane, **Priority** declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

User analysis: This section provides several ways of investigating the nature and structure of Candidate Roles from a User approach.

You can use the filters shown in the table below to help you find Users (click on **Filter**):

Table 548. User filters.

Attribute	Description
Master UID	Univocal identifier of the User
Last Name	Surname of the User.
First Name	Name of the User.
Organization Unit	Indicates the OU in which the User is registered.
Hier.	Flag this check box to get the tree view of the Organization unit.
Entitlement Coverage	This filter can assume three distinct values: • ◌ **Out of Role**: the User is not aggregated to any Entitlement through the Candidate Roles. • ◕ **Partially covered**: the User is aggregated only to a subset of Entitlements through the Candidate Roles. • ● **Covered**: the User is aggregated to ALL Entitlements through the Candidate Roles.

Upon selecting a User in the **Users** tab on the left, the **User Details** tab, on the right, is shown by default with the relevant information, distinguished in the following groups: **User - Entitlements - Applications**.

Table 549. User details.

User	
Attribute	**Description**
Last Name	Indicates the User's last name
Name	Indicates the User's name
User ID	Indicates the User's User ID
Organization Unit	Indicates the OU in which the User is registered
Entitlements	
Entitlements	Indicates the number of Entitlements assigned to the selected User
Entitlement Support (%)	Indicates the percentage of Entitlements that should be assigned to the User from the entire set of Entitlements involved in the Request

Table 549. User details. (continued)

User	
Attribute	**Description**
Covered Entitlements	Indicates the number of Entitlements assigned to the User
Entitlement Coverage (%)	Indicates the percentage of Entitlements actually assigned to the User from the entire set of Entitlements that should be assigned to the User
Applications	
Applications	Indicates the number of Applications involving the selected User
Application Support (%)	Indicates the percentage of Applications that should be assigned to the User from the entire set of Applications involved in the Request
Covered Applications	Indicates the number of Applications assigned to the User
Application Coverage(%)	Indicates the percentage of Applications actually assigned to the User from the entire set of Applications that should be assigned to the User

The other operations for User analysis are:

- Entitlements assigned to the selected User
- Applications assigned to the selected User

Role analysis:

The Role Mining tab contains many features for investigating the structure of the candidate roles indicated by the analysis.

The left frame contains four tabs:

- Roles (default active tab)
- Entitlements
- Users
- Statistics

In the **Roles** tab, the candidate roles are characterized by a set of statuses, according to the role position in the operational flow managed by the role engineer.

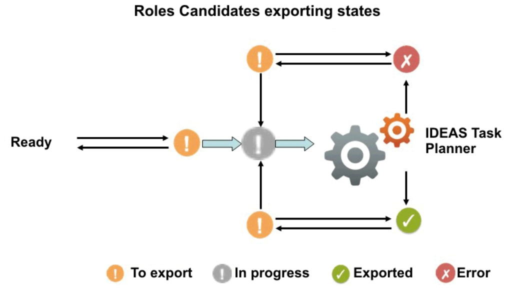


Figure 141. Possible states of candidate roles.

The main goal of Role Mining activity is to identify and import candidate roles, into "Enterprise" roles set (AG Core database).

Click **Filter** to filter candidate roles according to their names.

Each candidate role row presents the attributes shown below:

For any candidate role selected in the **Roles** tab, in the right pane you can select several tabs.

In particular, in **Roles Details** tab are shown all the characteristics of the candidate role, grouped for entity:

Table 550. Entitlement details.

Detail	Description
Role Name	Name of role
Rep. Status	Status of the role
Application	Name of the application.
Application Support (%)	Percentage of application to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
Entitlements	Name of the entitlement.
Entitlements Support (%)	Percentage of entitlements to be assigned to the candidate roles, from the entire set of entitlements involved in the analysis.
Users	Number of users assigned to the selected role.
User Support (%)	Percentage of users to be assigned to the role, from the entire set of users involved in the analysis.
Org Units	Number of organization units involved in the selected role.
Org Unit Support (%)	Percentage of organization units to be assigned to the role, from the entire set of organization units involved in the analysis.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.

Table 550. Entitlement details. (continued)

Detail	Description
Minimum Farness	Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness.
Average Farness	Average distance of all OUs from the centroid of distribution. See Farness.
Average Coverage (%)	Average percentage of OUs assigned with the entitlement.
Maximum Coverage (%)	Maximum percentage of OUs assigned with the entitlement.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the section Entitlement attributes.

In the“Role map” on page 472, is shown the map of the candidate role.

Four other tabs (**Entitlements**, **Applications**, **Users**, **Organization Units**) can be selected for showing the related entities involved with the candidate role selected.

Finally, the **Impact Analysis** tab allows you to evaluate the changes involved in the organization if you are going to import the candidate role into "Enterprise" roles set (AG Core database).

Entitlements analysis:

This section contains many useful features for investigating the structure of the Candidate Roles from an Entitlement approach.

Entitlements are characterized by the following icons (✓ , ✓ , ○) related to the concept of "User coverage". Entitlements can be filtered (clicking **Filter**) using the filters described in the table below:

Table 551. Entitlement filters

Attribute	Description
Name	Indicates the name of the entitlement.
Entitlement Type	The entitlement can be one of the following: • : **Permission** • : **IT role** • : **Business role** • : **External role**
Application	Name of the application.

Table 551. Entitlement filters (continued)

Attribute	Description
User Coverage	This filter can assume three different values: • ○ Out of Role: the entitlement cannot be assigned to any qualified user using the candidate roles. • ✓ Partially covered: the entitlement can be assigned only to a subset of qualified users using the candidate roles. • ✓ Covered: the entitlement can be assigned to all qualified users using the candidate roles.

Upon selecting an entitlement in the **Entitlements** tab on the left, the **Entitlements Details** tab is by default shown on the right with the relevant information. The information is organized in the following groups: **Entitlements - Users - Organization Units**.

Table 552. Entitlement details

Attribute	Description
Application	Name of the application.
Entitlement Name	Name of the entitlement.
Users	Number of users assigned to the selected entitlement.
User Support (%)	Percentage of users that have the entitlement from the entire set of users that must have the entitlement.
Covered Users	Number of users covered with the entitlement.
User Coverage (%)	Percentage of users in the OU who are assigned to the entitlement.
Org Units	Number of organization units involved in the selected entitlement.
Org Unit Support (%)	Percentage of organization units to be assigned to the entitlement, from the entire set of organization units involved in the analysis.
Covered Org Units	Number of organization units covered with the Role entitlement.
Org Unit Coverage(%)	Percentage of organization units that are assigned with the entitlement, from the entire set of organization units that must be assigned with the entitlement.
OU Spread	OU Spread indicates the inclination towards obtaining a very scattered or localized entitlement distribution in the OU hierarchy. See Spread.

Table 552. Entitlement details (continued)

Attribute	Description
Minimum Farness	Minimum distance between an OU and the centroid of distribution, rather than between an OU and a particular attribute such as an entitlement. See Farness.
Average Farness	Average distance of all OUs from the centroid of distribution. See Farness.
Average Coverage (%)	Average percentage of OUs assigned with the entitlement.
Maximum Coverage (%)	Maximum percentage of OUs assigned with the entitlement.
Attribute 0... Attribute 9 (for Entitlements)	Attributes configured in the Entitlement attributes section.

The other operations for Entitlements analysis are:

- Users aggregated with the selected Entitlement
- OUs aggregated with the selected Entitlement

Users aggregated with the selected entitlement

The **Users** tab lists all candidate roles containing the entitlement previously selected in the **Entitlements**tab.

For each candidate role, the data set in the table below is displayed:

Table 553. Candidate Role attributes

Attribute	Description
Role Name	Indicates the name of the role.
Exportation (Report/Release)	The role can have one of the following statuses: • ! **Scheduled to be exported** • ! **Exportation in progress** • ✓ **Successfully exported** • ✗ **Error**
Users	Indicates the number of users for the selected candidate role.
Entitlements	Indicates the number of entitlements for the selected candidate role.
Assignments	Indicates the number of user-entitlement assignments for the selected candidate role.
OU Spread	"Spread" on page 468 is a numeric index that provides an estimate of the "homogeneous diffusion" of a role in the hierarchical structure of an organization. OU spread indicates the tendency towards a scattered/localized role distribution in the OU hierarchy.
Org Units	Indicates the number of OUs for the selected candidate role.
Applications	Indicates the number of applications for the selected candidate role.

Table 553. Candidate Role attributes (continued)

Attribute	Description
Entitlement Type	Entitlement types include the following ones: • **Permission** • **IT role** • **Business role** • **External role**
Attribute 0... **Attribute 9** (for Users)	Attributes that are configured in the User Attributes section.
Attribute 0... **Attribute 9** (for Entitlements)	Attributes that are configured in the Entitlements Attributes section.

When you select a candidate role from the central pane, the users joined to the candidate role are automatically highlighted in the **Users** tab in the far right.

Listed Users are characterized by the attributes shown in the table below:

Table 554. User attributes

Attribute	Description
In/Out	The user status can be one of the following: • ✓ In Role (Role aggregated to the User) • ✗ Out of Role (Role not aggregated to the User)
Last Name	Surname of the user.
Name	Name of the user.
User ID	Unique ID assigned to the user.
Organization Units	Name of the OU, in which the user is registered.
Attribute 0... Attribute 9 (for Users)	Attributes configured in the User attributes section.

When you select a user from the **Users** tab in the far right, all aggregated candidate roles are automatically highlighted in the central pane.

OUs aggregated with the selected entitlement

The **Organization Units** tab lists all candidate roles containing the entitlement previously selected in the **Entitlements**tab .

The attributes described in the table below are displayed for each candidate role:

Table 555. Candidate Role attributes

Attribute	Description
Role Name	Indicates the name of the role.
Exportation (Report/Release)	The role can have one of the following statuses: • ! **Scheduled to be exported** • ! **Exportation in progress** • ✓ **Successfully exported** • ✗ **Error**
Users	Indicates the number of users for the selected candidate role.
Entitlements	Indicates the number of entitlements for the selected candidate role.
Assignments	Indicates the number of user-entitlement assignments for the selected candidate role.
OU Spread	“Spread” on page 468 is a numeric index that provides an estimate of the “homogeneous diffusion” of a role in the hierarchical structure of an organization. OU spread indicates the tendency towards a scattered/localized role distribution in the OU hierarchy.
Org Units	Indicates the number of OUs for the selected candidate role.
Applications	Indicates the number of applications for the selected candidate role.
Entitlement Type	Entitlement types include the following ones: • **Permission** • **IT role** • **Business role** • **External role**
Attribute 0... Attribute 9 (for Users)	Attributes that are configured in the User Attributes section.
Attribute 0... Attribute 9 (for Entitlements)	Attributes that are configured in the Entitlements Attributes section.

When you select a candidate role in the central pane, the OUs joined to the candidate role are automatically highlighted in the **Organization Units** tab in the far right.

The listed OUs are characterized by the attributes shown in the table below:

Table 556. OU attributes.

Attribute	Description
In/Out	The OU status can be one of the following: - ✓ In Role (Role aggregated to the OU) - ✗ Out of Role (Role not aggregated to the OU)
Code	Code assigned to the OU.
Name	Name of the OU, in which the user is registered.
Farness	Farness is a numeric index that provides an estimate of the virtual distance between OUs having the same entitlement/candidate role. It can measure the distance between OUs in which different registered users are assigned the same entitlement/candidate role.
Coverage (%)	Percentage of users in the OU who are assigned to the entitlement.
Users	Number of users assigned to the selected entitlement.

When you select an OU from the **OU** tab in the far right, all the aggregated candidate roles are automatically highlighted in the central pane.

Statistics:

The Statistics tab provides a set of graphical dashboards for the selected analysis.

The available dashboards are structured into two tabs:

- Analysis Statistics
- Role Statistics

Analysis Statistics

Table 557. Dashboard set.

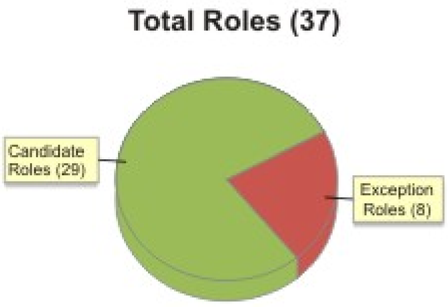
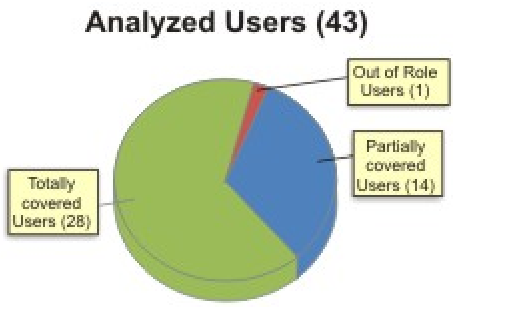
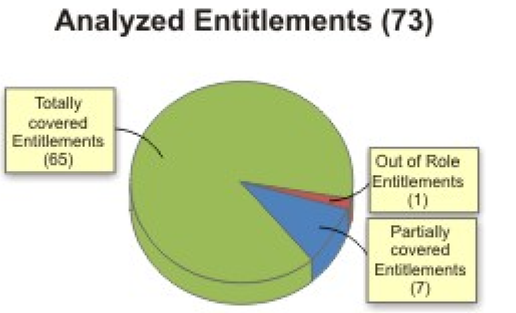
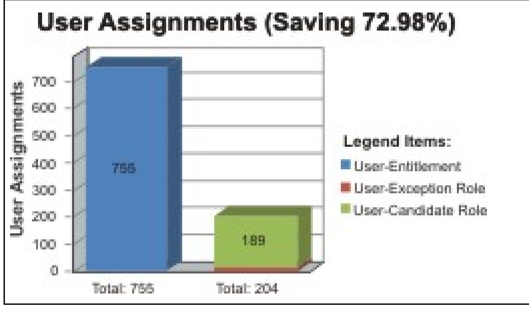
Dashboard	Description
	- The green zone represents the collection of candidate roles, for example roles whose adoption into the organization can be considered useful. - The red zone represents exception roles, for example those built with entitlements that are not aggregated to the set of candidate roles. Every exception role is composed of a single entitlement.

Table 557. Dashboard set. (continued)

Dashboard	Description
	• Users in the green zone: each of their assigned entitlements is involved in at least one candidate role. • Users in the blue zone: some of their assigned entitlements are not involved in any candidate role. • Users in the red zone: none of their assigned entitlements belong to any candidate role.
	• Entitlements in the green zone: each user assigned to these entitlements is involved in at least one candidate role. • Entitlements in the blue zone: some users assigned to these entitlements are not involved in any candidate role. • Entitlements in the red zone: none of the users assigned to these entitlements are involved in any candidate role.
	• The blue histogram shows all entitlements assigned to the considered users. • The green histogram shows all candidate roles assigned to the considered users. • The red histogram shows all exception roles assigned to the considered users.

Role statistics

The **Role Statistics** tab provides a set of histograms for a selected request.

Different filters can be chosen as described in the table below:

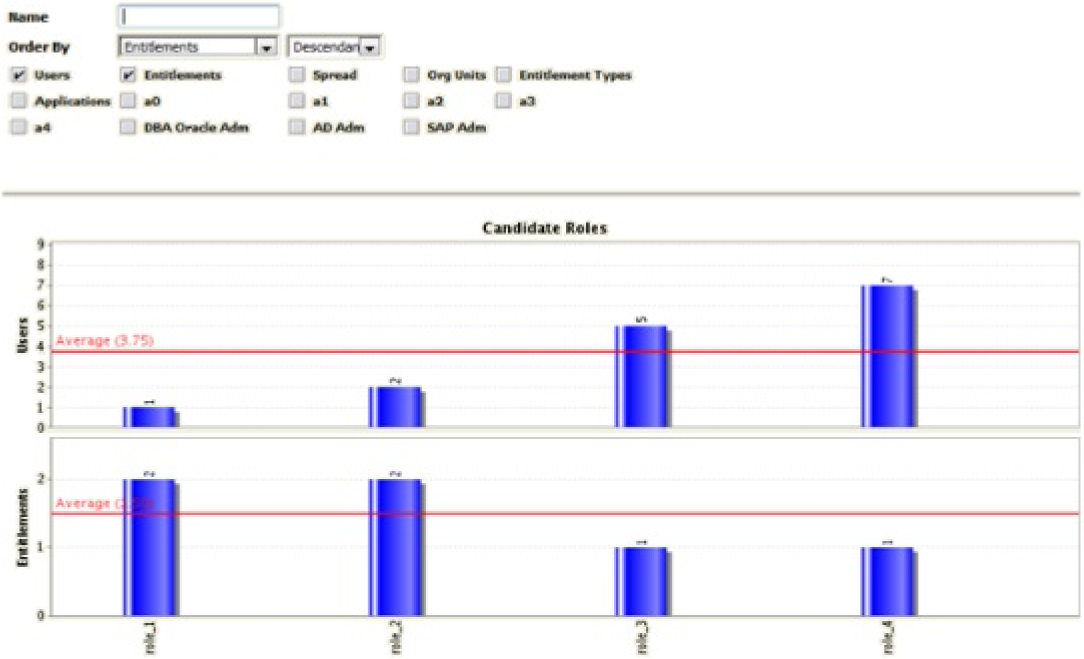
Table 558. Role statistics filters.

Filter	Description
Name	Name(s) of role(s) involved in the request.
Order By	You can sort the displayed data in ascending or descending order, based on the data elements provided. You can start with **Users**.
Listed in the rows below are all the algorithm parameters involved in the request, selectable by selecting the appropriate check box. The related histogram will be displayed only if the check box is selected.	
Users	Users involved in the request
Entitlements	Entitlements involved in the request
Spread	OU spread
Org Units	OUs involved in the request

Table 558. Role statistics filters. (continued)

Filter	Description
Entitlement Types	The entitlement can be one of the following: • : **Permission** • : **IT role** • : **Business role** • : **External role**
Applications	Applications involved in the request
User Attribute 0 ... Attribute 9	Only user attributes specified in the request are available
Entitlement Attribute 0 ... Attribute 9	Only entitlement attributes specified in the request are available
Role Attribute 0 ... Attribute 9	Only role attributes specified in the request are available

The next figure shows an example with the **User** and **Entitlements** check boxes selected, where statistics are listed by entitlement in descending order.



Name

Order By Entitlements ▾ Descendan ▾

☑ Users ☑ Entitlements □ Spread □ Org Units □ Entitlement Types

□ Applications □ a0 □ a1 □ a2 □ a3

□ a4 □ DBA Oracle Adm □ AD Adm □ SAP Adm

Figure 142. Example of Statistics with User and Entitlements check boxes selected.

Generating a request to update an entitlement

Create a request to update an entitlement.

As you select the tab that starts the wizard for generating the request, a list of the existing entitlements is displayed.

You can select **Filter** to search for a specific entitlement. Complete one or more of the following fields to narrow your search.

Table 559. Filters that you can use to search for entitlements.

Filter	Description
Application	The name of the parent application. Select ... to display a list and select an application
Name or Code	The name or the univocal identifier of the entitlement
Type	Select one of the following entitlement types: • Permission • IT Role • Business Role • External Role
Description	A brief description of the entitlement
Group	The name of the organizational unit with which the entitlement is associated

The entitlements that are available are listed with the following attributes under the **Entitlements** tab:

Table 560. Entitlement attributes in an Update Entitlement request generation.

Attribute	Description
Publishing Status	If the entitlement is in Publish status, it can be associated with organizational units. If it is in Not Publish status, it cannot be associated.
Application	The name of the parent application
Entitlement information icon	Select the icon to display the Entitlement information window. This window displays more entitlement information such as: • Extra details • Structure • The permissions that make up the entitlement • A list of the entitled users • The organizational units with which the entitlement is associated
Name	The name of the entitlement and the icon that identifies the entitlement type. • **Permission** • **IT role** • **Business role** • **External role**
Description	A brief description of the entitlement
Owner	The owner of the entitlement

Table 560. Entitlement attributes in an Update Entitlement request generation. (continued)

Attribute	**Description**
Start Date	The starting date of the entitlement validity period
End Date	The ending date of the entitlement validity period
VV	The ❗ icon denotes an entitlement in Role Alignment Violation. An entitlement is in VV when it is not associated to an OU but to a specific user of that OU. The entitlement is not available to the other users of the OU.
Risk Status	The risk status of the entitlement is indicated graphically. 🔵 The risk level is low. 🟠 The risk level is medium. 🔴 The risk level is high.

Select an entitlement and click **Next** to display the Entitlement Details page. The page includes two accordion panes where you can modify the entitlement. The changes are the object of the request generation process.

Details
You can update the following fields:

- Publishing Status
- Owner
- Name
- Code
- Description
- Expiration

Entitlement Properties
You can change the values of the keys that are listed.

Click **Next** again and you move to the Entitlement Designer page. The page shows the current structure of the entitlement in terms of other entitlements (permissions) that the entitlement comprises. The entitlement details and information show the changes that you made in the previous page. Any permissions that the entitlement comprises are listed under the **Current Structure** tab. Click **Remove** to take a permission off the entitlement structure.

Select **Available Entitlements** to display a list of permissions that you can add to the entitlement. Click **Add** next to the permissions that you choose.

Before you click **Next**, you can click **Analysis** to view the Impact Analysis window. This window shows if conflicts exist in the new structure of the entitlement.

Click **Next** to view a Summary page that displays the following items:

- The entitlement with the updates that you are about to request.
- The **Priority** field, where you can set a priority level for the request. This field might not be enabled, based on the setup of this type of requests.
- A **Request Notes** field for optional remarks.

When you are ready to generate the request, click **Submit**. Then, click **Ok** on the confirmation window that follows. The new request is displayed in the Service Center session of the assignee of the administrative role that authorizes Entitlement Update requests.

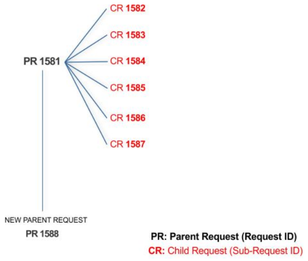
Insert/Update entitlement: processing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 561. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles

Table 561. Request Status (continued)

Status	Description
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

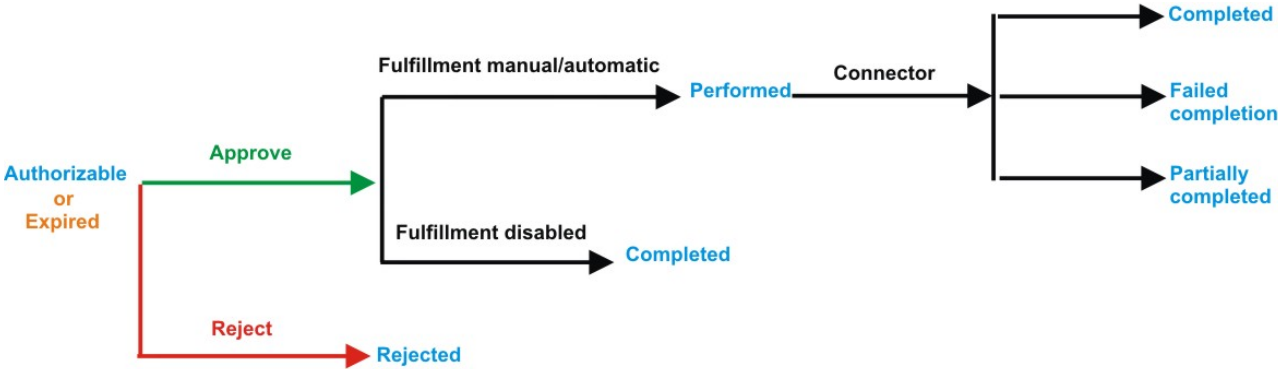


Figure 143. Subrequest status

Table 562. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.

Table 562. Subrequest status (continued)

Status	Description
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters.

Click **Filter/Hide Filter** and then click **Search**.

Table 563. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	**Description**
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	The status of the sub-requests (**Sub-Request ID**column).

Requests attributes	
Attribute	**Description**
Priority	The priority assigned to the request

Click an item under **Applicant** or **Beneficiary** to open the related User details window and show the following information:

Table 564. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click an item under **Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 565. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.

Table 565. Details of a request - upper section (continued)

Box	Details
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

The lower part of the frame shows a sub-set of fields related to the request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.

Click an item under **Sub-Request ID** to view the details.

The upper part of the frame shows the same information set shown in the above table, but related to the selected sub request.

The lower part of the frame shows a sub-set of fields related to the sub request associated to a request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.

Click the ⓘ **Info** icon to open the User details window and show the information in a set of tabs:

Table 566. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user

Table 566. User Details - Details tab (continued)

Detail	Description
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 567. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 568. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 569. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 570. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.

Table 570. User Details - Rights (continued)

Detail	Description
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows the following information about the requests:

Table 571. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ! icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 572. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission
It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)
A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role
A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

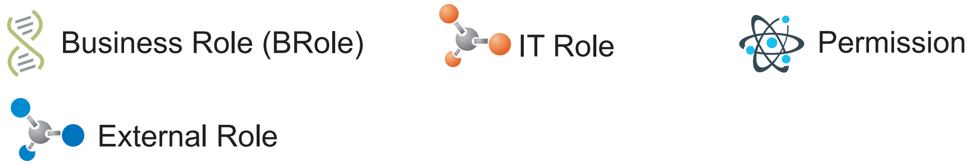
- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role
Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Insert/Updates entitlements: executing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are red.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 573. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress

Table 573. Request Status (continued)

Status	Description
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 574. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The results are displayed in the same frame, according to the following attributes:

Requests attributes	
Attribute	**Description**
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.
Priority	The priority assigned to the request

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 575. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 576. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.

Table 576. Details of a request - upper section (continued)

Box	Details
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

Click the ⓘ **Info** icon to open the User details window and show the information in a set of tabs:

Table 577. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 578. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user

Table 578. User Details - Entitlements tab (continued)

Details	Description
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 579. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 580. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 581. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows the following information about the requests:

Table 582. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**

- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 583. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)

- External Roles
- Permissions

The following icons represent these entitlements:

Business Role (BRole)

IT Role

Permission

External Role

If notes about the considered entitlement are in the request, the **Note** icon is available. Click it to open the Notes window and show the contents of the note.

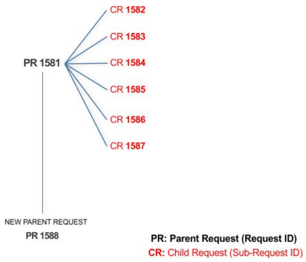
Viewing the requests present in the system

You can view a summary of the generated requests and click a **Request ID** or **Sub-Request ID** to browse the details.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**s, 1582 - 1587.

You can view all the requests that are registered by the Request Report activity.

Even if you are logged-in as the authorizer, some of the requests and subrequests might not be visible because they are outside the scope that is defined for the authorizer.

The requests that are generated during the authorization process are characterized by a status. The status can be one of the statuses that are summarized in the following table.

Table 584. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization

Table 584. Request Status (continued)

Status	Description
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

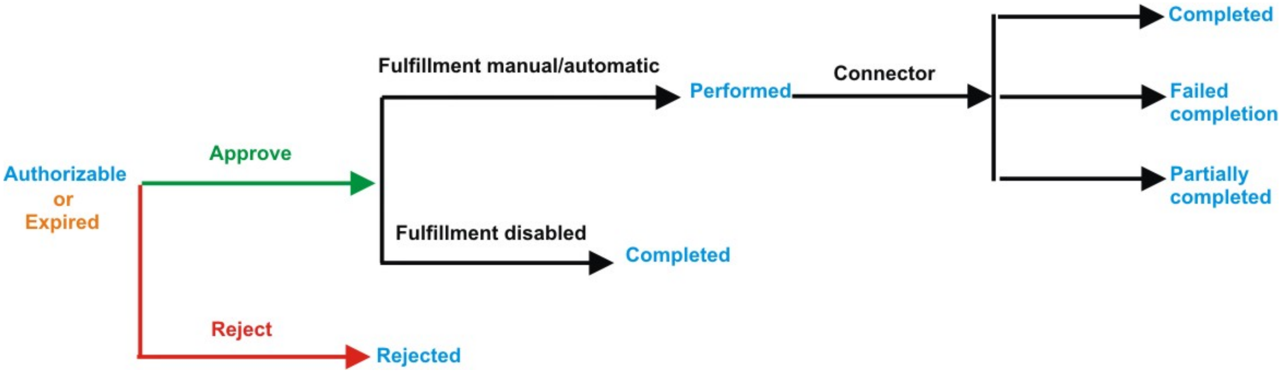


Figure 144. Subrequest status

Table 585. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization

Table 585. Subrequest status (continued)

Status	Description
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can use filters to search for specific requests. Select **Filter**, enter your search parameters, and click **Search**.

Table 586. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The results are displayed in the same frame. The request attributes shown in each row are listed in the next table.

Table 587. Request attributes

Attribute	Description
Request ID	The univocal identifier of the parent request
Sub-Request ID	The univocal identifier of the child request
Type	The type of the request

Table 587. Request attributes (continued)

Attribute	Description
Applicant	The name of the applicant of the request
Beneficiary	The name of the beneficiary of the request
Escalation	Specifies whether the request was escalated
Created on	The date (`dd/mm/yyyy`) and time (`hh:mm`) that the request was created.
Status	The status of the subrequest
Priority	The priority that is assigned to the request
Notes	Click the icon to display comments that were added by the applicant in the request

In every row, you can select the **Applicant** and **Beneficiary** of a request to open the User details window and view their user information.

Table 588. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

You can click **Request ID** and **Sub-Request ID** to view the details of the request and of the subrequest.

The upper part of the frame shows information about the request and about its applicant. Depending on the type of request, other information is displayed.

Table 589. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (dd/mm/yyyy) and time (hh/mm) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

You can click the available ⓘ **Info** icons to view further details about an item.

The **Request Notes** occupy the middle section of the frame. Request notes can be specified by the author of the request or by a rule. In this field, you can add free text for any reason during the authorization or execution of the request.

The lower part of the frame shows more information on the request. The contents depend on the request type. If the request concerns a user, an entitlement, or an account, this part of the frame displays details about these items.

When you finished viewing the request details, select **Back** to return to the list of requests.

Viewing expired requests that require to be approved or rejected

You can view a summary of requests that passed their expiration time and that await your approval or rejection. Select a **Request ID** or **Sub-Request ID** to browse the details.

Every request in this list was generated with a priority that defines an expiration time. An Escalation action was also defined if the request was not processed within this time.

The requests that are in this list reached their expiration time without being processed and await your intervention.

You can use filters to search for specific requests. Select **Filter**, enter your search parameters, and click **Search**.

Table 590. Filters that you can use to search for specific requests

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The expired requests that await your intervention are listed with the attributes that are shown in the following table.

Table 591. Request attributes

Attribute	Description
Request ID	The univocal identifier of the parent request
Sub-Request ID	The univocal identifier of the child request
Type	The type of the request
Applicant	The name of the applicant of the request
Beneficiary	The name of the beneficiary of the request
Created on	The date (`dd/mm/yyyy`) and time (`hh:mm`) that the request was created.
Status	The status of the subrequest. In this context, it is always Expired.
Priority	The priority that is assigned to the request

In every row, you can select the **Applicant** and **Beneficiary** of the request to open the User details window and view detailed user information.

You can click **Request ID** and **Sub-Request ID** to view the details of the request and of the subrequest.

The upper part of the frame shows information about the request and about its applicant. Depending on the type of request, other information is displayed.

Table 592. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

You can click the available ⓘ **Info** icons to view further details about an item.

The **Request Notes** and **Additional Notes** boxes occupy the middle section of the frame. These notes can be specified by the author of the request or by a rule. In these fields, you can add free text for any reason during the authorization or execution of the request.

The lower part of the frame shows more information on the request. The contents depend on the request type. If the request concerns a user, an entitlement, or an account, this part of the frame displays details about these items.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

User access: generating a request

Select this tab to add role access to one or more selected users.

The **Users** tab is the first step of a wizard that guides you to select users and grant them access to entitlements.

Use the following filters to search specific users and then click **Search**.

Table 593. User filters

Filter	Description
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
First Name/Last Name/Master UID	The name or surname or the unique identifier of the user
Enabled	The user is enabled to be assigned entitlements
Activity	The business activity that the user is involved with. After the selection of the activity, you can flag **Hierarchy** to search also all the activities that are defined from this point down in the hierarchical structure.

Users are displayed with the following attributes:

Table 594. Attributes in the Users list

Attribute	Description
Info	Click ⓘ **Info** to open the User details window. This window shows several user details like external data, assigned entitlements, assigned accounts, and rights.
First Name	The name of the user
Last Name	The surname of the user
User ID	The Unique identifier of the user
User Type	The type of user. For example, Administrative, Business, Employee, Training, External.
Group [Code]	The Organization Unit [Univocal identifier of the OU] to which the user belongs

Note: The order of the columns that are indicated in the table can be freely configured by the Administrator.

To select the entire list of users, select the check box on the attributes row; otherwise, for selecting a specific user, select the check box in the user's row.

Click the ⓘ **Info** icon to open the **details** window. This window displays user information in the following tabs:

Table 595. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	

Table 595. User Details - Details tab (continued)

Detail	Description
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 596. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 597. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 598. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

Table 599. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

From the **Entitlement** tab, click the ⓘ **Info** icon to open the **Entitlement info** and show a set of information that is grouped in

- **Details**
- **Structure**
- **Permissions**
- **Users**
- **Groups**
- **Rights**

The tabs **Details** and **Structure** are always available.

The other tabs can be present or not according to the configurations adopted and with the nature of the entitlement.

For example, if the entitlement is a permission that is not associated to any right, the tab **Rights** not is present in the **Entitlement info** pop-up.

The following list describes the various types of entitlements:

Permission

It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)

A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role

A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role

Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:

Business Role (BRole)
IT Role
Permission
External Role

Click **Next** to open the Catalog tab.

User Access: Catalog

The **Catalog** tab is the second step of the wizard.

You can choose the entitlements and roles for the users that are selected in the first step of the wizard, Users.

The upper part of the frame summarizes the information about the selected users.

Table 600. User data.

Data	Description
ⓘ Info	Click the **Info** icon to open the **Entitlement info** window.
User ID	Unique identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Group [Code]	Name of the organization unit or univocal identifier of the OU.
User Type	Type of user.

Table 600. User data. (continued)

Data	Description
Risk Status	The risk status that is associated with the user is displayed by a symbol: ✓ Absence of risks. 🔵 The risk level is low. 🟠 The risk level is medium. 🔴 The risk level is high. Click the colored dot to open a window that shows: • The Risk Activities Tree (related to a specific user) in the **Risk Info** tab. • The Activities that are involved in a specific risk, in the **Mitigations** tab.

Note: The order and the presence of some columns in this tab can be freely configured by the Administrator.

Click **Refresh** to update the risk situation of the user.

The lower part of the frame includes the following tabs:
- **Current entitlements**
- **Business Roles**
- **Application Roles**
- **Permissions**
- **External Roles**

Note: The order and the presence of some columns in these tabs can be freely configured by the Administrator.

According to the configuration of the activity:
- Some of the previous tabs might not be present.
- On the right side of these tabs, might be present the **Business Activity Impact** frame that hosts a flat list of the activities of the user.

You can select an activity from the flat list to highlight in yellow, in any tab, the entitlements involved in the selected activity.

If you remove (click **Remove**) an entitlement, the user loses the control on certain activities.

The lost activities are colored in red.

If you add (click **Add**) an entitlement, the user might acquire a control on certain activities.

The acquired activities are colored in green.

Before to add or remove an entitlement, you can view the set of activities that are related to it.

Every row of the campaign host an entitlement and you must consider every row as a node of a tree.

The type of entitlement might be

- **Permission**
- **IT Role**
- **Business Role**

Click the little dark row, on the left of the selected node, for expanding a possible a flat list of the activities associated to the selected entitlement.

Note: If an entity row of the campaign is displayed without **Approve/Revoke**, the entity is no longer available for the reviewer. It can be no longer available for several reasons. For example, the entity was deleted by another process, such as an entitlement, that was originally involved in the certification process.

Note: In some views, only a subset of the data that is indicated might be shown.

Current entitlements tab

The **Current Entitlements** tab lists the entitlements that are assigned to the selected users. You can use the following filters to search specific entitlements (click **Filter** > **Search**):

Table 601. Current entitlements filters.

Filter	Description
Application	The name of the parent application.
Name or Code	The name or identification code of the entitlement.
Type	It can be Permission, IT Role, Business Role, or External Role.
Description	A brief description of the entitlement.
Group	The Organization unit with which the entitlement is associated.

You can start the following actions from the list of entitlements listed:

- **Remove** (entitlement)
- **Change**(value of a right or validity date of an entitlement)

To remove an entitlement, click the related **Remove** button (**Remove** is shown in red).

If you try to remove an attribute permission required (icon), a warning message is shown.

If you need more details, see “Permissions based on user attributes” on page 16.

To change the value of a right or the date of validity of an entitlement, click the related **Change** button (**Change** is shown in orange).

Click freely one of the other tabs if you want to assign Business Roles, Application Roles, Permissions, or External Roles to the selected user.

Click **Next** to go to the “User Access: Shopping Cart” on page 858 tab to process the request.

Business Roles tab

The **Business Roles** tab displays the list of available Business roles for the selected users. You can use the following filters to search specific Business roles (click **Filter** > **Search**):

Table 602. Business roles filters.

Filter	Description
Name or Code	The name or identification code of the entitlement.
Description	A brief description of the Business role.
Family	Business roles can be logically grouped in a super set named Family. For example, the Administrative Roles are in the Identity Management Administration family.
Group	The Organization unit with which the entitlement is associated.
Activity	You can set this filter for selecting all Business roles that are associated to the selected activity.
Hierarchy	If this check-box is selected, the Business roles are filtered through the hierarchy that starts from the activity previously set.

From the list of Business roles, you can assign one or more roles to the selected users. Click **Add** (**Add** is highlighted in green).

The **Actions** menu includes the following items:

All Roles
Select this action to choose roles to assign to a selected user from the full set of available roles.

Like Mike
Select this action to assign to a selected user the same roles of another user that is chosen from the full set of users.

Application Roles tab

The **Application Roles** tab displays the list of available IT roles that are ordered by parent application. You can use the following filters to search specific entitlements (click **Filter** > **Search**):

Table 603. Application roles filters.

Filter	Description
Application	The name of the parent application.
Name or Code	The name or identification code of the entitlement.
Description	A brief description of the IT role.
Family	IT roles can be logically grouped in a super set named Family.
Group	The Organization unit with which the entitlement is associated.
Activity	You can set this filter for selecting all IT roles that are associated to the selected activity.
Hierarchy	If this check-box is selected, the IT roles are filtered through the hierarchy that starts from the activity previously set.

Each row of the list includes two **Info** icons (ⓘ). Click the one under the **Application** heading to view details of the parent application. Click the one on the far right to view details of the entitlement.

From the list of entitlements, you can assign one or more roles to the selected users. Click **Add** (**Add** is highlighted in green).

The **Actions** menu includes the following items:

All Roles
Select this action to choose roles to assign to a selected user from the full set of available roles.

Like Mike
Select this action to assign to a selected user the same roles of another user that is chosen from the full set of users.

Permissions tab

The **Permissions** tab displays the list of available permissions that are ordered by parent application. You can use the following filters to search specific permissions (click **Filter** > **Search**):

Table 604. Permissions filters.

Filter	Description
Application	The name of the parent application.
Name or Code	The name or identification code of the entitlement.
Description	A brief description of the IT role.
Permission Type	Permissions can be logically grouped through a Permission Type.
Group	The Organization unit with which the entitlement is associated.

Table 604. Permissions filters. (continued)

Filter	Description
Activity	You can set this filter for selecting all IT roles that are associated to the selected activity.
Hierarchy	If this check-box is selected, the Business roles are filtered through the hierarchy that starts from the activity previously set.

Each row of the list includes two **Info** icons (ⓘ). Click the one under the **Application** heading to view details of the parent application. Click the one on the far right to view details of the entitlement.

From the list of entitlements, you can assign one or more permissions to the selected users. Click **Add** (**Add** is highlighted in green).

The **Actions** menu includes the following items:

All Roles
Select this action to choose roles to assign to a selected user from the full set of available roles.

Like Mike
Select this action to assign to a selected user the same roles of another user that is chosen from the full set of users.

External Roles tab

The **External Roles** tab displays the list of available External roles that are ordered by parent application. You can use the following filters to search specific External roles (click **Filter** > **Search**):

Table 605. External roles filters.

Filter	Description
Name or Code	The name or identification code of the entitlement.
Description	A brief description of the External role.
Family	External roles can be logically grouped in a super set named Family. For example, the External roles incoming from Target X, might be grouped as *ER_from_X*.
Group	The Organization unit with which the entitlement is associated.
Activity	You can set this filter for selecting all Business roles that are associated to the selected activity.
Hierarchy	If this check-box is selected, the External roles are filtered through the hierarchy that starts from the activity previously set.

Each row of the list includes two **Info** icons (ⓘ). Click the one under the **Application** heading to view details of the parent application. Click the one on the far right to view details of the entitlement.

From the list of entitlements, you can assign one or more External Roles to the selected users. Click **Add** (**Add** is highlighted in green).

The **Actions** menu includes the following items:

All Roles
Select this action to choose roles to assign to a selected user from the full set of available roles.

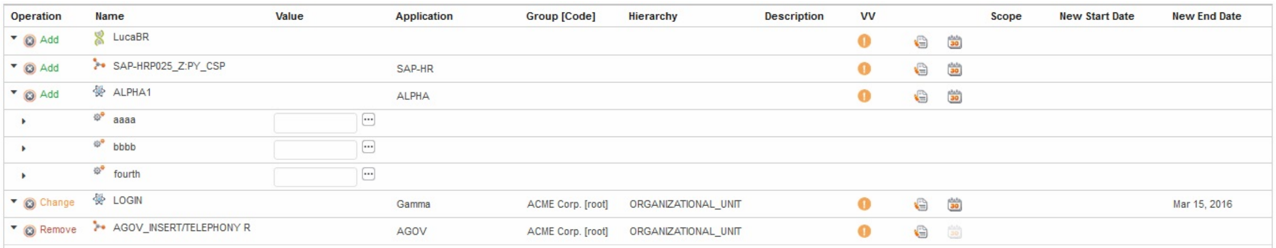
Like Mike
Select this action to assign to a selected user the same roles of another user that is chosen from the full set of users.

Click **Next** to go to the "User Access: Shopping Cart" tab to process the request.

User Access: Shopping Cart

The **Shopping Cart** tab is the third step of the wizard.

The tab hosts a summary tree structure:



Operation	Name	Value	Application	Group [Code]	Hierarchy	Description	VV	Scope	New Start Date	New End Date
Add	LucaBR						!			
Add	SAP-HRP025_Z:PY_CSP		SAP-HR				!			
Add	ALPHA1		ALPHA				!			
	aaaa									
	bbbb									
	fourth									
Change	LOGIN		Gamma	ACME Corp. [root]	ORGANIZATIONAL_UNIT		!			Mar 15, 2016
Remove	AGOV_INSERT/TELEPHONY R		AGOV	ACME Corp. [root]	ORGANIZATIONAL_UNIT		!			

Figure 145. Shopping Cart summary tree structure.

The **Operation** column lists the operations that are performed in the tabs under "User Access: Catalog" on page 852 tab:

- **Add**
- **Remove**
- **Change**

When you select the ⊗ **Clear** button, the operation is revoked and excluded by the next steps.

The **Name** column lists the entitlements that are involved in the operation.

If the entitlement is permission, it might have one or more associated **Rights**.

You can assign one or more values to a right (according to the specific nature of the right).

When you have a right is with lookup, a ⋯ **Browse** button is available nearby. Click it to display the pop-up window, where you can set values.

If you need more details, see AGC_Rights tab.

The **Application** column lists the names of the parent application of the considered entitlement.

The presence of the ❗ **Role Alignment Violation** icon in the **VV** column, denotes an entitlement that is assigned violating the segregation group policy.

An entitlement is in VV when is assigned (for such reason) to a user but is not associated to the group (OU) where the user is stored.

This entitlement in VV is not available for to be assigned to the others users of the group (OU).

One or more of the following buttons might be enabled for each entitlement and displayed after to the VV column:

Table 606. Buttons and Icons.

Button/Icon	**Description**
📝	Click **Note** to display the **Notes** window where you can add notes for other authorization steps.
30	Click **Validity** to open the **Date Selection** window where you can enter the *Start Date* and the *End Date* for operations of • **Add** • **Change** (only the *End Date*)
💻	Click **Application Scope** to display the **Resource Assign** window where you can select one or more applications to assign. **Note:** This button is only available for the Admin Access Request.
🖧	Click **Org. Units Scope** to display the **Resource Assign** window where you can select one or more organizational units to assign. **Note:** This button is only available for the Admin Access Request.
🧬	Click **Business Role Scope** to display the **Resource Assign** window where you can select one or more business roles to assign. **Note:** This button is only available for the Admin Access Request.
⚠	Click **Risk Scope** to display the **Resource Assign** window where you can select one or more risks to assign. **Note:** This button is only available for the Admin Access Request.
🖧	Click **Attribute Hierarchy Scope** to display the **Resource Assign** window where you can select one or more attribute hierarchies to assign. **Note:** This button is only available for the Admin Access Request.

The **New Start Date** and **New End Date** columns list the dates set with the **Validity** button.

If you try to change the *End Date* of an attribute permission required (icon) directly assigned to a user, an automatic job check if the operation can be validated.

If you need more details, see “Permissions based on user attributes” on page 16.

Priority declares the priority level that is assigned to this request.

If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

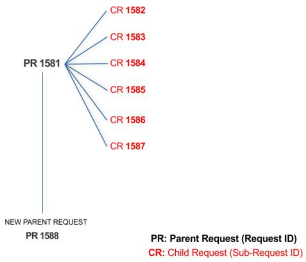
User access: processing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 607. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization

Table 607. Request Status (continued)

Status	Description
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

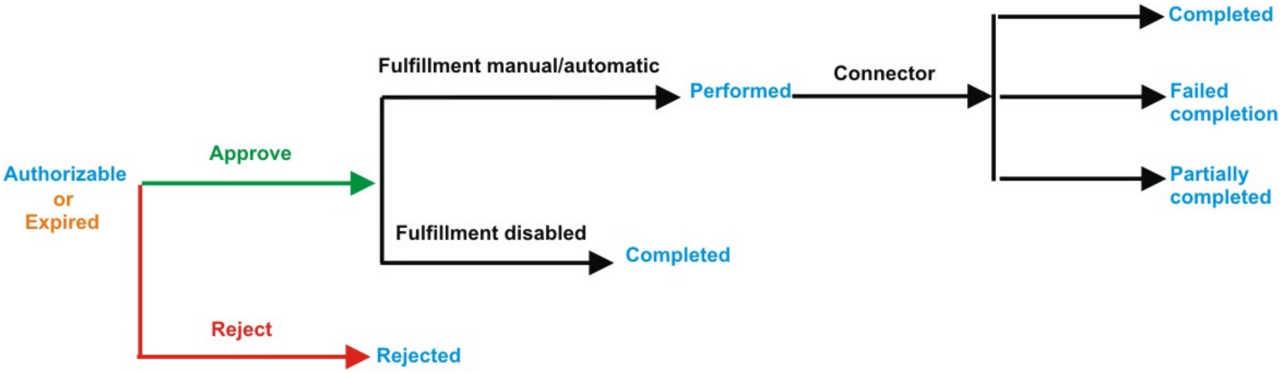


Figure 146. Subrequest status

Table 608. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization

Table 608. Subrequest status (continued)

Status	Description
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 609. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The results are displayed in the same frame, according to the following attributes:

Table 610. Requests attributes

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.

Table 610. Requests attributes (continued)

Attribute	Description
Created on	The day (`dd/mm/yyyy`) and time (`hh:mm`) when the request was created.
Status	Request Status.
Priority	The priority that is assigned to the request. It can be High, Medium, Low, or Unassigned.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 611. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 612. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.

Table 612. Details of a request - upper section (continued)

Box	Details
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

Click the **Info** icon to open the User details window and show the information in a set of tabs:

Table 613. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 614. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 615. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 616. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 617. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows the following information about the requests:

Table 618. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user

Table 618. Request attributes (continued)

Attribute	Description
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 619. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission
It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)
A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role
A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

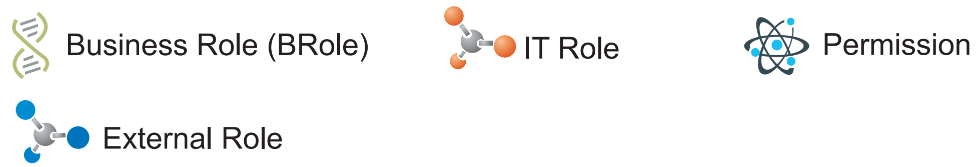
- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role
Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the 📝 **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

User access: executing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Requests** and are red.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 620. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

You can search specific requests with the following filters. Click **Filter/Hide Filter** and then click **Search**.

Table 621. Filters

Filter	Description
Request ID	The Unique identifier of the request

Table 621. Filters (continued)

Filter	Description
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The results are displayed in the same frame, according to the following attributes:

Table 622. Requests attributes

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	Request Status.

Click **Applicant** and **Beneficiary** to open the User details window and show the following information:

Table 623. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).

Table 623. User Details - Details tab (continued)

Detail	Description
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click **Request ID** and **Sub-Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 624. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

Click the ⓘ **Info** icon to open the User details window and show the information in a set of tabs:

Table 625. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 626. User Details - Entitlements tab

Details	Description
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 627. User Details - Accounts tab

Detail	Description
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 628. User Details - Activities tab

Detail	Description
Name	Name of the activity
Path	Position of the activity in the Activity Tree

Table 628. User Details - Activities tab (continued)

Detail	Description
Description	Brief description of the activity

Table 629. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows the following information about the requests:

Table 630. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 631. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement

Table 631. Entitlement info - Structure (continued)

Detail	Description
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission
It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)
A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role
A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

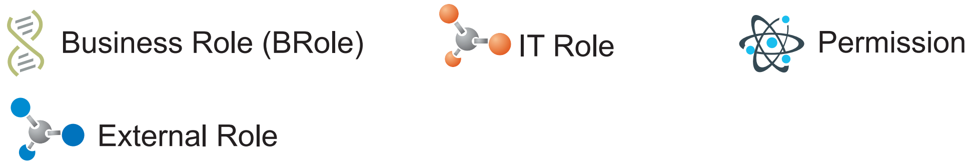
- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role
Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the **Note** icon is available. Click it to open the Notes window and show the contents of the note.

Create/Update user: generating a request

You can insert a new user or update information for a registered user.

- Create User
- Update User

Create user: generating a request

You can insert or update a new user.

Insert User

From the **User Creation** tab, you can complete the form for the **User Create Request**.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

The structure and the contents of the form depend by the configuration provided through:

- the Access Governance Core module, in **Settings** > **Core Configurations** > **User Virtual Attributes** panel.
- the Process Designer module, in **Manage** > **Activity** panel.

An example of a possible form it's indicated in the table below:

User Creation field	
Field	**Description**
Code	Univocal identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Email	Email of the user.
User Type	Type of user.
ID External Table	Univocal identifier of the External Table.
Address	Address of the user.
City	City of the user.
State	State of the user.
Country	Country of the user.
Phone Number	Phone number of the user.
Gender	Gender of the user.
Date of Birth	Date of birth of the user. Click **Calendar** to choose the date. Click **Clear** to delete the date of birth.

The fields mandatory are indicated with the presence of an *.

Click **Submit** to process the request.

Note: **Previous** and **Next** are disabled. The request has one step.

Update user: generating a request

You can update information about a registered user.

Update User

From the **Users** tab, you can view a list of users.

You have to select the user that you want to manage in the next step.

Clicking on the blue icon on the left, you can view the details related to the user.

Click **Next** button to proceed.

Note: **Previous** is disabled.

From the **User Update** tab, you can complete the form for the **User Update Request**.

Priority declares the priority level that is assigned to this request. If the field is enabled, you can change the priority level. Select the field to display the available priority levels to which you can move the request.

The structure and the contents of the form depend by the configuration provided through:

- the Access Governance Core module, in **Settings** > **Core Configurations** > **User Virtual Attributes** panel.
- the Process Designer module, in **Manage** > **Activity** panel.

An example of a possible form it's indicated in the table below:

User Creation field	
Field	**Description**
Code	Univocal identifier of the user.
First Name	Name of the user.
Last Name	Surname of the user.
Email	Email of the user.
User Type	Type of user.
ID External Table	Univocal identifier of the External Table.
Address	Address of the user.
City	City of the user.
State	State of the user.
Country	Country of the user.
Phone Number	Phone number of the user.
Gender	Gender of the user.

User Creation field	
Field	**Description**
Date of Birth	Date of birth of the user. Click **Calendar** to choose the date. Click **Clear** to delete the date of birth.

The fields mandatory are indicated with the presence of an *.

Click **Submit** to process the request.

Note: Previous and **Next** are disabled.

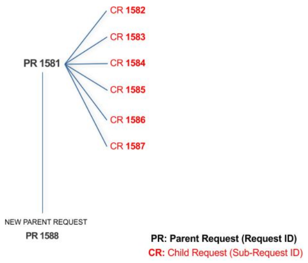
Insert/Update user: processing a request

You can view a summary of the generated requests.

You can view two types of requests:

- **Request ID**
- **Sub-Request ID**

The **Request ID**, which is in black, is the parent request. Parent requests (PR) are associated to one or more child requests (CR), which are called **Sub-Request ID** and are in red.



In the previous example, **Request ID 1581**, generates six **Sub-Request ID**: 1582, 1583, ... and 1587.

There is ALWAYS the possibility to view ALL the requests registered through the Request Report activity.

However, when you are logged-in as authorizer some of the request (and sub-request) listed through the Request Report activity might not be visible because out of the scope defined for the authorizer.

The requests that are generated during the authorization process can be characterized by different statuses, which are summarized in the following table:

Table 632. Request Status

Status	Description
Approved	Request was successfully approved and is waiting to be processed
Authorizable	Request is waiting for authorization

Table 632. Request Status (continued)

Status	Description
Completed	Request was successfully propagated to the target system. It is a final status for the request.
Escalation	Request is being escalated because it contains incompatible roles
Expired	Request exceeded the time limit that is specified by its **Priority** without being processed
In execution	Request is waiting for the propagation to the target system
Operation failed to complete	Completed request with faulty propagation to the target system. It is a final status for the request.
Partially Approved	Request with some sub requests in **Approved** status
Partially Authorized	Request with some sub requests in **Authorizable** status
Partially Completed	Request with all sub requests at end of their lifecycle, some **Completed** and some in **Failed Completion** status.
Partially Executed	Request with some sub requests in **Executed** status.
Partially Terminated	Request with some sub requests in **Completed** status and some in progress
Pending	Source request is waiting for formalization by one or more approvers
Rejected	Request can no longer be processed. It is a final status for the request
Terminated With Reservation	This status includes all the requests that present an unclear or unexpected behavior. It is a final status for the request.

Every request includes one or more subrequests. Subrequests are characterized by a status.

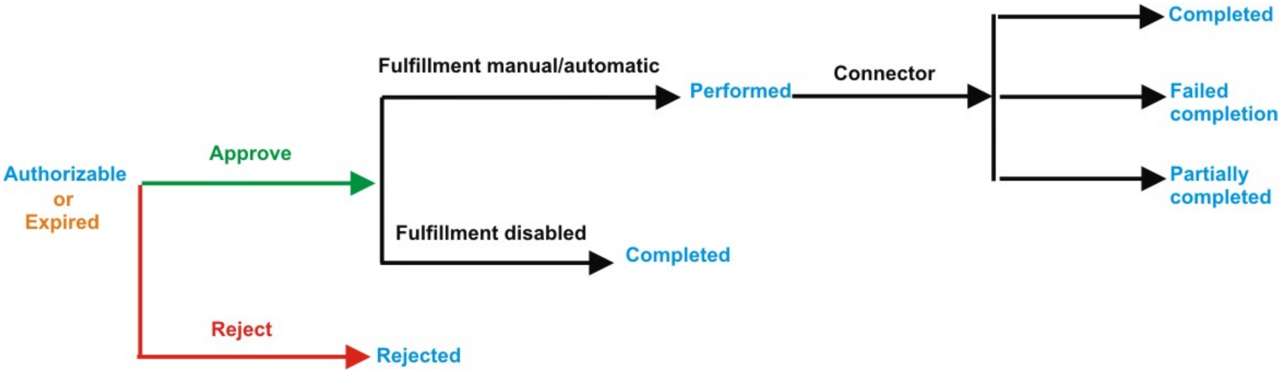


Figure 147. Subrequest status

Table 633. Subrequest status

Status	Description
Authorizable	The request is waiting for authorization

Table 633. Subrequest status (continued)

Status	Description
Completed	If the fulfillment is disabled, the action is completed. If the fulfillment is on Manual/Automatic, it means that the connector successfully aligned every permission on the target system.
Expired	The request exceeded the time limit that is specified by its **Priority** without being processed. It needs to be escalated to an authorized approver.
Failed Completion	The connector failed to align all permission on the target system.
Incompatibility	The request contains incompatible roles
Partially Completed	The connector failed to align some of the permissions. Others were successfully propagated.
Performed	The connector did not yet align the permissions on the target system.
Rejected	The request was rejected by the approver, and is not fulfilled.

You can search specific requests with the following filters.

Click **Filter/Hide Filter** and then click **Search**.

Table 634. Filters

Filter	Description
Request ID	The Unique identifier of the request
Sub Request ID	A single request can generate from 1 to N subrequests. All are identified by a proper ID number.
Applicant Identity	The identifier of the IAG actor who generated the request
Beneficiary Identity	The identifier of the beneficiary of the request
Type	The action that is requested
Status	The status of the subrequest
Created between	**Start Date** The start of a time interval when the request was submitted. **End Date** The end of a time interval when the request was submitted.

The results are displayed in the same frame, according to the following attributes:

Table 635. Requests attributes

Attribute	Description
Request ID	Univocal identifier of the parent request.
Sub-Request ID	Univocal identifier of the child request.
Type	Type of request.

Table 635. Requests attributes (continued)

Attribute	Description
Applicant	Name of the applicant of the request.
Beneficiary	Name of the beneficiary of the request.
Created on	Date (`dd/mm/yyyy`) and hour (`hh:mm`) the request was created.
Status	The status of the sub-requests (**Sub-Request ID**column).
Priority	The priority assigned to the request

Click an item under **Applicant** or **Beneficiary** to open the related User details window and show the following information:

Table 636. User Details - Details tab

Detail	Description
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Click an item under **Request ID** to view the details.

The upper part of the frame shows the following information about the **Actors of the Request**:

Table 637. Details of a request - upper section

Box	Details
Request	**ID** The unique identifier of the request. **Type** The type of the request. **Status** The status of the request. **Priority** The priority that is assigned by the applicant to the request. **Created on** The date (`dd/mm/yyyy`) and time (`hh/mm`) that the request was created.
Applicant/ **Beneficiary/** **Delegator/**	**Group** The group of the Applicant/Beneficiary/Delegator. **First Name** The given name of the Applicant/Beneficiary/Delegator. **Last Name** The surname of the Applicant/Beneficiary/Delegator. **User ID** The unique identifier of the Applicant/Beneficiary/Delegator. Click ⓘ **Info** to view the user details.
Modified Entitlement	**Application** The application with which the entitlement is associated. **Name** The name of the entitlement. **Description** A description of the entitlement. **Publishing Status** The Publishing Status of the entitlement. Can be Published or Unpublished.

Note: The Request Notes are not mandatory. If there are no notes in the request, the fields of the Request Notes are blank.

The lower part of the frame shows a sub-set of fields related to the request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.

Click an item under **Sub-Request ID** to view the details.

The upper part of the frame shows the same information set shown in the above table, but related to the selected sub request.

The lower part of the frame shows a sub-set of fields related to the sub request associated to a request submitted during the generation phase.

This subset depends by the configuration set by the Administrator through Process Designer module.

Click the ⓘ **Info** icon to open the User details window and show the information in a set of tabs:

Table 638. User Details - Details tab

Detail	**Description**
Group	The organization unit to which user belongs
First Name	Names of user
Last Name	
User ID	Unique identifier of user
User Type	Information that helps describe the position of the user in the organization. Use it to indicate the user's title (User Manager, Security Officer) or - for external users - the type of relationship with the organization (for example, Business Partner, Customer, Supplier).
Address	Address details of user
City	
Email	
State	
Zip/Postal code	
Country	
Phone	

Table 639. User Details - Entitlements tab

Details	**Description**
ⓘ	Click **Info** to open the Entitlement information window
Application	Type of application
Name	Name of the entitlement
Description	A brief description of the nature of the entitlement
Owner	Owner of the entitlement
Start Date	Start date of the assignation of the entitlement to the user
End Date	End date of the assignation of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation

Table 640. User Details - Accounts tab

Detail	**Description**
Config.Name	Configuration name of the account
Code	Unique identifier of the account

Table 641. User Details - Activities tab

Detail	**Description**
Name	Name of the activity
Path	Position of the activity in the Activity Tree
Description	Brief description of the activity

Table 642. User Details - Rights

Detail	Description
Name	Name of the entitlement.
Value	This field is referred to the value of a right that is possibly associated to a permission, present in the list.
Application	Name of the parent application of the entitlement considered.
Group[Code]	The Organization Unit [Unique identifier of the OU] to which the user belongs.
Hierarchy	Name of the attribute hierarchy.

The lower part of the frame shows the following information about the requests:

Table 643. Request attributes

Attribute	Description
Application	Type of application
Name	Name of the entitlement
Description	Brief description of the entitlement
Owner	Owner of the entitlements that are involved in the Request
Start Date	Start date of the assignment of the entitlement to the user
End Date	End date of the assignment of the entitlement to the user
VV	The ❗ icon denotes an entitlement in Role Alignment Violation
Group [Code]	Code of the node of the hierarchy, for example, the organization unit (OU) code in the hierarchy of OUs.
Hierarchy	Name of the hierarchy

Click the ⓘ **Info** icon to open the Entitlement info window and show the summarized information in the following set of tabs:

- **Details**
- **Structure**
- **Activity**
- **Permissions**
- **Groups**
- **Rights**

The **Structure** tab is always available. It shows the structure of the entitlement of the request. The other tabs are available only when the entitlement is characterized by **Activities** or **Rights**.

Table 644. Entitlement info - Structure

Detail	Description
Name	Name of the entitlement
Application	Type of application
Description	Brief description of the entitlement
Owner	User who is responsible for the considered entitlement

Table 644. Entitlement info - Structure (continued)

Detail	Description
Family	Family of the selected entitlement

A generic Entitlement has a hierarchical structure.

The following list describes the various types of entitlements:

Permission
It is the basic authorization object. It is defined as an authorized action on a protected object, such as reading and writing a local file or creating a connection.

IT Role (Application Role)
A collection of permissions that are defined in the context of a single system or application. It can contain other IT roles of the same application, in other words:

- IT Roles
- Permissions

External Role
A set of permissions and roles that are received from an external application or target. It is conceptually like a business role, but is received directly from a connected target. It can contain other external roles, in other words:

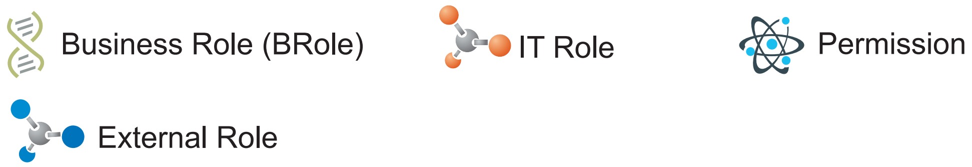
- External Roles
- Permissions

Remember: Because an external role originates from without IBM Security Identity Governance and Intelligence virtual appliance, it is handled as a unit. The permissions that constitute it cannot be separated from the role and handled individually.

Business Role
Any combination of application permissions, IT roles, external roles, and other business roles. Different business roles can be defined in the same organizational unit. It can contain:

- Business Roles
- IT Roles (Application Roles)
- External Roles
- Permissions

The following icons represent these entitlements:



If notes about the considered entitlement are in the request, the **Note** icon is available. Click it to open the Notes window and show the contents of the note.

In the central side of the frame, you find:

- Elements related to the request to be authorized.
- Elements related to the approver of the request.

Select an option at the bottom to process the request.

Back Returns you to the list of requests without acting.

Approve
Approves the request.

Reject Rejects the request.

Redirect
Redirects the request to another approver. The Request Redirection window displays a list of candidate users. Select the user to whom you want to redirect the request for approval or rejection.

This option does not change the status of the request.

Send Back
This option is displayed only if the request was redirected to you by the original approver. You can return the request to the original approver, if you determine that you cannot approve or reject it. Write comments in the **Additional Notes** box.

This option does not change the status of the request.

Insert/Update user: executing a request

For this type of authorization workflow the execution step is an empty step.

For technical reasons of compatibility, this workflow is ended by an empty execution step, that don't requires any action.

Chapter 38. Introduction to Business Activity Mapping

Business Activity Mapping (TT) module aimed at managing relations between permissions and activities

The Business Activity Mapping module allows the user to act on these relations from two perspectives:

- Permissions-Activities
- Activities-Permissions

Dashboard

The upper part of the Dashboard contains a summary of the following permission statuses:

Linked
The permission is joined to an activity.

Ignored
The permission is not joined to any activity.

Missing Activity
The operator does not know to which activities to join the permission.

To be Defined (TBD)
The permission is not joined to any activity but is not in the **Ignored** or **Missing Activity** status.

The green status bar and the numbers **X/Y** change according to the number of permissions processed.

For example, the following figure shows 342 permissions to process, where 90 are **Linked**, 0 are **Ignored** or in **Missing Activity**, and 252 are **To be Defined**.

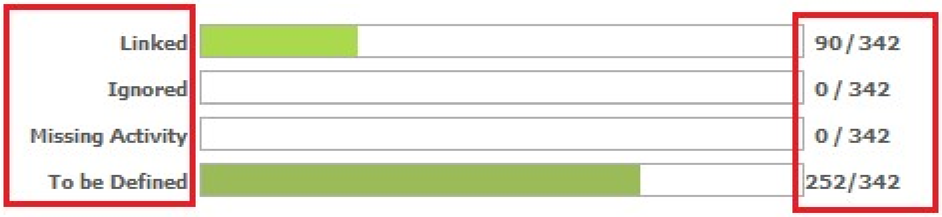


Figure 148. Summary of permissions statuses

The upper right part of the page contains information about **Last Changed** and about the user who made them.

The ℹ icon here indicates that the data beyond the green status bar refers to the number of the permissions and not to the association between entities.

The following filters are available by clicking **Filter/Hide Filter**:

Table 645. Dashboard filters

Filter	Description
Application	Clicking ⋯ **Application** opens the Applications window. You can select the available application from the list. The list of available applications changes, depending on the visibility of the user.
Activity	Clicking ⋯ **Activity** opens the Activities window. You can select activities from the **Activity tree** tab or search from the **Activity** tab.
Permission	Name of the permission.
Status	Status of the permission • **To be Defined** • **Linked** • **Ignored** • **Missing Activity**

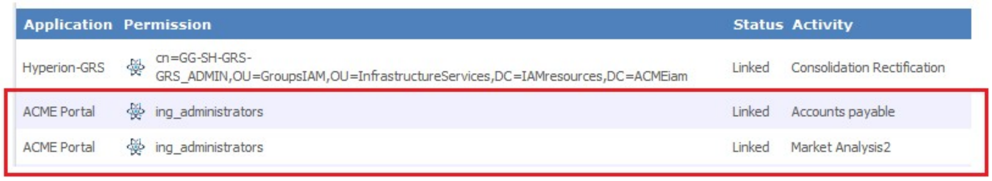
The results are displayed in the same page and summarize the associations made according to the following attributes:

Table 646. Dashboard details

Detail	Description
Application	Name of the application.
Permission	Name of the permission.
Status	Status of the permission.
Activity	Activity that is associated with the permission.

If the same permission is joined to more than one activity, the permission is displayed several times.

Figure 149. Permission-activity relationship



Application	Permission	Status	Activity
Hyperion-GRS	cn=GG-SH-GRS-GRS_ADMIN,OU=GroupsIAM,OU=InfrastructureServices,DC=IAMresources,DC=ACMEiam	Linked	Consolidation Rectification
ACME Portal	ing_administrators	Linked	Accounts payable
ACME Portal	ing_administrators	Linked	Market Analysis2

Permission Perspective

On this tab, you can associate Permissions with one or more Activities.

On the **Permission** tab (left), you can search a specific Permission with the following filters. (Click **Filter/Hide Filter**.)

Permission filters	
Filter	**Description**
Application	Name of the Application. Click ... **Application** to open the Applications window. You can choose the available Application from the list. The list changes depending on the User's visibility.
Permission	Name of the Permission.
Status	Status of the Permission.

Results are displayed in the same frame according to the following attributes:

Permission attributes	
Attribute	**Description**
Status	Status of the Permission.
Permission	Name of the Permission.
Application	Name of the Application.

On the **Permission** tab, click a Permission to enable the **Details** tab (right).

The upper part of this frame displays information about the selected Permission. It also displays two radio-buttons to switch the status of the selected Permission from **TBD** to **Ignore** or **Missing Activity**.

Permission details	
Detail	**Description**
Name	Name of the Permission.
Application	Name of the Application.
Description	Brief description of the Permission.

The **Actions** menu provides the following functions:

- **Add** assigns an Activity to the selected Permission.
- **Remove** removes an Activity from the selected Permission.

When the Permission-Activity association is removed, the status of the Permission returns to **To be Defined**.

When you finish, click **Save** on the lower right side of the frame.

Note: When a Permission is in **Linked** status, you cannot change to any other status. To switch the status of the Linked permission, you must remove the joined Activity.

Business activity Perspective

You can associate activities to one or more permissions or groups.

On the **Business activity tree** tab, you can browse the activity tree for the required activity. On the **Business activity** tab, the Name (name of the activity) and the Identifier (univocal identifier of the activity) filters for search activity are indicated. Click the **Filter/Hide Filter.**

On the **Business activity** > **Actions** menu, **View** switches from the Business activity flat view to the hierarchical view (**Business activity tree** tab).

By selecting an activity from the list, the **Details** tab is enabled and shows the permissions and groups that are joined to the selected activity.

The **Actions** menu provides the following functions:

- **Add Group** adds a root level group that is identified as **`PROFILE_GROUP_random_number`**

  Where

  `PROFILE_GROUP` is a fixed string.

  `random_number` is a random label that is composed of five ciphers.You cannot modify this name. A root level group can include permissions and groups. The groups included in the root level group are identified by the **Group** icon.
- **Add Permision** adds a permission directly to the selected activities or to a group.
- **Add Rights** is enabled only if the activity is joined to a permission with rights, and it can define the values for the rights.
- **Remove** removes permissions and groups. Removing a group instantly removes everything that is joined with the group.
- **And/Or** inverts the value of the Boolean condition of the selected node (Groups, Permissions, and Rights).

Note: The **`AND/OR`** condition is applied to all properties of permissions and groups and to everything contained in the groups. This condition is useful for the `segregation of duty` analysis.

Chapter 39. Introduction to Report Client

Report Client (RC) module allows to configure and run reports designed by the administrator through Report Designer.

IBM Security Identity Governance and Intelligence Report Designer module's front-end component, provides a modeler that can outline every type of report. Using this modeler, the administrator can visually describe the entire report creation process.

Configuring a report determines:

- The data model entities that are in the report
- The output format of the report
- The scheduling of the effective run of the report

These three main actions are supported by a wizard.

Users can configure all the aspects of the report with a discrete number of steps, which vary according to the report.

Report

The following functions for managing the main entities of this module are available:

- Request
- Download
- Passphrase

Note: For unauthorized users, the **Reports** menu is not active. If the menu is active but the **Request** tab is empty, no reports are assigned to or available for the user who is logged in.

Request

The left side of the Reports page is tree-structured and contains the assigned reports. Reports are always the leafs of the hierarchy.

All elements of the report set are represented as leaf nodes. Every node is labeled with the report name that was created by an administrator of the Report Designer (RD) module.

The Report Designer administrator can classify the available reports into a hierarchy of folders that are labeled with specific names. Every folder can contain specific set of reports. A folder can contain a set of report (leaves of the hierarchy) or other folders. You can recursively repeat this structure for each folder.

When the authorized user considers a report, that user can configure some settings, which are organized into a wizard that has several steps. The available settings are outlined by the administrator of the Report Designer module.

If the user does not add an item to the **Assigned Applications** page, all the **Visibility-Entities** are selected for the report.

After the report is configured, click **Execute** as the last step.

The Report Configuration wizard: how to configure a report

The configuration of a report is managed with a wizard, which is an interactive utility that guides users through a multistep process.

In every step of the wizard, the user can configure a specific tab, which is dedicated to a limited subset of information.

The user can navigate back and forward through the sequence of steps in the wizard.

See the sequence of steps for the configuration wizard in the following table:

Table 647. Configuration steps

Step (tab)	Description	Always/Optional
Details tab	Shows the description of the report (read-only).	Always present
Visibility - Users tab	Specifies which users are considered in the report generation.	Optional
Visibility - Applications tab	Specified which application is considered in the report generation.	Optional
Visibility - Entitlements tab	Specifies which entitlements are considered in the report generation.	Optional
Visibility - Organization Units tab	Specifies which organization units are considered in the report generation.	Optional
Visibility - Activities tab	Specifies which activities are considered in the report generation.	Optional
Visibility - Configurations tab	Specifies which type of account configurations are considered in the report generation.	Optional
Filters tab	Specifies which type of filters are used for the report generation.	Always present
Schedule tab	Specifies the scheduling parameters for the report.	Always present

Download

After you run a report, you can check its status or download it.

The following table describes the various status labels for reports:

Table 648. Status labels for reports

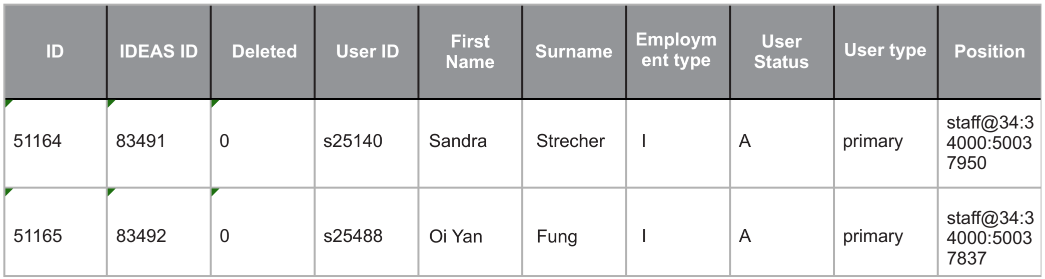
Status	Description
Pending	The report is waiting to run.

Table 648. Status labels for reports (continued)

Status	Description
Running	The report is running.
Download	The report can be downloaded by the user.
Error	An error occurred while the report was running.

Note: When the report is in the Download status, you can download it so it cannot be deleted.

The following figure shows a sample report in XLSX file format (User Imported report):



ID	IDEAS ID	Deleted	User ID	First Name	Surname	Employment type	User Status	User type	Position
51164	83491	0	s25140	Sandra	Strecher	I	A	primary	staff@34:34000:50037950
51165	83492	0	s25488	Oi Yan	Fung	I	A	primary	staff@34:34000:50037837

Figure 150. Report sample: User Imported

If provided by the Report Designer administrator, the report can have either a cake or bar chart, as shown in the following example:

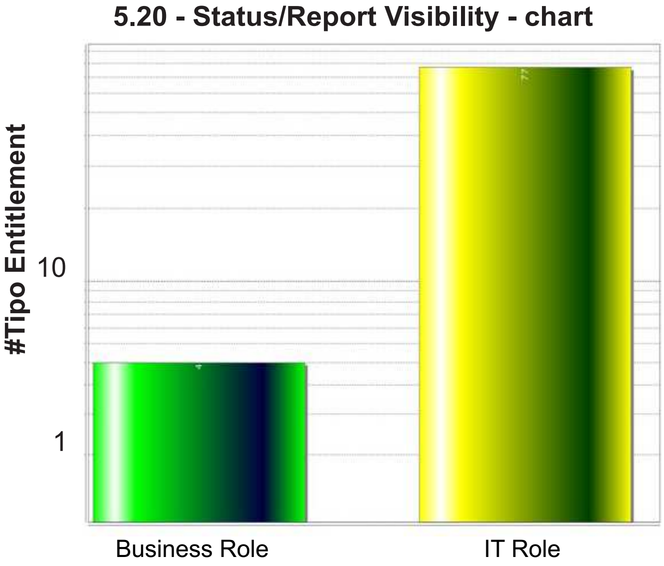


Figure 151. Chart: Bar type

Passphrase

A report console user can receive an email that contains a passphrase so that the user can download a report that was run by another user.

Set the received passphrase in the Download Report window and follow the system dialog window to download the report.

Use this method to obtain a report that is not in the set of available reports for the logged in user. See the **Request** tab.

Part 3. Employees

Employees are defined in the *Regular Users schema* and can perform tasks in the Service Center.

For more information about the tasks that employees can do, see Personas and use cases.

Chapter 40. Logging in to the Service Center

When you log in to the Service Center for the first time, you are prompted to provide answers to security questions.

Before you begin

You must have your user ID and password from your system administrator.

About this task

The Service Center includes applications that are intended for users who are not administrators. Business users, such as managers and employees can do tasks in the Service Center, depending on the access that is granted to them by an administrator.

The Self Care application is available in the Service Center. Within the Self Care application, employees can change their account passwords, view their password change requests, and update their security questions.

Be sure to change your password after you log in to the Service Center for the first time.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**.
2. Select the security questions and provide answers that you can easily remember. The answers are not case-sensitive.
3. On the Service Center home page, click the application menu icon, and select **Self Care**.

What to do next

You can change your account password, view your requests, and update your security questions from the Self Care application.

“Resetting my forgotten password” on page 673
If you forgot your Service Center password, you can either specify a new password or have the system generate new password.

Chapter 42, “Changing my account password,” on page 899
Employees can change their own passwords by using the Self Care application in the Service Center.

Chapter 43, “Viewing my requests in the Self Care application,” on page 901
You can view your requests by using the Self Care application in the Service Center.

Chapter 44, “Updating my security questions,” on page 903
You can set up your account recovery security questions and answers by using the Self Care application in the Service Center.

Chapter 41. Resetting my forgotten password

If you forgot your Service Center password, you can either specify a new password or have the system generate new password.

Before you begin

The administrator must configure the forgotten password service in the Administration Console. Otherwise, the **Forgot your password?** link does not display on the Service Center Login page. For more information, see "Configuring password services" on page 110.

Your security questions must already be set up. For more information, see Chapter 44, "Updating my security questions," on page 903.

About this task

When you forget your password, you must answer the security questions correctly to reset your password. The new password replaces the old password for your Service Center account. Depending on how your system is configured, you can either specify a new password or use a system-generated password. The new password is sent to the email address that is specified in your personal profile.

If no email address is defined in your personal profile, the system-generated password cannot be sent. Contact the help desk or administrator to add an email address to your profile.

Procedure

1. From the Service Center Login page, type your user ID, and then click **Forgot your password?**
2. On the Forgot Your Password page, answer the security questions, and then click **Continue**. The following scenarios are possible, depending on how a system administrator configured the system:

Option	Description
The questions are answered correctly, and your system is configured for you to specify a new password.	Type your new password in the **New Password** field, and then type your new password again in the **Confirm Password** field. Then, click **Change Password**. When you see a message that indicates a successful password change, click **OK**.
The questions are answered correctly, and your system is configured to generate a new password and send the password to a predefined email address.	A new system-generated password is automatically sent to the email that is defined in your personal profile. You must use this new password on your next login, and then you can change your password on your next login. Click **Return to Login**.

Option	Description
The questions are answered correctly, and your system is configured to generate a new password and prompts you to type an email address.	Type the email address where you want the new system-generated password to be sent. You must use this new password on your next login, and then you must change your password on your next login. Click **Continue**. When you see a message that indicates a successful operation, click **Return to Login**.
The questions are answered correctly, and your system is configured to generate a new password. However, an email address is not defined in your personal profile.	Contact the help desk or administrator to add your email address to your personal profile. Click **Return to Login**. After the email address is added to your profile, you can follow the **Forgot your password?** link again from the Service Center Login page to receive the system-generated password in your email address.
The questions are not answered correctly, and an error message is displayed. Depending on how your system is configured, you might have more attempts to correctly answer the questions.	You cannot access the system unless you remember your password or answer the questions correctly. If you exceed the maximum number of attempts to verify your identity, your Service Center account is locked. Contact your help desk or administrator to unlock your Service Center account or reset your Service Center password.

Related reference:

Chapter 34, “Forgot Your Password,” on page 677
If you forgot your Service Center password, you can reset it.

Chapter 42. Changing my account password

Employees can change their own passwords by using the Self Care application in the Service Center.

Before you begin

If single sign-on is not enabled, you must know your current Service Center password.

About this task

Depending on how a system administrator configured the system, you can change your password by using the Self Care application in the Service Center.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**. The Service Center home page is displayed.
2. On the Service Center home page, click the application menu icon, and then select **Self Care**. The Self Care page is displayed.
3. On the Self Care page, click the **Change My Password** tab.
4. Select the accounts that you want to change the password for, and click **Change Password**. Click **Filter** to show options for filtering the list of accounts. You can search for accounts by name or user ID. To toggle the filter off, click **Hide Filter**. The Change Password window is displayed.
5. In the **Current password** field, enter your current Service Center password. This field is displayed only if single sign-on is *not* enabled.
6. In the **New password** field, type a new password, and then type the new password again in the **Confirm password** field. Then, click **Change Password**. Your new password must conform to the rules that are indicated on the Change Password window. The system administrator configured the rules in the Administration Console.
7. When an information message is displayed, which indicates that the request was successfully submitted, click **OK**.
8. Check the status of your password change request. See Chapter 43, “Viewing my requests in the Self Care application,” on page 901. Some requests are immediately completed, while other requests might take more time to complete. Even when the password change request is submitted successfully, it might take time for the password change operation to be complete.

Results

The password is changed, and the Change My Password page is displayed.

What to do next

You can change the password for another account, or do a different task in the Service Center.

Related reference:

Chapter 45, “Change My Password,” on page 905
You can change the password for one or more of your own accounts.

Chapter 43. Viewing my requests in the Self Care application

You can view your requests by using the Self Care application in the Service Center.

About this task

Depending on how a system administrator configured the system, you can do these tasks:

- Check the status of a change password request for your account.
- Check the status of a change password request that a manager or help desk administrator submitted for your account.
- See which requests are complete and which requests are not complete.
- Search for requests that are based on the filter criteria that you specify.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**. The Service Center home page is displayed.
2. On the Service Center home page, click the application menu icon, and then select **Self Care**. The Self Care page is displayed.
3. On the Self Care page, click the **View Self Care Requests** tab.
4. Optional: Click **Filter** to show options for filtering the list of requests. For example, you can view the requests that are completed in the last 30 days. To toggle the filter off, click **Hide Filter**.

What to do next

You can do a different task in the Service Center.

Related reference:

Chapter 46, "View Self Care Requests," on page 907
You can view the requests that you submitted by using the Self Care application in the Service Center.

Chapter 44. Updating my security questions

You can set up your account recovery security questions and answers by using the Self Care application in the Service Center.

Before you begin

You must know your current Service Center password.

About this task

You are required to provide answers to the security questions when you log in to the Service Center for the first time, or when the system administrator changes the security question configuration.

You can update the answers to the security questions whenever you would like to. The steps for changing the account recovery settings are included below.

Procedure

1. From the Service Center Login page, type your user ID and password, and then click **Log In**. The Service Center home page is displayed.
2. On the Service Center home page, click the application menu icon, and then select **Self Care**. The Self Care page is displayed.
3. On the Self Care page, click the **Account Recovery Setup** tab.
4. In the **Security Questions** tab, select the questions from the list and provide answers. Then click **Save**. The account recovery settings are saved.
5. Optional: In the **Contact Information** tab, you can view your email address in the **Primary email address** field.

What to do next

You can do a different task in the Self Care application, such as changing your password or viewing your password change requests.

Related reference:

Chapter 47, "Account Recovery Setup," on page 909
You can configure your security questions in case you need to recover your forgotten password or reset your password in the Service Center Self Care application.

Chapter 45. Change My Password

You can change the password for one or more of your own accounts.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

Select the check box next to one or more of your accounts, and then click **Change Password**.

On the Change Password window, if single sign-on is enabled, you are not prompted to enter your current password. If single sign-on is *not* enabled, then you must enter your current Service Center password in the **Current password** field.

Table 649. Change My Password

Column Name	Description
Active	Indicates whether the account is active.
Name	The account configuration name that is associated with the user ID.
User ID	The user ID of the account.

You can display the results in different ways by using the controls at the bottom of the page:

- Click the drop-down list next to the **Items Per Page** field and select the number of items you want to display on the page.
- Click the arrows to move backward or forward through multiple pages.

Related tasks:

Chapter 42, "Changing my account password," on page 899
Employees can change their own passwords by using the Self Care application in the Service Center.

Chapter 46. View Self Care Requests

You can view the requests that you submitted by using the Self Care application in the Service Center.

Click **Filter** to toggle the filter on, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests and then click **Search**.

Table 650. View Self Care Requests

Column Name	Description
Status	Status of the password change request. The following statuses are valid: **Failed** The request failed. **Pending** The request is waiting for approval. **Performed** The request is in the queue to be completed. **Successful** The request is successful and complete.
User ID	Account user ID.
Name	Account configuration name.
Requester Last Name	The surname of the person who requested the password change.
Requester First Name	The given name of the person who requested the password change.
Submitted	Date that the request was submitted.
Completed	Date that the request was completed.
Request ID	System-generated ID for the request.

You can display the results in different ways by using the controls at the bottom of the page:

- Click the drop-down list next to the **Items Per Page** field and select the number of items you want to display on the page.
- Click the arrows to move backward or forward through multiple pages.

Related tasks:

Chapter 43, "Viewing my requests in the Self Care application," on page 901
You can view your requests by using the Self Care application in the Service Center.

Chapter 47. Account Recovery Setup

You can configure your security questions in case you need to recover your forgotten password or reset your password in the Service Center Self Care application.

You are required to provide answers to the security questions when you log in to the Service Center for the first time, or when the system administrator changes the security question configuration.

You can also update the answers to the security questions whenever you would like to.

The Account Recovery Setup page includes two tabs:

Security Questions
For each question, select a question from the list and then provide an answer that you can easily remember. The answers are not case sensitive.

Contact Information
View your contact information that is configured in the system. If you forget your login credentials, you will be contacted using this information. If this information is incorrect, you cannot recover your credentials. If necessary, ensure that changes are made to this information in your user profile.

Related tasks:

Chapter 44, “Updating my security questions,” on page 903
You can set up your account recovery security questions and answers by using the Self Care application in the Service Center.

Part 4. Appendixes

Appendix. Accessibility features for IBM Security Identity Governance and Intelligence

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Accessibility features

IBM Security Identity Governance and Intelligence Version 5.2.2 is not tested for accessibility.

The online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described at http://www.ibm.com/support/knowledgecenter/about/releasenotes.html.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has established a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see (www.ibm.com/able).

Index

Printed in USA