IBM Security Identity Governance and Intelligence
Version 5.2.3

# *Product Overview Topics*

IBM Security Identity Governance and Intelligence
Version 5.2.3

# *Product Overview Topics*

# Table of contents

# Table list

# Chapter 1. Identity Governance and Intelligence overview

IBM® Security Identity Governance and Intelligence is a network appliance-based integrated identity governance solution. This solution employs business-centric rules, activities, and processes. It empowers line-of-business managers, auditors, and risk managers to govern access and evaluate regulatory compliance across enterprise applications and services.

Identity Governance and Intelligence offers:

- A single identity governance foundation platform to help organizations understand, control, and make business decisions that are related to user access and access risks.
- A business-activity-based approach to facilitate communication between auditors and IT staff and to help determine segregation of duties violations across enterprise applications, including SAP.
- Better visibility and user access control through consolidating access entitlements from target applications and employing sophisticated algorithms for role mining, modeling, and optimization.
- User lifecycle management including provisioning and workflow capabilities, along with integration with IBM Security Identity Manager and third-party tools.
- Access request management that delivers easier-to-implement, business-friendly, self-service access request functions.
- Target integration that automates the process of data collection and fulfillment of identity and access from distributed target systems.
- Persona-based dashboards that help with tasks prioritization.
- Option to authenticate users from an external user registry to the Local Management Interface.
- Options for using the applicable FIPS 140-2 specifications.

For more information about the Identity Governance and Intelligence capabilities and what's new in this release, see the following references:

- “Features overview” on page 5
- Chapter 2, “What's new in Version 5.2.3,” on page 15

## Technical overview

IBM Security Identity Governance and Intelligence is designed to retrieve and manage data from multiple targets through a set of modules, a directory integrator, and a database.

The following diagram illustrates the Identity Governance and Intelligence architecture.

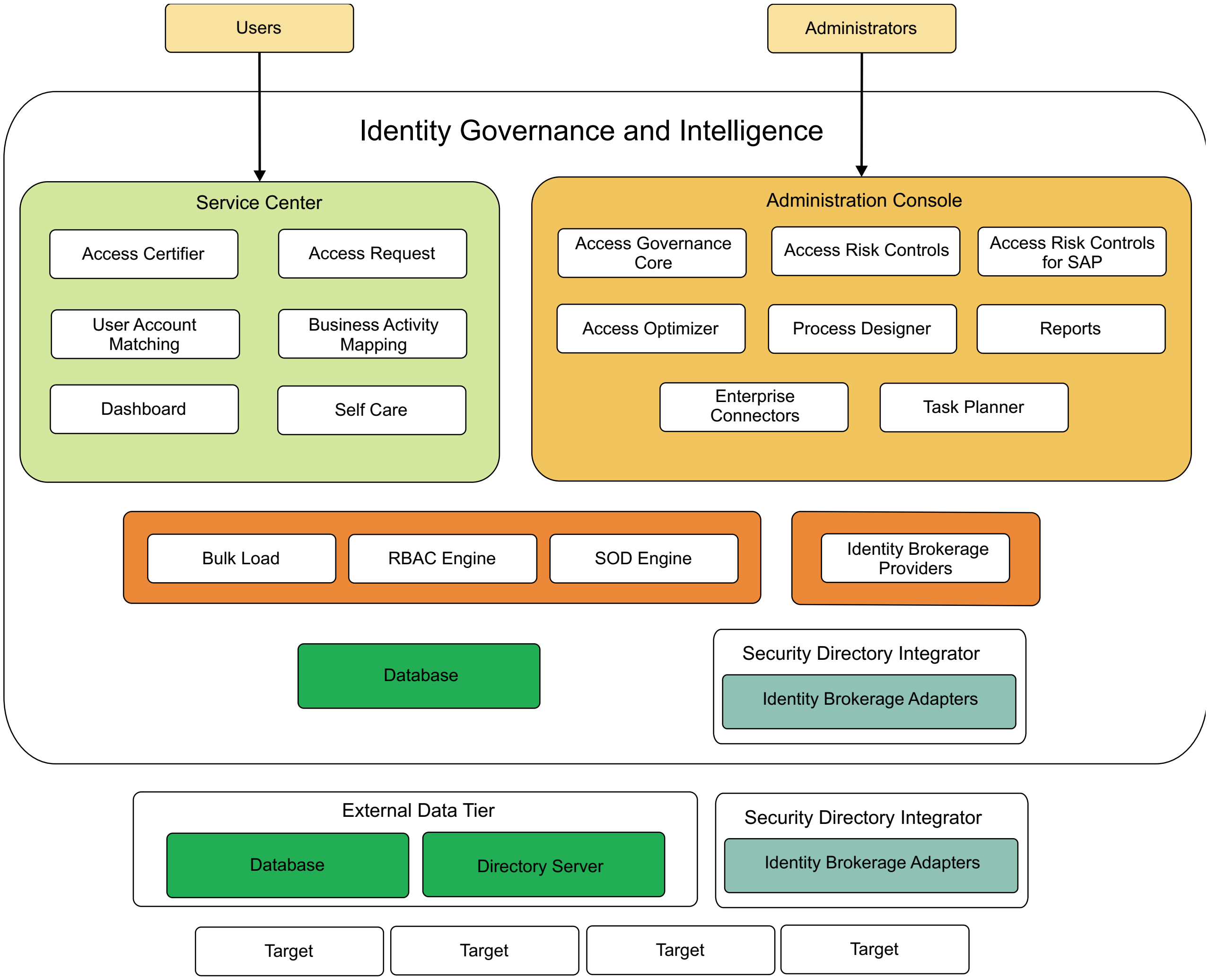

*Figure 1. Identity Governance and Intelligence architecture*

Identity Governance and Intelligence has the following access points, which contains the different modules intended for the Identity Governance and Intelligence administrators and Business users.

- Administration Console
- Service Center

See "Features overview" on page 5 and Chapter 5, "User interface," on page 37 for more information about the user interfaces and the modules.

Identity Brokerage is the gateway to directly integrate Identity Governance and Intelligence with targets and hubs using IBM Security Identity Adapters. These IBM Security Identity Adapters are sometimes referred to as Identity Brokerage Adapters in Identity Governance and Intelligence.

## Directory integrator

The Security Directory Integrator is built-in to the Identity Governance and Intelligence virtual appliance and multiple instances of it can be installed and configured.

The Security Directory Integrator is pre-configured with the following Identity Brokerage Adapters:

- AIX®
- HP
- LDAP
- Linux
- Solaris

All Identity Governance and Intelligence supported adapters can be installed externally on the virtual appliance. Depending on the adapter, an external Security Directory Integrator may be required.

Some IBM Security Identity Adapters can be installed in the selected Security Directory Integrator instance on the virtual appliance:

See the *Identity Adapters* product documentation at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm to determine which adapters are supported in Identity Governance and Intelligence, and which can be installed on the virtual appliance.

## Data tier

The Identity Governance and Intelligence data source is composed of various data entities, which are stored in the database and directory server.

**Database server**

The database server contains the following data entities.

*Table 1. Data entities stored in the database server*

| Data entities | Description |
|---|---|
| Identity Governance and Intelligence data store | It is inherited from the IBM Security Identity Governance data store, but it contains other data artifacts that are used for the Identity Brokerage Providers module.<br>Changes that are initiated from Identity Governance and Intelligence or from external target systems are recorded and processed in an asynchronous manner through queues.<br>Identity Governance and Intelligence support backward compatibility with existing IBM Security Identity Governance releases to support database upgrade. |
| Identity Brokerage data store | It contains data entities that are used by Identity Brokerage. |

The virtual appliance can be deployed with an internal Postgres database or an external database. For the supported external database server and directory server, see the IBM Security Identity Governance and Intelligence *Software Product Compatibility Report*, http://www-969.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.

The Virtual appliance administrator can later change the setup, from using an internal database to using an external database. See Managing the database server configuration and Managing the Postgres database.

**Directory server**

Data that is stored in the directory server includes the target configuration and target cache. Identity Brokerage uses these data entities when processing change requests.

## Data models

The Identity Governance and Intelligence database model is patterned on how the organization is structured in terms of the:

- Different entities that are registered in the organization
- Links and relationships between these entities
- Sets of application policies and processes that the organization uses to manage those entities

Identity Governance and Intelligence consists of a core data model and an extended data model.

*Table 2. Data models*

| Data models | Elements |
|---|---|
| Core data model<br>This data model contains elements that define the organizational structure. | • Organization units<br>• Users<br>• Entitlements<br>• Resources<br>• Rights<br>• Applications<br>• Accounts |
| Extended data model<br>This data model contains elements that support the risk definition and detection layer of Identity Governance and Intelligence. | • Business activities model and application permissions<br>• Risk definition and detection<br>• Segregation of Duties<br>• External SoD<br>• Risk mitigation<br>• Mitigation actions<br>• Domains<br>• Risk hierarchy |

## High availability and disaster recovery

Implementing high availability is about ensuring that services are always available. Disaster recovery is the process of restoring the service to a production state in the event of an outage.

To deploy Identity Governance and Intelligence with high availability, set up a virtual appliance cluster and use a load balancer. See Planning for high availability.

If the master Postgres database fails or the primary node becomes unavailable, follow the failover procedure to recover the system. See Recovering from a Postgres database failure.

For a basic level of disaster recovery, set up the Identity Governance and Intelligence virtual appliance into two appliances with active-passive configuration. See Setting up a secondary virtual appliance for active-passive configuration.

# Features overview

IBM Security Identity Governance and Intelligence is an appliance-based, integrated identity governance and administration solution, which offers several capabilities.

## Simplified virtual appliance deployment and administration

Identity Governance and Intelligence provides:

- A configuration wizard for the first time configuration of the virtual appliance, and for creating clusters.
- A virtual appliance dashboard, a tool to:
  - Access the Administration Console and Service Center.
  - Quickly view the disk usage, partition information, available interfaces, notifications, middleware status, cluster status; and control the server status.
  - Monitor system event logs, memory, CPU, and storage usage, and configure the Simple Network Management Protocol.
  - Configure the directory server, database server, OpenID connect providers, and mail server.
  - Configure and manage the Postgres replication, IBM Security Directory Integrator instances, and cluster nodes.
  - Manage custom files, and certificate stores.
  - Manage the virtual appliance updates and licensing.
  - Manage the virtual appliance and Identity Governance and Intelligence logs retrieval and configuration, core dumps, Identity Brokerage Providers configuration, and build information.
  - Manage network settings such as application interfaces, hosts files, static and system routes, and the network file system.
  - Manage the Export and Import settings
  - Manage the virtual appliance administrator settings, and system settings such as tuning parameters, snapshots, support files, system audit events, BiDi properties, and management authentication.

## Access governance

Identity Governance and Intelligence provides an identity governance infrastructure based on business requirements rather than on IT processes. Users are classified by organizational roles, group membership, job activities, and access needs, not as individuals.

Using the Identity Governance and Intelligence Access Governance Core module, Identity Governance and Intelligence administrators can outline the organizational structure in terms of its units, users, accounts, entitlements, resources, rights, and applications. The module aligns the IT teams, business managers, and auditors to model the company organization and operating processes.

Business managers can assign and evaluate appropriate user roles and access privileges.

IT staff can automate the creation, modification, and termination of user access. There are audit trails and detailed reports, periodic review and certification of privileges, and detection and correction of non-compliant accounts.

See Introduction to Access Governance Core.

## Access risk assessment and management

Segregation of Duties (SoD) is designed to manage conflicting relationships between certain model entities. Entities that are characterized by reciprocal conflict cannot be aggregated to the same user. Segregation of Duties violations can reveal security vulnerabilities and cause serious damage when users have access to highly sensitive data. The Identity Governance and Intelligence data model identifies a Segregation of Duties violation as a specific type of risk.

Identity Governance and Intelligence helps mitigate access risks and Segregation of Duties violations through its Access Risk Controls module. It reduces risks by identifying violations and preventing users from conflicting activities. Managers and resource owners can use the information gathered to close inactive, unauthorized, and outdated accounts.

There is also the option of managing an External SoD. Identity Governance and Intelligence displays user risk information from external target systems.

The Access Risk Controls module manages the risk definition and detection layer based on two relationships:

- The relationship between the business activities model and the application permissions.
- The relationship between risks and business activities.

See Introduction to Access Risk Controls.

## Access certification

Users' access entitlements tend to grow over time if they are not managed. Periodic review prevents users from acquiring accesses that are not necessary for their jobs. Regulations, such as Sarbanes-Oxley, require that companies periodically review all users' access rights and certify that these rights are correct.

Identity Governance and Intelligence ensures that access entitlements and rights are granted to authorized users only. It monitors and ensures that users' accesses are up-to-date and at the appropriate levels. When user access and entitlements are granted, potential Segregation of Duties violations are identified.

Identity Governance and Intelligence uses the Access Certifier module to enable managers and resource owners to do the following tasks:

- Review, on a periodic basis, the access that their users have on resources.
- Certify that the access rights are appropriate for users and applications and are still reasonable, based on policy and business needs.

If there are changes to the role or access is no longer required, it is revoked.

See Introduction to Access Certifier.

## Audit and reports

External audits ensure that the organization is current with government and industry regulations. Taking an internal audit of the employees, contractors, and business partners is also an essential part of securing the gateway to your organization. Proper tracking and auditing helps to gain deep insights and essential visibility into all accounts, access privileges, and entitlements across all users.

Identity Governance and Intelligence optimizes visibility into user access, privileges, and policies, which is an essential identity security capability. It consolidates access entitlements from enterprise applications in a central repository. It structures them into business roles and activities as collectively defined by business divisions, IT staff, and auditors.

All Identity Governance and Intelligence modules send notifications to the Audit module for large sets of operations. IT teams, business managers, and auditors can run regular reports to determine where and when users gained access and what users are doing with it. It provides documentation of who granted access to whom and when. Identity Governance and Intelligence highlights Segregation of Duties violations.

Reports are defined through the Report Designer and Report Client modules.

See Introduction to Report Designer and Introduction to Report Client.

## Access optimization

Identity Governance and Intelligence uses the Access Optimizer to:

- Evaluate the business rules and controls and current Identity Management policies that are enforced.
- Review the accounts, access privileges, and entitlements across all users and determine inactive, unauthorized, and outdated accounts that require action.
- Enhance governance and provide valuable intelligence to the organization.

See Introduction to Access Optimizer.

## Automated identity governance and control processes

Identity Governance and Intelligence streamlines and automates the following processes through the Administration Console and Service Center:

- Access request management processes
- Certification and re-certification processes

## Workflow and policy management

Administrators can create and manage authorization policies on entitlements through the Access Governance Core and Process Designer modules. Entitlements that require control, can be assigned with a policy that:

- Controls the visibility of the entitlement.
- Defines the conditions under which users can have access without requiring approval.
- Identifies which person or group approves the access request.

## Entitlements management

Entitlements management is concerned with maintaining the entitlements repository. Identity Governance and Intelligence provide a means to capture, organize, and assign the accounts and other entitlements that determine the access that users have across the environment. Entitlements can take many forms, but they are most commonly reflected in target systems as accounts, group memberships, role assignments, and access levels.

## Target profile administration

Target profile integration automates the process of collecting data from distributed target systems and reflects changes that are initiated from Identity Governance and Intelligence in these target systems. Target systems are user repositories that contain user account information.

Identity Governance and Intelligence provides two methods of integration with target systems, using Identity Brokerage Adapters and Enterprise Connectors.

Identity Brokerage is the gateway to directly integrate Identity Governance and Intelligence with targets and hubs using IBM Security Identity Adapters. These IBM Security Identity Adapters are sometimes referred to as Identity Brokerage Adapters in Identity Governance and Intelligence.

Identity Governance and Intelligence administrators can use the Enterprise Connectors module to perform target profile and connector administration, including:

- Import target profiles.
- Import account attribute mapping files.
- Configure account defaults for target profiles.
- Search, add, modify, and delete target profiles.
- Manage reconciliation and synchronization of change logs.
- Set up account defaults for a target.

See the following topics:

- Target profile administration
- Target management using Enterprise Connectors

## Identity Brokerage Adapters and Enterprise Connectors

The following table summarizes the similarities and differences between the Identity Brokerage Adapters and Enterprise Connectors.

*Table 3. Comparison between the Identity Brokerage Adapters and Enterprise Connectors*

| **Compare** | **Identity Brokerage Adapters** | **Enterprise Connectors** |
|---|---|---|
| Framework | Identity Brokerage | Enterprise Connector Framework |
| Target integration | Identity Administration Points (IAP) | Identity Administration Points (IAP) |
| Repository | Identity cache and metadata that is stored in LDAP v3 store | Cache |
| User interface | **Administration Console** > **Enterprise Connectors** | **Administration Console** > **Enterprise Connectors** |

Table 3. Comparison between the Identity Brokerage Adapters and Enterprise Connectors (continued)

| Compare | Identity Brokerage Adapters | Enterprise Connectors |
|---|---|---|
| Custom integration | Its framework can be used to develop a custom adapter to integrate with target systems that are currently not supported by Identity Governance and Intelligence.<br>The Identity Brokerage Adapters framework provides out-of-the-box functionality for all adapters that are deployed within the Identity Brokerage.<br>See the *Identity Brokerage Adapters Development and Customization Guide* at Adapters for IBM Security Identity Manager v7.0: http://www-01.ibm.com/support/docview.wss?uid=swg21687732, for information about adapter customization. | Its framework can be used to develop a custom connector but it is advised that you use the Identity Brokerage Adapters framework instead to integrate with target systems that are currently not supported by Identity Governance and Intelligence. |

## Password administration and management

Identity Governance and Intelligence offers change and reset password capabilities for the following passwords:

- The Service Center password is used to log in to the Service Center.
- The account password is used to access the accounts that a user is entitled to use.

Employees can change their account passwords on their own by using the Self Care application, or they can contact their Manager or Help Desk to reset the password. If they forgot their Service Center password or if it expired, they can reset it using the **Forgot password** feature of the **Service Center**. See Logging in to the Service Center.

When granted the permission, using the **Service Center** > **Access Requests** application:

- Managers can reset the account passwords for their Employees.
- Help Desks can also reset the account passwords for other users.

See Password management.

The Identity Governance and Intelligence administrator:

- Configures these password services through the **Access Governance Core** module in the Administration Console.
- Configures the following Access Requests workflows for the *Account Change* process, through the **Process Designer** module in the Administration Console:
  - ChangePassword
  - ForgotPassword
  - ManagePasswordReset
  - HelpDeskPasswordReset

- Can force users to change their Service Center password on their next log in to the Service Center.

See Password administration.

### Persona-based dashboards

Dashboards help a user view several conditions at a glance and respond quickly. They are aligned with Administrator Roles. When a user logs in to Service Center, the home page shows all dashboard items for all Administrator Roles assigned to the User.

### Self-service features

Identity Governance and Intelligence provides a Service Center for Business users to do access request, access certification, access analytics, reporting, and password management tasks.

Self-service features help make access or change request tasks more accurate, appropriate, and secure. First-time users can submit a request without assistance from Help Desks or Managers.

Employees can use the Self Care application to change their own passwords and update their *security questions*. They can also view the status of their password change requests.

## Cross-product integrations

IBM Security Identity Governance and Intelligence can be used with other security products to deliver an integrated solution.

### Integration with IBM Security Identity Manager

IBM Security Identity Manager is an automated and policy-based solution that manages user access across IT environments. By using roles, accounts, and access permissions, it helps automate the creation, modification, and termination of user privileges throughout the entire user lifecycle. It centralizes the process of provisioning and accessing user accounts on the operating systems and applications.

Organizations with IBM Security Identity Manager implementation can leverage IBM Security Identity Governance and Intelligence for the following scenarios:

- Attribute hierarchy
- User access certification and accounts certification for employees
- Risk management for employees
- Risk scoring and trends
- Role management for employees
- On-boarding a new application
- User and entitlement re-certification
- Attribute mapping service
- Bulk load extension to import role-permission relation
- Standardized authentication across applications and services

Use the IBM Security Identity Governance and Administration Data Integrator to synchronize the following information between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence:

- User account
- Roles
- Services
- Groups
- Organization unit
- Entitlement changes

See the following references to implement the integration:

- Cookbook for IBM Security Identity Governance and Intelligence integration with IBM Security Identity Manager
- *Integration between IBM Security Identity Manager and IBM Security Identity Governance* at http://www-01.ibm.com/support/docview.wss?uid=swg21968516.

## Integration with IBM Security Privileged Identity Manager

IBM Security Privileged Identity Manager helps organizations manage, automate, and track the use of shared privileged identities.

Organizations can use IBM Security Identity Governance and Intelligence together with IBM Security Privileged Identity Manager for the re-certification of privileged user's access entitlement.

With the IBM Security Directory Integrator based Privileged Identity Manager adapter, the Identity Governance administrator can bulk load privileged users' access entitlements into Identity Governance and Intelligence.

The integration supports the following:

- Reconciliation of users and access entitlements
- Reconciliation of users entitlement assignments
- Assignment and revocation of accesses to and from users

The IBM Security Privileged Identity Manager integration does not support:

- Reconciliation of admin roles, and domain admins
- Reconciliation of credentials and credential pools associated with an access
- Reconciliation of the credentials and credential pools granted to a user
- Automatic fulfillment of users including creations and modifying users attributes
- Automatic fulfillment of admin roles (entitlement assignments)
- Automatic fulfillment of domain admins (entitlement assignments)

See the following references to implement the integration:

- *IBM Security Privileged Identity Manager (SDI-based) Guide* at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm

## Integration with IBM Security Access Manager

IBM Security Access Manager helps organizations secure and manage user access and protect applications against fraudulent or unauthorized access.

Organizations that already uses IBM Security Identity Manager, and IBM Security Access Manager for single sign-on can enable IBM Security Access Manager based authentication on Identity Governance and Intelligence to implement single sign-on authentication between the IBM Security Identity Manager and IBM Security Identity Governance and Intelligence Service Center.

The Identity Governance and Intelligence Service Center authentication can be based on the *OpenID Connect Protocol*, with the application server configured as an *OpenID Connect* relying party pointing to an *OpenID Connect Provider*. The Identity Governance administrator can set up an *OpenID Connect Federation* between IBM Security Access Manager and IBM Security Identity Governance and Intelligence.

See the following references to implement the integration:

- Managing OpenID connect configuration
- **Access Governance Core** > **Settings** > **Core Configurations** > **Login User ID**

## Lightweight Third-Party Authentication (LTPA) based single sign-on

Lightweight Third Party Authentication (*LTPA*) is a single sign-on credential format. With *LTPA*, the user authenticates with the first server that is accessed, by using a user name and password. After authenticating, the user receives an *LTPA key*, which is only valid for one session. The token is used to identify the user on other servers within the same domain name system, where the servers are configured to use *LTPA*. Therefore, the user enters a user name and password only once, and the user directory is accessed only once to verify the identity of that user.

Organizations can enable single sign-on between the IBM Security Identity Manager and IBM Security Identity Governance and Intelligence Service Center without external authentication, by exploiting the *LTPA key* generated directly by the application servers. A user who got authenticated through the IBM Security Identity Manager Service Center login page, can access the IBM Security Identity Governance and Intelligence Service Center without re-authenticating and vice-versa.

Manage the *LTPA* based single sign-on through the Virtual Appliance Dashboard **Configure** > **Manage Server Setting** > **Single Sign-On Configuration**. It includes options to import, export, or generate the *LTPA key*

See the following references to implement the integration:

- Managing LTPA-based single sign-on configuration
- **Access Governance Core** > **Settings** > **Core Configurations** > **Internal authorization**

## Integration with zSecure

IBM® Security zSecure™ Manager for RACF® z/VM® improves the efficiency of IBM Resource Access Control Facility (RACF®) administration and auditing compliance. It automates functions to help optimize IT resources, mitigate complexity, improve security and quality of service, demonstrate regulatory compliance and reduce errors and costs in virtual machine environments.

The IBM Security Identity Governance and Intelligence adapter works with the zSecure RACF product on an MVS™ environment. The adapter:

- Receives requests from IBM Security Identity Governance and Intelligence.
- Processes the requests to reconcile user, group, and resource profile access information from the zSecure RACF CARLA scripts, which consult the Resource Access Control Facility (RACF) security server database.
- Returns the results of the zSecure RACF CARLA scripts commands, which include the success or failure message of a request to the IBM Security Identity Governance and Intelligence server.
- Processes the requests to add, modify, or delete RACF user accounts by using the R_admin callable service (IRRSEQ00).

See the following references to implement the integration:

- *zSecure RACF Guide* at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm

## Integration interfaces

Application programming interfaces (APIs) are part of a plug-in model that you can use to add applications without disrupting existing applications. The REST APIs provide third-party applications some functionality and the interface for operating with Identity Governance and Intelligence.

Identity Governance and Intelligence supports:

- REST API calls to the Identity Governance and Intelligence external authorization services.
- Virtual appliance REST APIs to administer tasks outside the virtual appliance user interface.
- Identity Brokerage REST APIs for managing accounts, groups membership, and permissions.

See the following references to implement the integration:

- Application programming interfaces

# Chapter 2. What's new in Version 5.2.3

This version delivers enhancements in the virtual appliance deployment, product and security integration, and in the technical foundation.

## Option for using the applicable FIPS 140-2 specifications

IBM Security Identity Governance and Intelligence provides now the option to run in FIPS 140-2 mode.

When in FIPS 140-2 mode, IBM Security Identity Governance and Intelligence uses the FIPS 140-2 approved cryptographic provider; IBMJCEFIPS (certificate 376) and/or IBMJSSEFIPS (certificate 409) and/or IBM Crypto for C (ICC (certificate 384) for cryptography.

To run in FIPS 140-2 mode, you must select the option to enable it in the virtual appliance setup wizard that runs the first time that you connect to the virtual console of an unconfigured virtual appliance.

This automatically enables to FIPS also the peripheral components of Identity Governance and Intelligence such as: the PostgreSQL internal database, the WebSphere® Application Server, and the Java™ Runtime Environment.

You must also configure for SSL the virtual appliance features that you are using, such as the external database server, the mail server, the directory server, and the LMI authentication option from external user registries, and either accept the default digital certificate or import your own one.

If you plan to work with the Access Risk Controls for SAP module, and connect with a FIPS-enabled SAP system, you must create certificates and properly configure the SAP system details pane in the Access Risk Controls for SAP module.

See Support for FIPS 140-2 specifications for more information.

## Account Management

IBM Security Identity Governance and Intelligence provides several advanced features for managing user accounts.

The account management features are present in three modules:

- Access Governance Core
- Process Designer
- Access Requests

In Access Governance Core you can:

- Build by scratch a new account, setting the account attributes and the related properties (see Target Attributes).
- Load an external account (see Discovering attributes from an imported account).
- Manage multi-values attributes.

In Process Designer, you can define new work flows for creating or updating an account. Through dedicated configurations, you can filter the account to be managed, possibly choosing only a subset of attributes of a specific account deployed in Access Governance Core.

Another new feature is related to the possibility of setting a user account together to the assignment of a role.

The configurations that are provided by Process Designer, can be consumed by work flow processes that you can access through Access Requests.

## Target Administration Console is converged with Enterprise Connectors module

The functions from the Target Administration Console that were available in previous versions of Identity Governance and Intelligence are moved to the Enterprise Connectors module as of Version 5.2.3.

In previous versions of Identity Governance and Intelligence, target types and targets were managed in two different places in the product: the Identity Brokerage target types (adapter profiles) and targets were managed in the Target Administration Console, and all other drivers and connectors were managed in the Enterprise Connectors module. With Identity Governance and Intelligence V5.2.3, all of the functions are contained in the Enterprise Connectors module.

Use the Enterprise Connectors module to integrate with target systems, including those that the Identity Brokerage supports.

*Table 4. Identity Brokerage target management terminology*

| Target Administration Console terms used in previous versions | Enterprise Connectors terms in V5.2.3 |
|---|---|
| Target type or adapter profile | Target profile or driver |
| Target | Connector |
| Reconciliation | Change log synchronization |

*Table 5. Where to find the new documentation*

| Target Administration Console documentation in previous versions | Enterprise Connectors documentation in V5.2.3 |
|---|---|
| Target type administration | Target profile administration |
| Target administration | Connectors administration |
| Reconciliation management | Change log synchronization overview |

## What is and what should be

IBM Security Identity Governance and Intelligence provides now features for the synchronization of the events that are associated to the permissions and rights that are assigned to a user.

When you try to assign a permission, you can detect a misalignment of the events that are associated to the permission.

For example, a permission is assigned to the user in Access Governance Core.

But the permission, for such reason, could not be propagated on the target system (for example, Active Directory).

From an alternative angle view, a permission is assigned to user in Active Directory (or another target system).

For such reason, the assignment is not propagated to Access Governance Core.

You receive a warning related to the permission not aligned (not synchronized) on both sides.

When you choose of synchronize (from target (Active Directory) to Access Governance Core), an event is generated for trying to align the situation in Access Governance Core.

In **Access Governance Core** > **Manage** > **Accounts** > **Out of Synchronization**, you can find all the permission or rights that are related to an account and associated to events that are not aligned between Access Governance Core and the target system.

This feature is related only to *automatic* target systems, thus the target systems that are linked to IBM Security Identity Governance and Intelligence through an adapter or a connector (see Introduction to Enterprise Connectors).

The same feature can be declined from the angle view of the user, considering the permission or rights of a specific user in **Access Governance Core** > **Manage** > **Users** > **Fulfillment**.

An extra function provides a list of all the permissions or rights of the user, thus also:

- The subset that is related to *automatic* target systems with events correctly aligned.
- The subset that is related to *manual* target systems.

The list can be obtained through **Access Governance Core** > **Manage** > **Users** > **Entitlement** > **Action** > **Fulfillmet**.

## Support password rule for customizing password management

IBM Security Identity Governance and Intelligence provides the option to specify a custom rule for providing a complete customization of password management.

The rule can provide custom constraints that are added to the other constraints that you can specify in Password Creation panel.

## New command changes the duration of the SSH session timeout

With the **`ssh_timeout`** command of the virtual appliance command line interface, you can now set the number of minutes that the SSH session of the virtual appliance can be idle before it closes. See Setting a timeout for the SSH session for details.

## Option for authenticating users from an external user registry to the Local Management Interface

The new option enables the virtual appliance administrator to use an external user registry to designate which users can authenticate to the local management interface (LMI) of the virtual appliance.

The administrator can specify users or groups of users that are defined in a directory server. The directory servers that are provided by IBM Security Directory Server or by Microsoft Active Directory are supported.

See Authenticating users from an external user registry to the Local Management Interface for more information.

## Usability improvements

The graphical user interface presents the following improvements in the Administration Console and in the Service Center:

- A confirmation window pops up when you leave a pane that you were editing without saving your data. To prevent the loss of your input, the window asks you to confirm that you want to leave without saving your changes. This occurs when you do any of the following actions before you save the new data:
  - Switch tabs, at the same level or at levels above
  - Change accordion panes
  - Change modules by the hamburger menu
  - Switch from one record to another in the same list
  - Select an action in the **Actions** menu while editing a record
  - Select the **Logout** button
  - Edit the page number field or click the navigator buttons to change page
  - Sort or refresh a table
  - Run a filtered search
  - Switch between flat and hierarchical views in the left hand side pane
- **Save** and **Cancel** are more visible and prominent throughout the user interface.
- Feedback on the Dashboard Loading Progress is enhanced.
- Icons throughout the user interface are improved and modernized.
- The behavior of the **Cancel** action in the wizards of the Administration Console modules is more consistent. The action rolls back all the unsaved changes in all the panes of a wizard.

## Additional language support

This version of Identity Governance and Intelligence is available also in the following languages:

- Arabic
- Czech
- Dutch
- Hebrew
- Hungarian
- Korean
- Polish

- Russian
- Spanish
- Turkish

For languages that have bidirectional characteristics, you can set up your own display preferences. See also the currently known limitations that affect the display of user interface items in these languages.

## Documentation updates

In addition to the documentation that supports the new product features, the following sections of the documentation are either new or significantly updated:

- Managing the Administration Realm
- Configuring enterprise connectors in a clustered environment
- Dashboard
- Available reports
- Query

# Chapter 3. Getting started

Before you deploy or use the product, you must complete the prerequisites and become familiar with product features to avoid issues.

The following table lists the main tasks to get started, including the corresponding reference topics or guides for each task.

*Table 6. How to get started*

| **Task** | **Reference** |
|---|---|
| Check what's new in this release. | Chapter 2, “What's new in Version 5.2.3,” on page 15 |
| Learn about the different components, personas, and user interfaces. | • Chapter 1, “Identity Governance and Intelligence overview,” on page 1<br>• Chapter 4, “Roadmap of personas and tasks,” on page 23<br>• Chapter 5, “User interface,” on page 37 |
| Check the hardware and software requirements. | For the detailed system requirements, see the IBM Security Identity Governance and Intelligence *Software Product Compatibility Report*, http://www-969.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.<br>1. Enter `Security Identity Governance and Intelligence`.<br>2. Select the product version.<br>3. Select the deployment unit.<br>4. Click **Submit**. |
| Deploy the product. | Deployment overview in the Installing Guide |
| Use the product functions. | Administering Guide |
| If you encounter an issue, check the existing limitations and issues. | • Chapter 7, “Known limitations, issues, and workarounds,” on page 45<br>• Troubleshooting and support Guide |

# Chapter 4. Roadmap of personas and tasks

*Persona* is a user archetype based on role and other characteristics that influence how a user interacts with the offering. A *Persona* has a related set of responsibilities. In Identity Governance and Intelligence, you can represent those responsibilities by implementing *Roles*, and assigning them to *Users*. Any Role can be associated with any set of tasks, dashboards, reports, campaigns, and other resources. This topic provides examples of tasks that a certain Role can perform.

The main personas are:

- Administrators
- Business users

**Administrators**

In Identity Governance and Intelligence, there are:

- "Virtual appliance administrators"
- "Identity Governance and Intelligence administrators" on page 26

**Business users**

Business users are defined in the *Regular Users schema* and can perform tasks in the Service Center.

Examples of Business users:

- Application Managers
- User Managers
- Role Managers
- Risk Managers
- Help Desks
- Employees

## Virtual appliance administrators

The Virtual appliance administrator is responsible for the setup and activation of the Identity Governance and Intelligence virtual appliance and for its day-to-day administration. See the following tables for the Virtual appliance administrators deployment and maintenance tasks.

*Table 7. Virtual appliance administrators deployment tasks*

| **Tasks** | **Subtasks and references** |
|---|---|
| Install and configure the database server. | For Oracle:<br>• Installing the Oracle server<br>• Configuring the Oracle server<br>For DB2®:<br>• Installing the DB2 server<br>• Configuring the DB2 server<br>Installation of database schemas in a high availability environment |

*Table 7. Virtual appliance administrators deployment tasks (continued)*

| Tasks | Subtasks and references |
|---|---|
| (Optional) Install and configure the directory server to use the Identity Brokerage Providers module. | Installing and configuring the directory server |
| Prepare the virtual machine. | Setting up the virtual machine |
| Install and set up the virtual appliance. | • Installing the IBM Security Identity Governance and Intelligence virtual appliance<br>• Setting up the initial virtual appliance |
| For high availability, set up a virtual appliance cluster. | Setting up a virtual appliance cluster<br>• Setting up a member node for IBM Security Governance and Intelligence by using the initial configuration wizard<br>• Promoting the secondary node to the primary node<br>• Promoting a member node to the secondary node<br>• Enabling and disabling replication between the primary and secondary nodes<br>• Promoting a member node to the primary node<br>• Removing a node from the cluster<br>• Reconnecting a node into the cluster<br>• Synchronizing a member node with a primary node |
| Configure the virtual appliance settings. | • Enabling Identity Brokerage Providers<br>• Managing directory server configuration<br>• Managing the database server configuration<br>• Managing OpenID connect configuration<br>• Managing the mail server configuration<br>• Managing application interfaces |

*Table 8. Virtual appliance administrators maintenance tasks*

| Tasks | Subtasks and references |
|---|---|
| Prepare for disaster recovery. Set up a secondary virtual appliance for an active-passive configuration. | 1. Setting up a primary virtual appliance<br>2. Backing up the virtual appliance<br>3. Reverting the virtual appliance to its backup<br>4. Creating a snapshot of the virtual appliance<br>5. Setting up a secondary virtual appliance |

*Table 8. Virtual appliance administrators maintenance tasks (continued)*

| Tasks | Subtasks and references |
|---|---|
| Monitor system event logs, memory, CPU, and storage usage, and configure the Simple Network Management Protocol. | • Viewing the event logs<br>• Viewing the memory usage<br>• Viewing the CPU usage<br>• Viewing the storage usage<br>• Viewing the cluster status<br>• Managing the SNMP monitoring |
| Configure the directory server, database server, OpenID connect providers, and mail server. | • Managing directory server configuration<br>• Managing the database server configuration<br>• Managing OpenID connect configuration<br>• Managing the mail server configuration |
| Configure and manage the Postgres replication, IBM Security Directory Integrator instances, and cluster nodes. | • Managing the Postgres database<br>• Managing Security Directory Integrator instances<br>• Managing LTPA-based single sign-on configuration |
| Manage custom files, and certificate stores. | • Managing custom files<br>• Managing certificates |
| Manage the virtual appliance updates and licensing. | • Viewing the update history<br>• Viewing the licensing<br>• Managing the firmware settings<br>• Installing a fix pack |
| Manage the virtual appliance and Identity Governance and Intelligence logs retrieval and configuration, core dumps, Identity Brokerage Providers configuration, and build information. | • Managing the log configuration<br>• Managing the core dump files<br>• Enabling Identity Brokerage Providers<br>• Viewing the About page information |
| Manage network settings such as application interfaces, hosts files, static and system routes, and the network file system. | • Managing application interfaces<br>• Managing hosts file<br>• Configuring static routes<br>• Managing a network file system (NFS) |
| Manage the Export and Import settings | Exporting or importing the configuration settings |
| Manage the virtual appliance administrator settings, and system settings such as tuning parameters, snapshots, support files, system audit events, BiDi properties, and management authentication. | • Configuring the date and time settings<br>• Configuring the administrator settings<br>• Managing advanced tuning parameters<br>• Configuring BiDi properties<br>• Managing the snapshots<br>• Managing the support files<br>• Configuring system audit events<br>• Configuring LMI authentication for external user registry<br>• Restarting or shutting down the appliance |

Table 8. Virtual appliance administrators maintenance tasks (continued)

| Tasks | Subtasks and references |
|---|---|
| Manage the virtual appliance by using the command line interface. | • Managing the core dump files<br>• Tailing logs and archiving logs<br>• Adding a JVM property<br>• Managing the SSL certificate<br>• Getting and setting the SIB schema names<br>• Getting and setting the reconciliation failure threshold |

Back to top

## Identity Governance and Intelligence administrators

An Identity Governance and Intelligence administrator, also called *Super Administrator* is predefined. This *Super Administrator* is responsible for defining other Identity Governance and Intelligence administrator profiles in the Administration Console by using a free configuration of *N* base permissions.

The *Super Administrator* can define an Identity Governance and Intelligence administrator as:

- An administrator of a single module or of all the Identity Governance and Intelligence modules.
- An administrator who is authorized to perform a selected set of tasks on module *A*, *B*, and others.

See *Super Administrator* for examples of tasks that a *Super Administrator* can perform.

See the following references for examples of tasks that an Identity Governance and Intelligence administrator can perform, when granted access to any of these modules.

- “Access Risk Controls module” on page 28
- “Process Designer module” on page 29
- “Access Optimizer module” on page 29
- “Report Designer module” on page 29
- “Task Planner module” on page 30

Examples of Identity Governance and Intelligence administrators that can be defined and used in the system:

- “Application Managers” on page 30
- “User Managers” on page 31
- “Role Managers” on page 32
- “Risk Managers” on page 33

Back to top

## Super Administrator

A *Super Administrator* can perform the following tasks in the Administration Console:

*Table 9. Super Administrator tasks*

| Tasks | Subtasks and references |
|---|---|
| For target integration, configure the target system. | • Import the target type, also known as the adapter profile. See Importing target types (adapter profiles).<br>• Create an instance of the target from the target type.<br>Specify the target identity and other information to connect to the server where the target resides. See Creating targets. |
| Configure the initial entities. | • Create realms. See Concept of Realm and Managing the Administration Realm.<br>• Create resources. See Resources.<br>• Create entitlements. See Hierarchy of entitlements.<br>• Create applications. See Applications.<br>• Create accounts. See Accounts. |
| Configure organizational units. | • Create organization units. See Organization units.<br>• Assign the organization unit to an entitlement. See Org Units.<br>• Assign resources to an organization unit. See Group Resources. |
| Configure groups. | • Create groups. See Groups.<br>• Assign entitlements to the group. See Entitlements.<br>• Assign resources to the group. See Group Resources. |
| Configure roles. | • Create and publish roles. See Roles.<br>• Define the entitlements. See Management. |
| On-board administrators. | 1. Create the Administrator role. See Admin Roles.<br>2. Assign organization units to the Administrator role. See Org Units.<br>3. Assign users to the Administrator role. See Users. |
| On-board users. For example, a new employee *UserA*, joined the organization. | 1. Create the user profile. See Users.<br>2. Assign user to a role. See Users.<br>3. Assign an entitlement to the user. See Entitlements.<br>4. Assign resources to the user. See User Resources.<br>5. Create and manage the accounts for the registered user. See Accounts.<br>6. Assign rights. See Rights.<br>7. Set a mitigation action if the user is assigned with a risk level. See Mitigations. |

*Table 9. Super Administrator tasks (continued)*

| **Tasks** | **Subtasks and references** |
|---|---|
| Add entitlements to the on-boarded user, such as an external role. For example, assign *UserA* with the external role *Senior Developer* on the *Data Manager* application. | 1. View the permissions that are defined for the application.<br>• Search for the external role you want to assign.<br>• Check whether the external role configuration is set for user assignment on the target system.<br>See Application Access.<br>2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements.<br>3. Check whether the assignment event *Add Permission* is generated for the external role. See Events. |
| Enable a custom Segregation of Duties policy. | 1. Enable the external Segregation of Duties feature.<br>2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface.<br>See General |
| Define a certification campaign. | Certification Campaigns |
| Change account passwords for users. | Changing user passwords |
| Force users to change their Service Center password on their next login. | Forcing a password change |
| Configure the password service. | Configuring the password service in Access Governance Core |
| Configure the Access Requests workflows for change password, forgot password, or password reset functionalities. | Configuring the password service in Process Designer |
| Configure and assign dashboards. | Dashboards for Service Center |

Back to top

## Access Risk Controls module

Administrators, who are granted access to the Access Risk Controls module, can perform the following tasks:

*Table 10. Sample tasks in the Access Risk Controls module*

| **Tasks** | **Subtasks and references** |
|---|---|
| Model a business activity tree structure. | Business activities |
| Associate the permissions to one or more activities. | Business activity mapping |
| Set mitigation controls. | Mitigation controls |
| Define risks. | Risk definition |
| Define domains. | Domains |
| Evaluate risk violations. | Risk violations |

*Table 10. Sample tasks in the Access Risk Controls module (continued)*

| **Tasks** | **Subtasks and references** |
|---|---|
| Compare configurations. | Configuration comparison |
| Request or download report. | Report |

Back to top

## Process Designer module

Administrators, who are granted access to the Process Designer module, can perform the following tasks:

*Table 11. Sample tasks in the Process Designer module*

| **Tasks** | **Subtasks and references** |
|---|---|
| Define activities that can be associated to a process. | Activity |
| Design a process. | Process |
| Assign one or more administrative roles to each activity defined in the process. | Assign |
| Configure the Access Requests workflows for change password, forgot password, or password reset functionalities. | Password administration |

Back to top

## Access Optimizer module

Administrators, who are granted access to the Access Optimizer module, can perform the following tasks:

*Table 12. Sample tasks in the Access Optimizer module*

| **Tasks** | **Subtasks and references** |
|---|---|
| Configure and compare data snapshots. | Data snapshot |
| Define access data sets. | Access data sets |
| Configure relevance criteria. | Relevance criteria |
| Create and manage a data exploration analysis. | Data Exploration analysis and details |
| Create a role mining request. | Role mining |

Back to top

## Report Designer module

Administrators, who are granted access to the Report Designer module, can perform the following tasks:

*Table 13. Sample tasks in the Report Designer module*

| **Tasks** | **Subtasks and references** |
|---|---|
| Create and customize report queries. | Query |

*Table 13. Sample tasks in the Report Designer module (continued)*

| Tasks | Subtasks and references |
|---|---|
| Create and customize reports. | Report |
| Create and customize dashboard items. | Dashboard |
| Assign the product report to a user or an entitlement. | Report assignment |
| Organize the product reports. | Menu |

Back to top

## Task Planner module

Administrators, who are granted access to the Task Planner module, can perform the following tasks:

*Table 14. Sample tasks in the Task Planner module*

| Tasks | Subtasks and references |
|---|---|
| Add jobs and configure job class attributes. | Jobs |
| Create and configure tasks, define job class parameters, and configure scheduling. | Tasks |
| Synchronize tasks to the selected scheduler. | Scheduler |
| Group tasks by context. | Context |

Back to top

## Application Managers

Application Managers, with administrative rights, can perform any of the following tasks in the Administration Console.

*Table 15. Application Managers tasks in the Administration Console*

| Tasks | Subtasks and references |
|---|---|
| For target integration, configure the target system. | • Import the target type, also known as the adapter profile. See Importing target types (adapter profiles).<br>• Create an instance of the target from the target type.<br>Specify the target identity and other information to connect to the server where the target resides. See Creating targets. |

*Table 15. Application Managers tasks in the Administration Console (continued)*

| Tasks | Subtasks and references |
|---|---|
| On-board users. For example, a new employee *UserA*, joined the organization. | 1. Create the user profile. See Users.<br>2. Assign user to a role. See Users.<br>3. Assign an entitlement to the user. See Entitlements.<br>4. Assign resources to the user. See User Resources.<br>5. Create and manage the accounts for the registered user. See Accounts.<br>6. Assign rights. See Rights.<br>7. Set a mitigation action if the user is assigned with a risk level. See Mitigations. |
| Add entitlements to the on-boarded user, such as an external role. For example, assign *UserA* with the external role *Senior Developer* on the *Data Manager* application. | 1. View the permissions that are defined for the application.<br>• Search for the external role you want to assign.<br>• Check whether the external role configuration is set for user assignment on the target system.<br>See Application Access.<br>2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements.<br>3. Check whether the assignment event *Add Permission* is generated for the external role. See Events. |
| Enable a custom Segregation of Duties policy. | 1. Enable the external Segregation of Duties feature.<br>2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface.<br>See General |

Back to top

## User Managers

User Managers, with administrative rights, can perform any of the following tasks in the Administration Console.

Table 16. User Managers tasks in the Administration Console

| Tasks | Subtasks and references |
|---|---|
| On-board users. For example, a new employee *UserA*, joined the organization. | 1. Create the user profile. See Users.<br>2. Assign user to a role. See Users.<br>3. Assign an entitlement to the user. See Entitlements.<br>4. Assign resources to the user. See User Resources.<br>5. Create and manage the accounts for the registered user. See Accounts.<br>6. Assign rights. See Rights.<br>7. Set a mitigation action if the user is assigned with a risk level. See Mitigations. |
| Add entitlements to the on-boarded user, such as an external role. For example, assign *UserA* with the external role *Senior Developer* on the *Data Manager* application. | 1. View the permissions that are defined for the application.<br>• Search for the external role you want to assign.<br>• Check whether the external role configuration is set for user assignment on the target system.<br>See Application Access.<br>2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements.<br>3. Check whether the assignment event *Add Permission* is generated for the external role. See Events. |
| Enable a custom Segregation of Duties policy. | 1. Enable the external Segregation of Duties feature.<br>2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface.<br>See General |

Back to top

## Role Managers

Role Managers, with administrative rights, can perform any of the following tasks in the Administration Console, including tasks in the Process Designer module.

Table 17. Role Managers tasks in the Administration Console

| Tasks | Subtasks and references |
|---|---|
| Configure roles. | • Create and publish roles. See Roles.<br>• Define the entitlements. See Management. |

*Table 17. Role Managers tasks in the Administration Console (continued)*

| Tasks | Subtasks and references |
|---|---|
| On-board users. For example, a new employee *UserA*, joined the organization. | 1. Create the user profile. See Users.<br>2. Assign user to a role. See Users.<br>3. Assign an entitlement to the user. See Entitlements.<br>4. Assign resources to the user. See User Resources.<br>5. Create and manage the accounts for the registered user. See Accounts.<br>6. Assign rights. See Rights.<br>7. Set a mitigation action if the user is assigned with a risk level. See Mitigations. |

Back to top

## Risk Managers

Risk Managers, with administrative rights, can perform any of the following tasks in the Administration Console, including tasks in the Access Risk Controls module.

*Table 18. Risk Managers tasks in the Administration Console*

| Tasks | Subtasks and references |
|---|---|
| Add entitlements to the on-boarded user, such as an external role. For example, assign *UserA* with the external role *Senior Developer* on the *Data Manager* application. | 1. View the permissions that are defined for the application.<br>• Search for the external role you want to assign.<br>• Check whether the external role configuration is set for user assignment on the target system.<br>See Application Access.<br>2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements.<br>3. Check whether the assignment event *Add Permission* is generated for the external role. See Events. |
| Enable a custom Segregation of Duties policy. | 1. Enable the external Segregation of Duties feature.<br>2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface.<br>See General |

Back to top

## Business users: Managers

The following list provides examples of tasks Managers can perform in the Service Center, depending on their configuration.

*Table 19. Manager tasks in the Service Center*

| **Tasks** | **Subtasks and references** |
|---|---|
| Approve or revoke campaign requests. | Campaign Management |
| Manage orphan accounts. | User-account matching |
| Manage access requests. | • Account change requests<br>– Selecting the user<br>– Answering security questions<br>– Selecting the accounts<br>– Entering the new password<br>– Authorizing the request<br>– Executing the request<br>• Delegating requests<br>– Generating a request<br>– Processing a request<br>• Creating entitlements<br>– Generating a request<br>– Processing a request<br>– Executing a request<br>• Modifying entitlements<br>– Generating a request<br>– Processing a request<br>– Executing a request<br>• Request user access<br>– Generating a request<br>– Processing a request<br>– Executing a request<br>• Creating users<br>– Generating a request<br>– Processing a request<br>– Executing a request |
| Reset the account password for other users. | Resetting account passwords for other users |
| Reset own Service Center password. | Resetting my forgotten password |
| Map permissions and activities. | • Dashboard<br>• Permission Perspective<br>• Activity Perspective |
| Configure, run, and download the report. | • Request<br>• Download |

**Note:** User Managers and Application Managers have customized Service Center dashboards from which they can view and manage their activities. For more information, see:

- User Manager dashboard
- Application Manager dashboard

Back to top

## Business users: Help Desks

The following list provides examples of tasks that Help Desks can perform in the Service Center, depending on their configuration.

*Table 20. Help Desks tasks in the Service Center*

| **Tasks** | **Subtasks and references** |
|---|---|
| Reset the account password for other users.. | Resetting account passwords for other users |

Back to top

## Business users: Employees

The following list provides examples of tasks that Employees can perform in the Service Center, depending on their configuration.

*Table 21. Employees tasks in the Service Center*

| **Tasks** | **Subtasks and references** |
|---|---|
| Reset own Service Center password.. | Resetting my forgotten password |
| Change the account password for active accounts. | Changing my account password |
| View **Self Care** requests status | Viewing my requests in the Self Care application |
| Update the *security questions* for account recovery | Updating my security questions |

**Note:** Employees have customized Service Center dashboards from which they can view and manage their activities. For more information, see Employee dashboard.

Back to top

# Chapter 5. User interface

The Identity Governance and Intelligence solution has a web console for virtual appliance management and web consoles for identity governance and administration.

*Table 22. Identity Governance and Intelligence consoles*

| Consoles | URL | Description |
|---|---|---|
| Virtual Appliance Dashboard | `https://hostname:port` | Virtual appliance administrators can perform the following tasks:<br>• Access the Administration Console and Service Center.<br>• Quickly view the disk usage, partition information, available interfaces, notifications, middleware status, cluster status; and control the server status.<br>• Monitor system event logs, memory, CPU, and storage usage, and configure the Simple Network Management Protocol.<br>• Configure the directory server, database server, OpenID connect providers, and mail server.<br>• Configure and manage the Postgres replication, IBM Security Directory Integrator instances, and cluster nodes.<br>• Manage custom files, and certificate stores.<br>• Manage the virtual appliance updates and licensing.<br>• Manage the virtual appliance and Identity Governance and Intelligence logs retrieval and configuration, core dumps, Identity Brokerage Providers configuration, and build information.<br>• Manage network settings such as application interfaces, hosts files, static and system routes, and the network file system.<br>• Manage the Export and Import settings<br>• Manage the virtual appliance administrator settings, and system settings such as tuning parameters, snapshots, support files, system audit events, BiDi properties, and management authentication. |

*Table 22. Identity Governance and Intelligence consoles (continued)*

| **Consoles** | **URL** | **Description** |
|---|---|---|
| Administration Console | `http://hostname:port/ideas/wasLogin.jsp` | It includes modules intended for Identity Governance and Intelligence administrators.<br>See "Administration Console modules" for more information about the functions and activities that can be performed in each of these modules. |
| Service Center | `http://hostname:port/ideas/login.jsp?realm=IDEAS` | It includes applications intended for Business users who are not administrators, such as Managers and Employees.<br>See "Service Center applications" on page 41 for more information about the functions and activities that can be performed in each of these applications. |

## Administration Console modules

The Administration Console consists of the following Identity Governance and Intelligence modules.

*Table 23. Administration Console modules*

| **Administration Console modules** | **Description** |
|---|---|
| Access Governance Core | It is the central module, and base engine for all other modules. It is dedicated to the implementation of the authorization processes.<br>Access Governance Core manages entities such as Users, Organization Units, Hierarchies, Entitlements, and Applications.<br>It provides a modeler for outlining the organization's current situation.<br>Identity Governance and Intelligence administrators can:also use this module to configure password services.<br>See Introduction to Access Governance Core. |
| Access Optimizer | It is a tool that is integrated with role management and is intended for role mining and risks analysis.<br>It gets data from the Access Governance Core. It helps optimize roles and provide an analysis of user-privilege relations to identify critical situations, or potential side effects of analysis changes.<br>Access Optimizer includes a visual map of entitlements-users assignments and the level of risks in these assignments. This visual approach makes it easier to manage role mining and risk scoring.<br>See Introduction to Access Optimizer. |

*Table 23. Administration Console modules (continued)*

| **Administration Console modules** | **Description** |
|---|---|
| Access Risk Controls | It helps manage business activities, business activity mappings, and related risks. It helps determine users and roles that have Segregation of Duties violations.<br>Access Risk Controls enforces Segregation of Duties checks by relating the business activities model and application permissions.<br>It uses 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.<br>See Introduction to Access Risk Controls. |
| Access Risk Controls for SAP | It extends the capabilities of Access Risk Controls to the authorization framework of SAP systems.<br>It is designed to work specifically with SAP roles. It downloads SAP role definitions directly from SAP targets, analyzes them, and determines the ones that have Segregation of Duties risks.<br>An SAP administrator can use the acquired information to take action on the SAP system. Identity Governance and Intelligence can also use the information to run an in-depth analysis on user violations.<br>See Introduction to Access Risk Controls for SAP. |
| Process Designer | It is a tool used for designing and defining authorization processes based on custom business rules. It produces the Access Requests authorization workflows.<br>Process Designer provides a modeler for outlining the access request and approval process and for integrating other external target systems.<br>It works with the Access Governance Core module to manage:<br>• Requests to access the system application.<br>• Allocation and revocation of authorization profiles.<br>• Password lifecycle.<br>• Notifications that are sent to users during different phases of the authorization process.<br>• Temporary delegations of personal roles that are associated with users of the system.<br>• Definition of the visibility range that is associated with an administrative figure.<br>See Introduction to Process Designer. |

*Table 23. Administration Console modules (continued)*

| **Administration Console modules** | **Description** |
|---|---|
| Target Administration | It is a tool that is used by administrators to perform target administration, including:<br>• Import target profile.<br>• Import account attributes mapping.<br>• Configure account defaults for target profile.<br>• Search, add, modify, and delete targets.<br>• Manage reconciliation.<br>• Set up account defaults for a target.<br>See Target administration and Target type administration |
| Enterprise Connectors | Identity Governance and Intelligence use Enterprise Connectors as an alternative for integrating with target systems that the Identity Brokerage cannot support.<br>It provides a set of connectors to consolidate and synchronize user entitlements with the most common enterprise applications. These connectors can include SAP and Oracle applications, Active Directory, LDAP, and many others.<br>It keeps the Access Governance Core repository synchronized with the target systems if there are changes on the repository or on the target systems. |
| Report Designer | It manages reports and dashboard items.<br>Identity Governance and Intelligence provides several ready-to-use reports for every activity it manages, and a set of configured dashboard items to be used on Dashboard home pages in the Service Center.<br>Administrators can use Report Designer to:<br>• Create and customize report queries.<br>• Create and customize reports.<br>• Create and customize dashboard items<br>• Configure and assign dashboards.<br>• Assign the product report to a user or an entitlement.<br>• Organize the product reports.<br>See Introduction to Report Designer. |
| Task Planner | It manages scheduled tasks and custom jobs.<br>Identity Governance and Intelligence runs many internal jobs to support its own processes. Administrators can use Task Planner to:<br>• Define different execution schedules.<br>• Stop processes that are not required.<br>• Implement and schedule custom jobs to better support specific scenarios.<br>See Introduction to Task Planner. |

Back to top

## Service Center applications

Service Center consists of the following applications, which are designed to simplify actions and to guide users in their tasks.

*Table 24. Service Center applications*

| **Service Center applications** | **Description** |
|---|---|
| Access Certifier | It manages the reviews and certification of user access entitlements to prevent users from acquiring access that is not necessary for their jobs.<br>Managers can confirm or revoke user roles, roles assigned to the groups of a hierarchy (for example, organizational units), and user accounts.<br>Access reviews and certifications can be scheduled, triggered automatically, or started manually.<br>See Introduction to Access Certifier. |
| User-account matching | It manages orphan accounts from targets that are currently not matched with the organization's policies.<br>Identity Brokerage usually manages the unmatched accounts using rules defined on customer business policies. When these rules are unable to match the accounts, an entitled Manager can use this module to match them manually.<br>See Introduction to User-account matching. |
| Access Requests | It runs the Access Requests workflows configured in the Process Designer module.<br>The main tasks available are:<br>• Generate requests to change user roles.<br>• Lock and unlock user accounts.<br>• Request new roles.<br>• Change and reset user passwords.<br>Depending on the entitlements assigned to a user, this module shows the user which requests the user can operate. Typically, this module is used by managers.<br>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.<br>See Introduction to Access Requests. |
| Business Activity Mapping | It creates the correlation between Business Activities and Permissions, needed to perform a Segregation of Duties analysis.<br>This module provides a simplified Access Risk Controls functionality that can be made available to users.<br>See Introduction to Business Activity Mapping. |

*Table 24. Service Center applications (continued)*

| **Service Center applications** | **Description** |
|---|---|
| Report Client | It is a tool to configure and run reports that are designed through the Report Designer module. It provides a modeler that can outline every type of report.<br>See Introduction to Report Client. |
| **Self Care** | It enables Users to:<br>• Change the Service Center password.<br>• Change the account password for active accounts.<br>• View **Self Care** requests status.<br>• Update the *security questions* for account recovery. |
| Persona-based dashboard | It helps Users with tasks prioritization through customized views. When a User logs in to Service Center, the home page shows all dashboard items for all Administrator Roles assigned to the User.<br>The Administrator Roles are:<br>• Application Manager<br>• User Manager<br>• Employee |

Back to top

## Notes on using the user interface

Be aware of the following facts when you use either the Administration Console or the Service Center modules:

**Wildcard characters for the Search tool**

You can use either the asterisk (*) or the percent sign (%) when you search for specific items. You can also type the starting characters of the item you are searching to narrow your search results.

**Direct page changes in multi-pages lists**

When a list of items fills more than one page, you can move your mouse to the box that is located at the bottom of page 1, type your desired page number, and press the Enter key to traverse directly to one of the following pages.

Back to top

# Chapter 6. Language support

The IBM Security Identity Governance and Intelligence virtual appliance and user interfaces, including reports, are available in several languages.

The following are the supported languages:

*Table 25. Supported languages*

| Locale code | Language |
|---|---|
| ar | Arabic |
| cs | Czech |
| de | German |
| en | English (United States) |
| es | Spanish |
| fr | French |
| he | Hebrew |
| hu | Hungarian |
| it | Italian |
| ja | Japanese |
| ko | Korean |
| nl | Dutch |
| pl | Polish |
| pt, pt_BR | Brazilian Portuguese |
| ru | Russian |
| tr | Turkish |
| zh, zh_CN | Simplified Chinese |
| zh_TW | Traditional Chinese |

# Chapter 7. Known limitations, issues, and workarounds

You can view the known software limitations, issues, and workarounds on the Identity Governance Support site. Also, consider the known limitations described here.

The Support site describes not only the limitations and issues that exist when the product is released, but also any additional items that are found after product release. As limitations and issues are discovered and resolved, the IBM Software Support team updates the online knowledge base. By searching the knowledge base, you can find workarounds or solutions to issues that you experience.

To create your own query, go to the IBM Software Support website: https://www-947.ibm.com/support/entry/portal/support.

## Select All check box remains selected after the user clears selections in the table

The **Select All** check boxes that are present in all of the tables in the Service Center and Administration Console remain selected even after the user clears selections.

Proceed by continuing to clear selections as needed after you select the **Select All** check box, and ignore this issue. After you clear the selections that you do not need, those items are cleared even though the **Select All** check box remains selected.

## Turkish uppercase "I" is not correctly read from DB2 repository

During a search in a generic UI panel, for recovering textual data where the Turkey uppercase "I" could be present, the search fails in DB2 repository (but functions in Oracle DB).

## Non-English characters are missing in generated PDF reports

The generated report that contains non-English characters fails when you choose to export it in PDF format.

## Cannot rename the group name on the target endpoint

The group name cannot be renamed on the target endpoint.

# Chapter 8. Cookbooks

Cookbooks are scenario-based, step-by-step guides that provide how-to information and tasks so that you can successfully deploy the specified scenario.

IBM developers create Cookbooks, which are supplementary resources. They are located and updated in IBM developerWorks. Documents in IBM developerWorks might not be translated or supported by IBM Support.

Use the following Cookbooks with information in the IBM Knowledge Center:

- Cookbook for IBM Security Identity Governance and Intelligence integration with IBM Security Identity Manager

# Index

Printed in USA