IBM Security Identity Governance and Intelligence
Version 5.2.2

Product Overview Topics

IBM Security Identity Governance and Intelligence
Version 5.2.2

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.

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

- *Features overview*, https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.2/com.ibm.igi.doc/product_overview/cpt/cpt_feat_overview.html
- *What's new*, https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.2/com.ibm.igi.doc/product_overview/cpt/cpt_whats_new.html

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.

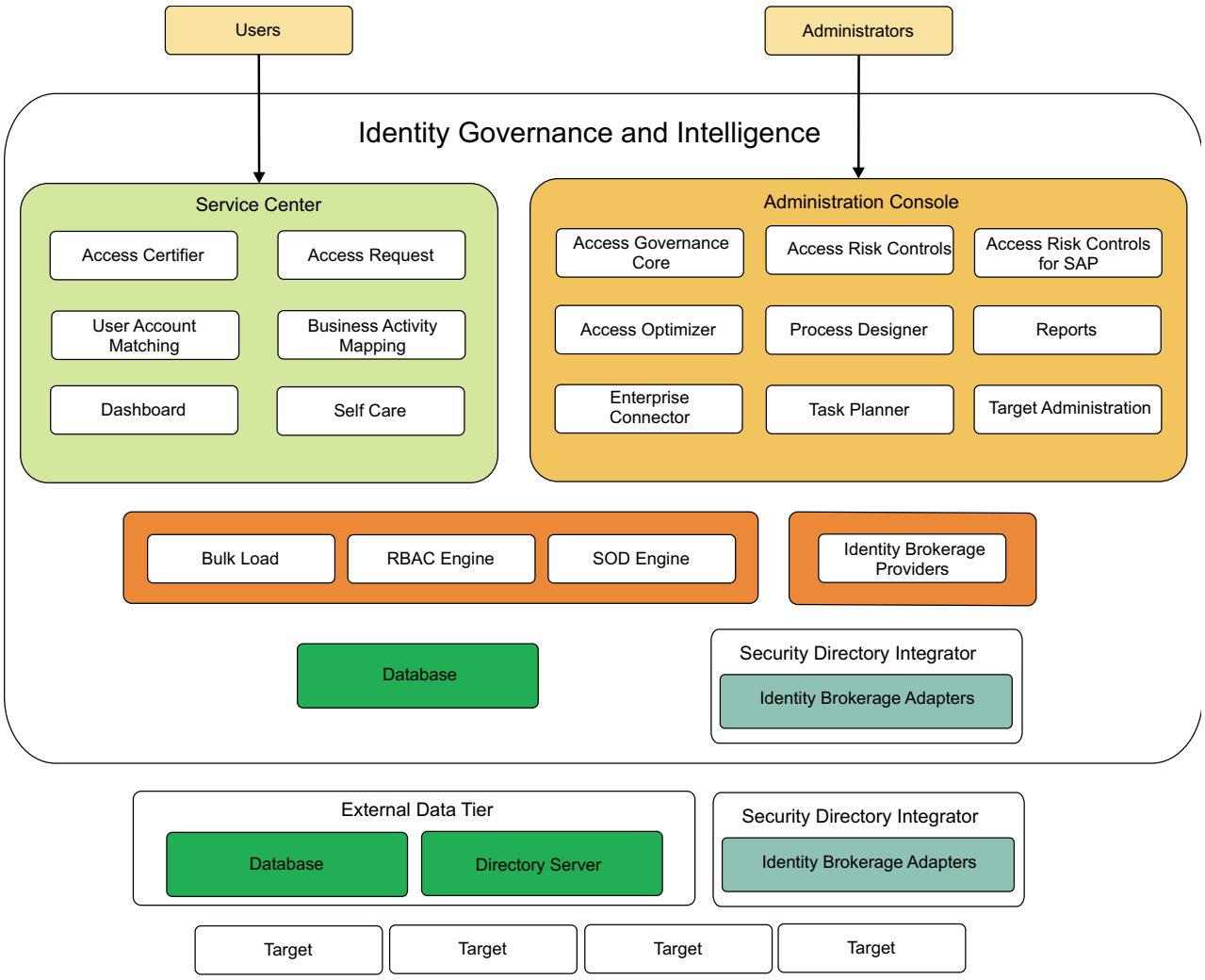

Figure 1. Identity Governance and Intelligence architecture

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 39 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. Changes that are initiated from Identity Governance and Intelligence or from external target systems are recorded and processed in an asynchronous manner through queues. 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 This data model contains elements that define the organizational structure.	• Organization units • Users • Entitlements • Resources • Rights • Applications • Accounts
Extended data model This data model contains elements that support the risk definition and detection layer of Identity Governance and Intelligence.	• Business activities model and application permissions • Risk definition and detection • Segregation of Duties • External SoD • Risk mitigation • Mitigation actions • Domains • 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, and system audit events.

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 management

Target 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 Target Administration Console to perform target administration, including:

- Import target profile.
- Import account attributes mapping.
- Configure account defaults for target profile.
- Search, add, modify, and delete targets.
- Manage reconciliation.
- Set up account defaults for a target.

See the following topics:

- Target type administration
- Target administration

Use Enterprise Connectors to integrate with target systems that the Identity Brokerage does not support. Enterprise Connectors cover connector or target types that are not available in the Identity Brokerage Adapters such as HR systems and CSV files.

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** > **Target Administration Console**	**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. The Identity Brokerage Adapters framework provides out-of-the-box functionality for all adapters that are deployed within the Identity Brokerage. 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 5.2.2

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

Simplified virtual appliance deployment

The IBM Security Identity Governance and Intelligence virtual appliance can be installed on a:

- XenServer hypervisor. See XenServer support
- Kernel-based virtual machine (KVM). See KVM support.

The Virtual appliance administrator can:

- Set up an in-house database, Postgres, which reduces dependency on external databases.
- Install and configure multiple IBM Security Directory Integrator instances within the virtual appliance.
- Install and update adapters on the built-in IBM Security Directory Integrator in the virtual appliance.
- Manage the failover in the in-house Postgres database, the built-in IBM Security Directory Integrator, and IBM DB2
- Scale the virtual appliance with external components, when necessary. The administrator can increase the virtual appliance storage any time after deployment and configure the external data storage (SAN / NFS) to meet data growth over a time.
- Configure the database connection pool settings and automatic client reroute settings.
- Manage cluster environments with primary, secondary, and member nodes.

  The first member node that is created automatically becomes the secondary node. Only a secondary node can be promoted to primary. A member node can be promoted to a secondary node only. You can no longer promote a member node directly to a primary node.

  If the internal Postgres database is used for the cluster, replication can be enabled between the databases of the primary and secondary nodes only.
- Upload CSV identity information directly to the virtual appliance.

  The virtual appliance includes a **File Upload** feature, and an option to map an external NFS drive on the virtual appliance, where the identity feed files are located.
- Manage the LMI security protocol and cipher suite settings.
- Increase CPU and memory capacity to increase appliance throughput.

Improved integration with IBM Security Identity Manager for re-certification

An IBM Security Identity Manager administrator can set up, manage, and run re-certification campaigns on IBM Security Identity Manager users and entitlements in IBM Security Identity Governance and Intelligence to re-certify the IBM Security Identity Manager roles. Results of the re-certification campaigns are reconciled in IBM Security Identity Manager.

Attribute mapping service

Some target systems have authorization information that is stored as user attributes. With the attribute mapping service, these attributes can be translated into permissions or rights. These translated attributes are included in Segregation of Duties checks in the Access Certifier and Access Requests modules.

For more information, see the following topics:

- Permissions based on user attributes
- Attribute-to-permission mapping service

The Identity Governance administrator can manually define the permission mapping rules in the Access Governance Core. For more information, see Adding an attribute-to-permission mapping manually.

The administrator can:

- Set attribute permission and rights values as required.
- Add an attribute permission into a business role or IT role.
- Use the **Bulk Load** tool to insert rights definitions and values. For more information, see Importing an attribute-to-permission mapping with a bulk load operation.
- View and modify the attribute mapping. For more information, see Editing an attribute-to-permission mapping.

An Application Manager can:

- Download an attribute permission configuration template. For more information, see Importing an attribute-to-permission mapping with a bulk load operation.
- Enable the attribute permission mapping of the target. For more information, see Enabling an attribute-to-permission mapping.
- Discover and import the attribute permission configurations. For more information, see Discovering attributes from a target system.
- Add, modify, or delete the attribute mapping for an attribute that is imported from a target. For more information, see the following topics:
  - Adding an attribute-to-permission mapping manually
  - Editing an attribute-to-permission mapping
  - Removing an attribute-to-permission mapping

The following help files describe the user interface for the attribute mapping service in the Access Governance Core:

- Bulk Load Tool page: Insert Attribute-to-Permission Mapping Track
- Attribute-to-Permission Mapping page: Attribute-to-Permission Mapping

Bulk load extension to import role-permission relation

The Identity Governance administrator can import the *Role-Permission* relation from a target system into the Administration Console. The administrator can use the **Bulk Load** function any time there are changes, and the structure is available in a bulk load file format. For more information, see Importing an attribute-to-permission mapping with a bulk load operation

Standardized authentication across applications and services

IBM Security Identity Governance and Intelligence users can single sign-on to the IBM Security Identity Manager Administration Console and Service Center, and OpenID Connect enabled web applications. Re-authentication is not required.

Improved Identity Intelligence - Business Activity Model

Business activities represent what can be done in an organization using a business "language". Business activity mappings define how the activities are done using the Application Permissions "language". The business activity model is designed specifically for Segregation of Duties Management..

Business activities are included in the Access Governance Core main entities - Users, Hierarchies, Entitlements, and Applications.

Business users can filter and view entities by business activities to help with task prioritization and decision making during access requests and certification. Business users can better understand their teams' access from a business perspective. They can review and align team roles and user entitlements to current business needs.

The Identity Governance administrator can:

- Filter campaign entities by business activities during a Campaign data set creation to make Business Activity based Campaigns.
- View business activities by users, by groups, or by entitlements.

  The following reports are available out-of-the-box in the Report Designer module.
  - Activities by user
  - Activities by group
  - Activities by entitlement
- Start a "Hierarchy Analysis" to determine the users that can have Risks and view the results in the Risk Info form.
- Visualize all the activities that are done by the Users of a Hierarchy to find whether there are outliers.
- Start Certification Campaigns on Users that do outlier activities.

In addition to persona-based dashboards, the Service Center includes a dashboard view of the:

- Business activities of selected users
- Business activities associated with authorization requests or pending execution

See Available reports and Dashboards with a business activity scope for more information.

Security integration

Integration with IBM Security Privileged Identity Manager: Recertification of privileged user's access entitlement

Use Privileged Identity Manager to manage shared access to privileged credentials and use Identity Governance and Intelligence to certify privileged users' access entitlements.

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 adapter can manage and reconcile privileged user accounts, roles, system groups, and admin domain information from the target system.

The administrator must create a target profile to connect Identity Governance and Intelligence and Privileged Identity Manager, define the attribute mapping rules, set up target reconciliation and certification campaigns, and verify that the entitlements are displayed properly in Identity Governance and Intelligence.

Business users such as an Application Manager and User Manager can then use Access Certifier to review and certify the Privileged Identity Manager entitlements.

Identity Brokerage REST APIs

REST APIs are available to enable customer to access and manage identity targets directly by developing client applications that can be invoked from anywhere within the network.

Technical foundation

Workflow notifications

The Identity Governance administrator can add, modify, or remove an email or SMS notification job for each activity in an Access Requests workflow in the Process Designer, including a reminder notification. The email or SMS is sent after the activity is completed.

Email notification templates are available out-of-the-box. There is an option to define the frequency, start date and time, and recipients for the reminder notification.

Use the **EmailService** task in Task Planner to view the job setup.

See Email and SMS notification administration to learn about adding an email or SMS notification job for an activity and for more information about the **EmailService** task.

Management of expired requests

In Access Requests, authorized managers and users can view a summary of requests that passed their expiration time and that await for approval or rejection. In Process Designer, the Identity Governance administrator configures the process flow for this service, by adding an expiration time in terms of priority, and an escalation action.

Redirection of authorization requests to other approvers

At times, the user with the role that is assigned to authorize a request might not be able to manage the request. 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 managers with the capability of redirecting an authorization request to another entitled person, the Identity Governance administrator can complete these tasks in the Administration Console.

1. Assign the *Redirection Approver* administrative role to selected users in the Access Governance Core.

2. Select classes of users in the **Redirect Scope** tab in the Activity pane of the authoritative step of a WorkFlow process in the Process Designer.

Permission rights reconciliation and management

The Identity Governance administrator can run reconciliation to synchronize the imported user attributes and view the applications' permissions, user assignments to permissions, and associated rights for managed targets.

The Business user can use the Service Center to request access to applications, which are managed by Identity Brokerage Adapters, that support rights on entitlements.

For more information, see Reconciliation management.

Bulk user onboarding from HR systems

An enterprise can have multiple HR systems for Employees in different locations. Changes in the HR system can be synchronized into Identity Governance and Intelligence periodically. Lifecycle rules are defined in Identity Governance and Intelligence to handle user change events and trigger access provisioning and de-provisioning for Employees based on governance policies that are defined in Identity Governance and Intelligence.

The Identity Governance administrator can install and configure HR-specific adapters. The administrator can use the adapters to reconcile and load users and organization units in the PeopleSoft and SAP HR systems into the Identity Governance and Intelligence Administration Console. The following HR adapters are supported:

PeopleSoft HR Feed adapter
For more information, see the *PeopleSoft HR feed adapter Installation and Configuration Guide* at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/peoplesoft_hr/install_config/adapter_html_mstr.htm.

SAP HR Feed adapter
For more information, see the *SAP HR feed adapter Installation and Configuration Guide* at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/sap_hr/install_config/adapter_html_mstr.htm.

The Identity Governance administrator can also map the imported HR user attributes with the Identity Governance and Intelligence `USER_ERC` table. The administrator can select which target attributes are mapped to which Identity Governance and Intelligence attributes.

These onboarded users can then log on and access Service Center.

For information about importing HR feed profiles and creating an HR feed target, see the following topics:

- Importing HR feed adapter profiles
- Creating targets to support HR feed

For information about importing mapped attributes on a target, including the HR feed adapter profiles, see the following topics:

- Target type administration
- Target administration

For information about reconciliation of managed targets, including the HR feed adapter profiles, see the following topics:

- Reconciliation management
- Reconciliation timeout and failure threshold

Enhanced password management

Desktop Password Reset Assistant (DPRA) uses Identity Governance and Intelligence for password validation. Windows users can use the DPRA to reset and change their Windows password from their desktops by answering their preconfigured *security questions*.

Help Desks can assist Employees to complete password resets. They can access the Employees' *security questions* and conduct verification. If the Employee does not have preconfigured *security questions*, the Help Desk can assist the Employee to set up *security questions* and to perform a password reset after user authentication.

Employees receive an email notification when their password is expiring. They can do a password reset by responding to the *security questions*. Alternatively, Employees can request a one-time password to do a password reset. The one-time password is sent to the Employee's registered email address.

For more information about Desktop Password Reset Assistant configuration and usage with Identity Governance and Intelligence, see the following topics:

- Desktop Password Reset Assistant
- *Desktop Password Reset Assistant Installation and Configuration Guide* at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/dpr/install_config/dpr_html_mstr.htm
- Configuring the password service in Access Governance Core
- Configuring the password service in Process Designer

Self-service user interface customization

An Identity Governance administrator can view all the account attributes imported from a target system, including custom properties that are useful in account matching. With UI customization, an Identity Governance administrator can define the visibility, position, label localization, and UI rendering of the account custom property.

Creation of custom dashboards

To create a custom dashboard, an Identity Governance administrator can use the **Add from Query** action in Report Designer to create a custom dashboard that is based on a defined query, and use the properties of the query to set up the dashboard visibility and attributes.

Single Sign-On support

Identity Governance and Intelligence provides alternative options to set up single sign-on for the Service Center with IBM Security Identity Manager and other applications.

OpenID Connect (OIDC)
Uses an external OIDC provider that works as a single point of authentication.

Lightweight Third-Party Authentication (LTPA)
Uses the LTPA token generated directly by the application servers.

IBM Security Access Manager based authentication
Uses LTPA keys that are shared by IBM Security Access Manager and the application servers.

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 4. How to get started

Task	**Reference**
Check what's new in this release.	Chapter 2, "What's new in Version 5.2.2," on page 15
Learn about the different components, personas, and user interfaces.	• Chapter 1, "Identity Governance and Intelligence overview," on page 1 • Chapter 4, "Roadmap of personas and tasks," on page 25 • Chapter 5, "User interface," on page 39
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. 1. Enter `Security Identity Governance and Intelligence`. 2. Select the product version. 3. Select the deployment unit. 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 47 • 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 28

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 5. Virtual appliance administrators deployment tasks

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

Table 5. 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 • Setting up the initial virtual appliance
For high availability, set up a virtual appliance cluster.	Setting up a virtual appliance cluster • Setting up a member node for IBM Security Governance and Intelligence by using the initial configuration wizard • Promoting the secondary node to the primary node • Promoting a member node to the secondary node • Enabling and disabling replication between the primary and secondary nodes • Promoting a member node to the primary node • Removing a node from the cluster • Reconnecting a node into the cluster • Synchronizing a member node with a primary node
Configure the virtual appliance settings.	• Enabling Identity Brokerage Providers • Managing directory server configuration • Managing the database server configuration • Managing OpenID connect configuration • Managing the mail server configuration • Managing application interfaces

Table 6. 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 2. Backing up the virtual appliance 3. Reverting the virtual appliance to its backup 4. Creating a snapshot of the virtual appliance 5. Setting up a secondary virtual appliance

Table 6. 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 • Viewing the memory usage • Viewing the CPU usage • Viewing the storage usage • Viewing the cluster status • Managing the SNMP monitoring
Configure the directory server, database server, OpenID connect providers, and mail server.	• Managing directory server configuration • Managing the database server configuration • Managing OpenID connect configuration • Managing the mail server configuration
Configure and manage the Postgres replication, IBM Security Directory Integrator instances, and cluster nodes.	• Managing the Postgres database • Managing Security Directory Integrator instances • Managing LTPA-based single sign-on configuration
Manage custom files, and certificate stores.	• Managing custom files • Managing certificates
Manage the virtual appliance updates and licensing.	• Viewing the update history • Viewing the licensing • Managing the firmware settings • 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 • Managing the core dump files • Enabling Identity Brokerage Providers • 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 • Managing hosts file • Configuring static routes • 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, and system audit events.	• Configuring the date and time settings • Configuring the administrator settings • Managing advanced tuning parameters • Managing the snapshots • Managing the support files • Configuring system audit events • Restarting or shutting down the appliance

Table 6. 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 • Tailing logs and archiving logs • Adding a JVM property • Managing the SSL certificate • Getting and setting the SIB schema names • 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 30
- "Process Designer module" on page 31
- "Access Optimizer module" on page 31
- "Report Designer module" on page 31
- "Task Planner module" on page 32

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

- "Application Managers" on page 32
- "User Managers" on page 33
- "Role Managers" on page 34
- "Risk Managers" on page 35

Back to top

Super Administrator

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

Table 7. 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). • Create an instance of the target from the target type. 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. • Create resources. See Resources. • Create entitlements. See Hierarchy of entitlements. • Create applications. See Applications. • Create accounts. See Accounts.
Configure organizational units.	• Create organization units. See Organization units. • Assign the organization unit to an entitlement. See Org Units. • Assign resources to an organization unit. See Group Resources.
Configure groups.	• Create groups. See Groups. • Assign entitlements to the group. See Entitlements. • Assign resources to the group. See Group Resources.
Configure roles.	• Create and publish roles. See Roles. • Define the entitlements. See Management.
On-board administrators.	1. Create the Administrator role. See Admin Roles. 2. Assign organization units to the Administrator role. See Org Units. 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. 2. Assign user to a role. See Users. 3. Assign an entitlement to the user. See Entitlements. 4. Assign resources to the user. See User Resources. 5. Create and manage the accounts for the registered user. See Accounts. 6. Assign rights. See Rights. 7. Set a mitigation action if the user is assigned with a risk level. See Mitigations.

Table 7. 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. • Search for the external role you want to assign. • Check whether the external role configuration is set for user assignment on the target system. See Application Access. 2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements. 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. 2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface. 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 8. 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 8. 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 9. 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 10. 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 11. Sample tasks in the Report Designer module

Tasks	Subtasks and references
Create and customize report queries.	Query

Table 11. 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 12. 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 13. 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). • Create an instance of the target from the target type. Specify the target identity and other information to connect to the server where the target resides. See Creating targets.

Table 13. 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. 2. Assign user to a role. See Users. 3. Assign an entitlement to the user. See Entitlements. 4. Assign resources to the user. See User Resources. 5. Create and manage the accounts for the registered user. See Accounts. 6. Assign rights. See Rights. 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. • Search for the external role you want to assign. • Check whether the external role configuration is set for user assignment on the target system. See Application Access. 2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements. 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. 2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface. See General

Back to top

User Managers

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

Table 14. 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. 2. Assign user to a role. See Users. 3. Assign an entitlement to the user. See Entitlements. 4. Assign resources to the user. See User Resources. 5. Create and manage the accounts for the registered user. See Accounts. 6. Assign rights. See Rights. 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. • Search for the external role you want to assign. • Check whether the external role configuration is set for user assignment on the target system. See Application Access. 2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements. 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. 2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface. 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 15. Role Managers tasks in the Administration Console

Tasks	Subtasks and references
Configure roles.	• Create and publish roles. See Roles. • Define the entitlements. See Management.

Table 15. 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. 2. Assign user to a role. See Users. 3. Assign an entitlement to the user. See Entitlements. 4. Assign resources to the user. See User Resources. 5. Create and manage the accounts for the registered user. See Accounts. 6. Assign rights. See Rights. 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 16. 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. • Search for the external role you want to assign. • Check whether the external role configuration is set for user assignment on the target system. See Application Access. 2. Add the entitlement. Assign the external role to the on-boarded user. See Entitlements. 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. 2. Set up the external service, which can be a REST WEB Service or an implementation of a JAVA interface. 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 17. 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 – Selecting the user – Answering security questions – Selecting the accounts – Entering the new password – Authorizing the request – Executing the request • Delegating requests – Generating a request – Processing a request • Creating entitlements – Generating a request – Processing a request – Executing a request • Modifying entitlements – Generating a request – Processing a request – Executing a request • Request user access – Generating a request – Processing a request – Executing a request • Creating users – Generating a request – Processing a request – 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 • Permission Perspective • Activity Perspective
Configure, run, and download the report.	• Request • 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 18. 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 19. 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 20. Identity Governance and Intelligence consoles

Consoles	URL	Description
Virtual Appliance Dashboard	`https://hostname:port`	Virtual appliance administrators can perform the following tasks: • 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, and system audit events.

Table 20. 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. 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. See "Service Center applications" on page 43 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 21. 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. Access Governance Core manages entities such as Users, Organization Units, Hierarchies, Entitlements, and Applications. It provides a modeler for outlining the organization's current situation. Identity Governance and Intelligence administrators can:also use this module to configure password services. 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. 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. 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. See Introduction to Access Optimizer.

Table 21. 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. Access Risk Controls enforces Segregation of Duties checks by relating the business activities model and application permissions. 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. 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. 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. 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. 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. Process Designer provides a modeler for outlining the access request and approval process and for integrating other external target systems. It works with the Access Governance Core module to manage: • Requests to access the system application. • Allocation and revocation of authorization profiles. • Password lifecycle. • Notifications that are sent to users during different phases of the authorization process. • Temporary delegations of personal roles that are associated with users of the system. • Definition of the visibility range that is associated with an administrative figure. See Introduction to Process Designer.

Table 21. Administration Console modules (continued)

Administration Console modules	Description
Target Administration	It is a tool that is used by administrators to perform target administration, including: • Import target profile. • Import account attributes mapping. • Configure account defaults for target profile. • Search, add, modify, and delete targets. • Manage reconciliation. • Set up account defaults for a target. 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. 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. 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. 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. Administrators can use Report Designer to: • Create and customize report queries. • Create and customize reports. • Create and customize dashboard items • Configure and assign dashboards. • Assign the product report to a user or an entitlement. • Organize the product reports. See Introduction to Report Designer.
Task Planner	It manages scheduled tasks and custom jobs. Identity Governance and Intelligence runs many internal jobs to support its own processes. Administrators can use Task Planner to: • Define different execution schedules. • Stop processes that are not required. • Implement and schedule custom jobs to better support specific scenarios. 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 22. 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. Managers can confirm or revoke user roles, roles assigned to the groups of a hierarchy (for example, organizational units), and user accounts. Access reviews and certifications can be scheduled, triggered automatically, or started manually. See Introduction to Access Certifier.
User-account matching	It manages orphan accounts from targets that are currently not matched with the organization's policies. 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. See Introduction to User-account matching.
Access Requests	It runs the Access Requests workflows configured in the Process Designer module. The main tasks available are: • Generate requests to change user roles. • Lock and unlock user accounts. • Request new roles. • Change and reset user passwords. 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. 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. 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. This module provides a simplified Access Risk Controls functionality that can be made available to users. See Introduction to Business Activity Mapping.

Table 22. 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. See Introduction to Report Client.
Self Care	It enables Users to: • Change the Service Center password. • Change the account password for active accounts. • View **Self Care** requests status. • 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. The Administrator Roles are: • Application Manager • User Manager • Employee

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 23. Supported languages

Locale code	**Language**
pt_BR	Brazilian Portuguese
en	English (United States)
fr	French
de	German
it	Italian
ja	Japanese
es	Spanish
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 upper-case "I" is not correctly read from DB2 repository

During a search in a generic UI panel, for recovering textual data where could be present the Turkey upper-case "I", the search fails into in DB2 repository (while is functioning 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.

Chapter 8. Cookbooks

Cookbooks are scenario-based, step-by-step guides that provide how-to information and tasks so 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

N

Printed in USA