IBM Security Identity Governance and Intelligence
Version 5.2.1

Product Overview Topics

IBM Security Identity Governance and Intelligence
Version 5.2.1

Product Overview Topics

Table of contents

Table list

Chapter 1. Identity Governance and Intelligence overview

IBM® Security Identity Governance and Intelligence delivers one platform for organizations to analyze, define, and control user access and access risks. 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.
- 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.
- Password management, which makes changing or resetting passwords more efficient and secure.
- Persona-based dashboards that help with tasks prioritization.

Virtual appliance overview

The IBM Security Identity Governance and Intelligence virtual appliance is an appliance-based identity governance and administration solution.

The virtual appliance includes the following features:

- A configuration wizard for the first time configuration of IBM Security Identity Governance and Intelligence virtual appliance, and for creating clusters.
- A dashboard for viewing system status, such as disk usage, and notifications, interfaces, middleware monitor, quick links, partition information, and server control.
- Analysis and diagnostics tools such as memory, CPU and storage statistics, SNMP monitoring, and troubleshooting log files.
- A configuration tool for managing the IBM Security Identity Governance and Intelligence database, service settings, certificates, and clusters.
- The controls for the virtual appliance settings such as updates and licensing, network settings, and system settings.

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 an external data tier.

The following diagram illustrates the Identity Governance and Intelligence architecture.

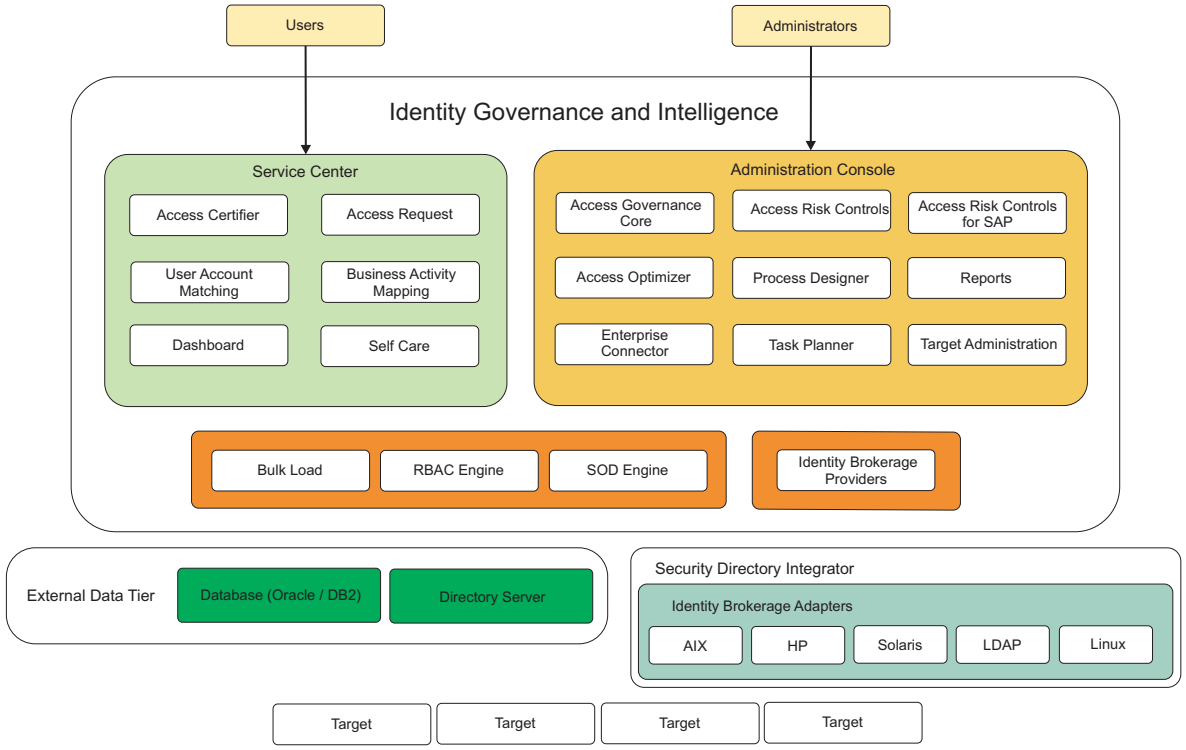

Figure 1. Identity Governance and Intelligence architecture

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 4 and Chapter 5, "User interface," on page 31 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 Manager Adapters. These IBM Security Identity Manager Adapters are called Identity Brokerage Adapters in Identity Governance and Intelligence.

Directory integrator

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

- AIX®
- HP
- LDAP
- Linux
- Solaris

To install additional adapters or update the embedded adapters, the Administrator must install the adapters externally. Depending on the adapter, an external Security Directory Integrator may be required.

To install and configure the supported adapters, see Installing and configuring Identity Brokerage Adapters for the general information. See the corresponding *Installation and Configuration Guide* for the prerequisites and other installation and configuration tasks specific to the Identity Brokerage Adapter that you want to use.

Note: The PDF formats are available at Identity Adapters Product Documentation in PDFs: http://www-01.ibm.com/support/docview.wss?uid=swg21689113.

External data tier

The external data-tier consists of the database server and the directory server.

For the supported database server and directory server, see the IBM Security Identity Governance and Intelligence Software Product Compatibility Report.

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.

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

Features overview

Identity Governance and Intelligence is an integrated identity governance solution, which offers several capabilities.

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.

Target integration:

- Provides a gateway to directly integrate with targets and hubs by using common adapters.
- Adds support for complex application entitlement structure through external roles.
- Adds support for zSecure-RACF integration by using a target integration framework and external roles.

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:

- "Identity Brokerage Adapters" on page 8
- Target type administration
- Target administration

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.

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.

Identity Brokerage Adapters

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 Manager Adapters. These IBM Security Identity Manager Adapters are called Identity Brokerage Adapters in Identity Governance and Intelligence.

Identity Brokerage Adapters enable communication between Identity Governance and Intelligence and the target systems. These adapters implement identity provisioning and target reconciliation.

Comparison summary

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

Important: Use the Identity Brokerage Adapters instead of the Enterprise Connectors except when you want to retrieve human resources (HR) data. HR data is only available through 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

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

Compare	Identity Brokerage Adapters	Enterprise Connectors
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**
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.

List of Identity Brokerage Adapters

This section lists the supported Identity Brokerage Adapters and links to their corresponding *Installation and Configuration Guide* in the Knowledge Center. The PDF formats of these publications are available at Identity Adapters Product Documentation in PDFs: http://www-01.ibm.com/support/docview.wss?uid=swg21689113.

Note:

- The following information are accurate at the time of publication. Alternatively, you can refer to the Adapters for IBM Security Identity Manager v7.0: http://www-01.ibm.com/support/docview.wss?uid=swg21687732. The technote is constantly updated to include the latest inventory of adapters that are released; their version, release date, download part numbers, and release notes.
- To install and configure the supported adapters:
  1. See Installing and configuring Identity Brokerage Adapters for the general information.
  2. See the corresponding product documentation for the prerequisites, other installation and configuration tasks, and issues and limitations specific to the Identity Brokerage Adapter that you want to use.
  3. See the Adapters release notes for any updates to these references.

Table 4. Host edition adapters

Adapters	Supported in Identity Governance and Intelligence	Product documentation
CA ACF2	**Yes**	CA ACF2 Security for z/OS Adapter

Table 4. Host edition adapters (continued)

Adapters	Supported in Identity Governance and Intelligence	Product documentation
CA TopSecret	*No*	CA Top Secret for z/OS® Adapter
iSeries (i5OS)	**Yes**	IBM i Adapter Installation and Configuration Guide
Password Sync Plug-in for iSeries	*No*	IBM i Password Synchronization Plug-in Installation and Configuration Guide
RACF	*No*	RACF Security for z/OS® Adapter
zSecure RACF	**Yes**	zSecure RACF Installation and Configuration Guide

Table 5. Application edition adapters

Adapters	Supported in Identity Governance and Intelligence	Product documentation
Box Cloud	**Yes**	Box Adapter Installation and Configuration Guide
Documentum Content Server	**Yes**	Documentum Adapter Installation and Configuration Guide
Google Applications	**Yes**	Google Apps Adapter Installation and Configuration Guide
Mircosoft Office 365	**Yes**	Office 365 Adapter Installation and Configuration Guide
Oracle eBusiness Suite	*No*	Oracle eBS Adapter Installation and Configuration Guide
PeopleTools	**Yes**	PeopleTools Adapter Installation and Configuration Guide
Remedy AR System	**Yes**	Remedy AR System Adapter Installation and Configuration Guide
Salesforce.com	**Yes**	Salesforce.com Adapter Installation and Configuration Guide
SAP HANA Database	**Yes**	SAP HANA Database Adapter Installation and Configuration Guide
SAP NetWeaver	**Yes**	Directory Integrator-based Adapter for SAP NetWeaver Adapter Installation and Configuration Guide
SAP Sybase DB	**Yes**	Sybase Adapter Installation and Configuration Guide
SAP UME (Portal)	**Yes**	Directory Integrator-based Adapter for SAP User Management Engine Adapter Installation and Configuration Guide
ServiceNow	**Yes**	ServiceNow Adapter Installation and Configuration Guide
SharePoint	**Yes**	Microsoft SharePoint Adapter Installation and Configuration Guide
Siebel	**Yes**	Siebel JDB Adapter Installation and Configuration Guide

Table 6. Infrastructure edition adapters

Adapters	Supported in Identity Governance and Intelligence	Product documentation
Azure Active Directory	**Yes**	Azure Active Directory Adapter Installation and Configuration Guide
Blackberry Enterprise Server	*No*	BlackBerry Enterprise Server Adapter Installation and Configuration Guide
Cisco Unified Communications Manager	*No*	Cisco Unified Communications Manager Adapter Installation and Configuration Guide
Command Line	**Yes**	CLIx Adapter Installation and Configuration Guide
Desktop Password Reset Assistant (DPRA)	*No*	Desktop Password Reset Assistant Installation and Configuration Guide
Groupwise (Windows only)	*No*	GroupWise Adapter Installation and Configuration Guide
IBM DB2	**Yes**	IBM DB2 Adapter Installation and Configuration Guide
IBM Security Access Manager (ISAM)	**Yes**	IBM Security Access Manager Adapter Installation and Configuration Guide
IBM Security Access Manager for Enterprise Single Sign-On (ISAM ESSO)	*No*	IBM Security Access Manager Enterprise Single Sign-On Adapter Installation and Configuration Guide
IBM Privileged Identity Manager	*No*	IBM Security Privileged Identity Manager Adapter Installation and Configuration Guide
LDAP	**Yes**	LDAP Adapter Installation and Configuration Guide
Linux	**Yes**	UNIX and Linux Adapter Installation and Configuration Guide
Lotus Notes (Windows only)	**Yes**	Lotus Notes Adapter Installation and Configuration Guide
Novell NDS (Windows only)	*No*	Novell Directory Services Adapter Installation and Configuration Guide
Oracle Database	**Yes**	Oracle Database Adapter Installation and Configuration Guide
Password Sync Plug-in for ISAM	*No*	Password Synchronization Plug-in for IBM Security Access Manager 7.0 Installation and Configuration Guide
Password Sync Plug-in for WinAD 64-bit	*No*	Password Synchronization for Active Directory Plug-in Installation and Configuration Guide
RSA Authentication Manager	**Yes**	RSA Authentication Manager Adapter Installation and Configuration Guide
SAP Sybase DB	**Yes**	Sybase Adapter Installation and Configuration Guide
SoftLayer	**Yes**	SoftLayer Adapter Installation and Configuration Guide

Table 6. Infrastructure edition adapters (continued)

Adapters	Supported in Identity Governance and Intelligence	Product documentation
SQL Server (Windows only)	**Yes**	SQL Server Adapter Installation and Configuration Guide
Unix/Linux (AIX)	**Yes**	UNIX and Linux Adapter Installation and Configuration Guide
Unix/Linux (HP-UX)	**Yes**	UNIX and Linux Adapter Installation and Configuration Guide
Unix/Linux (Solaris)	**Yes**	UNIX and Linux Adapter Installation and Configuration Guide
Windows Active Directory 64-bit	**Yes**	Active Directory Adapter Installation and Configuration Guide
Windows Local Account	**Yes**	Windows Local Account Adapter Installation and Configuration Guide

Chapter 2. What's new in Version 5.2.1

This version delivers password and user management services, persona-based dashboards, and a new method for clustering and OpenID authentication.

Password administration and management

The following password services are available:

- Administrators can force users to change their password the next time that they log in to the Service Center.
- Administrators, managers, and help desk personnel can reset passwords for other users.
- Employees can change or reset their own password by using the Self Care application.
- Employees can update their security questions by using the Self Care application.
- If Service Center users forget their Service Center password, they can reset it by using the **Forgot password** option.

In the Administration Console, a **Configure Password Service** panel is added in the **Access Governance Core** module, so administrators can:

- Enable the **Forgot password** option.
- Set the number of *security questions* that the users must answer at their first login and for password resets.
- Set the number of correct answers that the users must provide.
- Set the policy for changing or resetting passwords, such as the use of a system-generated password that is sent to a user's email address.
- Define new *security questions* for the users to select when they set up the answers to the security questions.

In the **Process Designer** module, the configuration of the *Account Change* process has options for password reset.

- Identity Governance and Intelligence administrators can create workflows that enable entitled users to reset user passwords with several options for identity verification, password generation, and delivery.
- The **Service Center** > **Access Requests** application has two predefined workflows:

  ManagerPasswordReset
  : User Managers can reset passwords for users of the same organization unit without using the *security questions*.

  HelpDeskPasswordReset
  : Help Desks can reset passwords for users only after the *security questions* are answered correctly.

For Business users such as Managers and Employees, the **Service Center** has the following enhancements:

- A Self Care application with options to change the Service Center password and account password. Employees can perform routine password management for their individual accounts.

- A **Forgot password** option, so users can reset their password if they forgot their Service Center password. Users are authenticated with their predefined *security questions*, and a system-generated password is sent through the registered email address.
- An Access Requests workflow that enables Managers to reset account passwords for their Employees.

Learn more:

- For Identity Governance and Intelligence administrators, see Password administration.
- For User Managers and Help Desks, see Password management.
- For Employees, see Logging in to the Service Center.

User management

Business users can create and update Users profile in the **Service Center** > **Access Requests** module. This feature is configured in the **Access Governance Core** and **Process Designer** modules.

Attribute mapping is enhanced to define default and editable attributes, attribute types, and possible values. An Identity Governance and Intelligence administrator, entitled to use the **Process Designer** module, can model the user management related activities using the attribute mapping configuration.

Learn more:

- User virtual attributes
- Modeling an activity
- Create user: generating a request
- Update user generating a request
- Create/Update user: processing a request

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.

An Identity Governance and Intelligence administrator can perform the following tasks.

- Copy and customize provided dashboard items in the **Report Designer** module.
- Assign dashboard items to an Entitlement.
- Review Administrator Role configuration.
- Assign users to Administrator Roles.

The following table lists the provided Administrator Roles and the dashboard items that are initially assigned to each.

Table 7. Dashboard items for provided Admin Roles

Administrator Role	Dashboard items
Application Manager	• Accounts created in the last *x* days • Activities created in the last *x* days • Permissions created in the last *x* days • Unmatched accounts • Account matching status • Accounts expiring in the next *x* days with Application scope • Business activity mapping status
User Manager	• Delegation assignments • User violations without mitigation control • Locked accounts • Accounts expiring in the next 30 days • Approval tasks • Access certification status • User violations
Employee	• Recent requests • My entitlements • My requests • Days until the next password expiration • Partial requests • Policy violation requests • Rejected requests • Access request history

Learn more:

- Dashboards for Service Center
- Available dashboard items
- Service Center

Administration and Management Services for Clusters

The Identity Governance and Intelligence virtual appliance is enhanced to provide administration and management services for clusters.

A configuration wizard can create multiple nodes for the IBM Security Identity Governance and Intelligence cluster. This feature replaces the manual process of setting up a virtual appliance cluster through the **Import/Export Service Settings**.

Virtual appliance administrators can also use the following options in the Appliance Dashboard:

- Use the **Configure** > **Manage Cluster** menu to
  - Change a member node to a primary node.
  - Remove a node from a cluster.
  - Reconnect a removed node into the cluster.
  - Synchronize a member node with a primary node.

Note: The **Configure** > **Manage Cluster** menu is displayed only in a cluster, not in a stand-alone environment.

- Use the **Cluster Status** widget to view the status of all the nodes in a cluster.

Learn more:

- Setting up a virtual appliance cluster
- Viewing the cluster status

OpenID authentication support

Administrators can add and configure OpenID Connect providers and use OpenID authentication in the Service Center.

Learn more: Managing OpenID connect configuration

Documentation updates

In addition to the documentation that supports new functionality in product, the following documentation sections are new or have significant updates:

- Configuring iToken to implement a custom single sign-on
- Amazon EC2 support
- Updating the DB2 server for V5.2.1 manually
- Updating the DB2 server for V5.2.1 semi-automatically
- Updating the Oracle server for V5.2.1 manually
- Updating the Oracle server for V5.2.1 manually
- Data import with Bulk Data Load

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 8. How to get started

Task	**Reference**
Check what's new in this release.	Chapter 2, "What's new in Version 5.2.1," on page 13
Learn about the different components, personas, and user interfaces.	• Chapter 1, "Identity Governance and Intelligence overview," on page 1 • Chapter 4, "Personas and use cases," on page 19 • Chapter 5, "User interface," on page 31
Check the hardware and software requirements.	For the detailed system requirements, see the IBM Security Identity Governance and Intelligence Software Product Compatibility Report. 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 39 • Troubleshooting and support Guide

Chapter 4. Personas and use cases

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 21

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 9. 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
(Optional) Install and configure the directory server to use the Identity Brokerage Providers module.	Installing and configuring the directory server

Table 9. Virtual appliance administrators deployment tasks (continued)

Tasks	Subtasks and references
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 • Changing a member node to a 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 10. 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
Monitor event logs, memory, CPU, storage, and cluster status.	• Viewing the event logs • Viewing the memory usage • Viewing the CPU usage • Viewing the storage usage • Viewing the cluster status
Configure SNMP monitoring.	Managing the SNMP monitoring
Configure external entities such as database servers, and OpenID connect providers.	• Managing directory server configuration • Managing the database server configuration • Managing OpenID connect configuration
Configure mail servers, custom files, and certificate stores.	• Managing the mail server configuration • Managing custom files • Managing certificates

Table 10. Virtual appliance administrators maintenance tasks (continued)

Tasks	Subtasks and references
Manage the virtual appliance update history, and license, firmware settings, and fix packs.	• Viewing the update history • Viewing the licensing • Managing the firmware settings • Installing a fix pack
Manage log 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, routes.	• Managing application interfaces • Managing hosts file • Configuring static routes
Manage the Export/Import settings	Exporting or importing the configuration settings
Manage the virtual appliance system settings	• Configuring the date and time settings • Configuring the administrator settings • Managing the snapshots • Managing the support files • Configuring system audit events • Restarting or shutting down the appliance
Manage the virtual appliance by using the command line interface.	• Cleaning core dump files • Tailing logs and archiving logs • Enabling trace for the virtual appliance services • Adding a JVM property • Management 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
- Process Designer
- Access Optimizer
- Report Designer
- Task Planner

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

- "Application Managers" on page 26
- "User Managers" on page 27
- "Role Managers" on page 27
- "Risk Managers" on page 28

Back to top

Super Administrator

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

Table 11. 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.

Table 11. Super Administrator tasks (continued)

Tasks	Subtasks and references
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.
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

Table 11. Super Administrator tasks (continued)

Tasks	Subtasks and references
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 12. 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
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 13. 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 14. 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 15. Sample tasks in the Report Designer module

Tasks	Subtasks and references
Create and customize report queries.	Query
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 16. 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 17. 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.
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 18. 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 19. 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 19. 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 20. 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 21. Managers 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 22. 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 23. 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 24. Identity Governance and Intelligence consoles

Interface	Description
Virtual Appliance Dashboard	Virtual appliance administrators can perform the following tasks: • Monitor event logs, memory, CPU, storage, and cluster status. • Configure SNMP monitoring. • Configure external entities such as database servers, and OpenID connect providers. • Configure mail servers, custom files, and certificate stores. • Manage the virtual appliance update history, and license, firmware settings, and fix packs. • Manage log retrieval and configuration, core dumps, Identity Brokerage Providers configuration, and build information. • Manage network settings such as application interfaces, hosts files, routes. • Manage the Export/Import settings • Manage the virtual appliance system settings
Administration Console	It includes modules intended for Identity Governance and Intelligence administrators. Administrators can perform the following administration and configuration tasks: • Manage access, risk controls, and role administration. • Manage tasks, schedules, dependencies, and performance. • Manage enterprise connectors, and target systems. • • Change account passwords for users. • Force users to change their Service Center password on their next login. • Configure the password service. • Configure the Access Requests workflows for change password, forgot password, or password reset functionalities. • Define reports, their layout, localization, and users visibility restrictions. • Analyze trends, users, and roles. • Create and customize dashboard items. • Configure and assign dashboards.

Table 24. Identity Governance and Intelligence consoles (continued)

Interface	Description
Service Center	It includes applications intended for users who are not administrators. Business users, such as Managers and Employees can perform these tasks, where applicable. • Request, change, or delete user or other users access, depending on the persona. • View, authorize, or delegate requests, depending on the persona. • Certify access. • Run or schedule reports. • View user or team access status, or the team risk score. • Change the Service Center password by using the Self Care application. • Change the account password for active accounts by using the Self Care application. • Reset the account password for other users. • Reset own Service Center password by using the **Forgot password** option. • View **Self Care** requests status. • Update the *security questions* for account recovery.

Administration Console modules

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

Table 25. 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. 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 25. 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 25. 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. See "Identity Brokerage Adapters" on page 8.
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 • 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 26. 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 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 26. 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 27. Supported languages

Locale code	**Language**
pt	Brazilian Portuguese
en	English (United States)
fr	French
de	German
it	Italian
ja	Japanese
es	Spanish
zh	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 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.

Index

N

Printed in USA