opentext™

Identity Governance 4.3

User and Administration Guide

24.3 (v4.3.1)

Legal Notice

Contents

About this Book and the Library

The *User and Administration Guide* provides conceptual information about the NetIQ Identity Governance product and step-by-step guidance for compliance administration and governance tasks.

Intended Audience

This book provides information for Identity Governance compliance administrators and other product users who are responsible for a variety of governance tasks including collecting and publishing identity and application data, creating policies, analyzing data, reviewing access, fulfilling change requests, and verifying changes in your environment. Specifically, it provides conceptual information and instructions for the following Identity Governance users:

- Administrators such as Data Administrator, Review Administrator, and Insight Query Administrator
- Policy owners such as Separation of Duties (SoD) policy owners
- Application owners, managers, or supervisors
- Auditors
- Other users such as Review Owners, Reviewers, and Fulfillers

Other Information in the Library

The library provides the following information resources in addition to this guide. Visit the Identity Governance Documentation Web site to access all the documents in this library.

Release Notes

Provides information specific to this release of the Identity Governance product, such as known issues.

Installation and Configuration Guide

Provides installation and configuration information for the Identity Governance product. This book also provides upgrade information for current product installations.

Reporting Guide

Provides information about Identity Reporting for Identity Governance and how you can use the features it offers.

NetIQ Identity Manager Driver for Identity Governance

Provides information about how to install and configure the Identity Manager Driver for NetIQ Identity Governance. The Identity Governance driver allows you to provision application-specific permission catalog data from Identity Governance to Identity Manager, giving you the

ability to review and certify permission assignments using Identity Governance, as well as to request and provision these permissions using Identity Manager. The driver also can provision users in the Identity Vault for Identity Manager.

Administrator's Guide to Form Builder

Provides information about creating custom forms for specific permissions or applications.

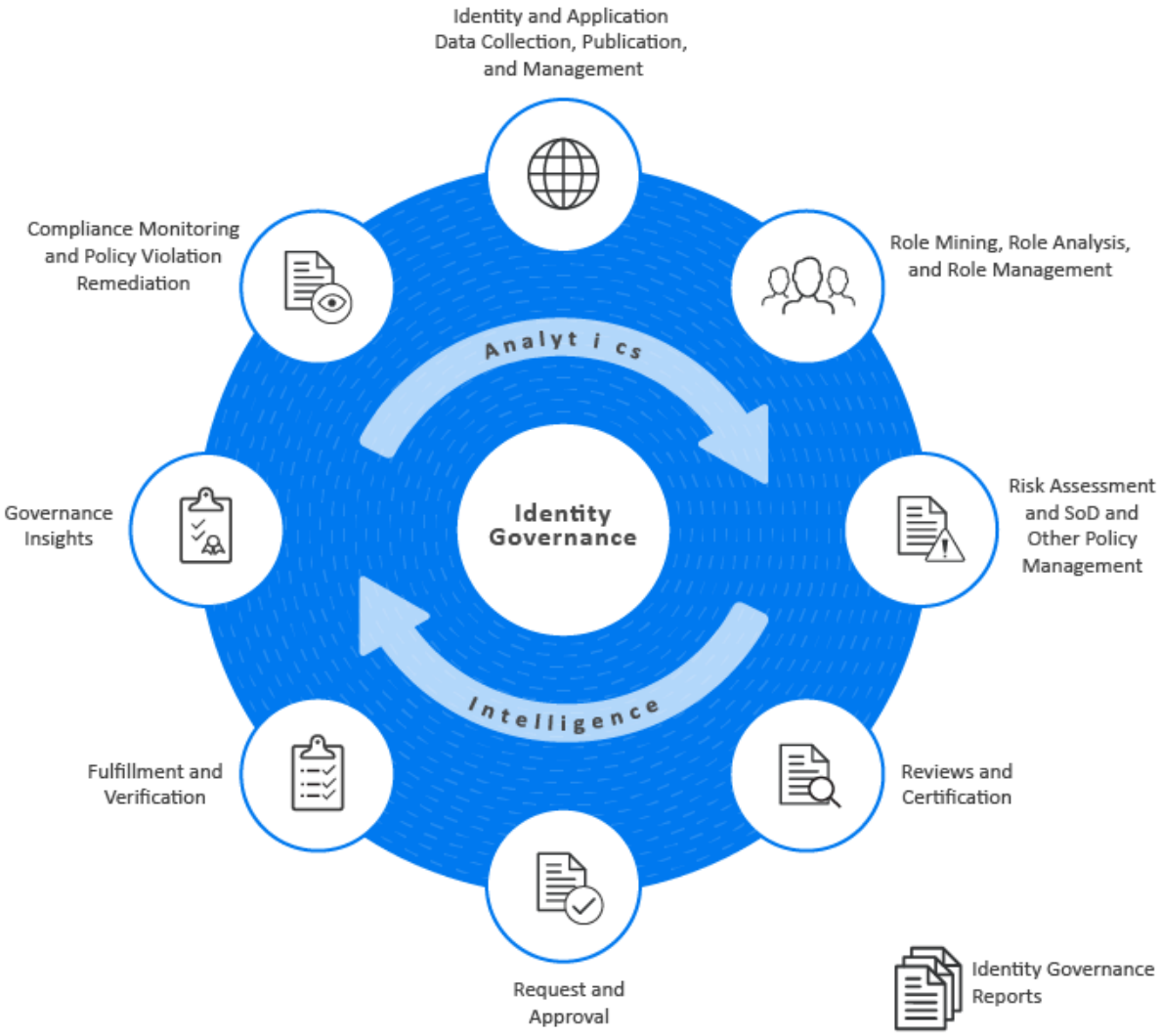
Technical References

Provide specific details about narrow topics relevant to few use cases.

1 Introduction

The Identity Governance product enables organizations to define policies, calculate risk, define and run reviews, and manage identity and access throughout your organization. With Identity Governance, administrators and business managers can prioritize governance activities based on risk and ensure that your employees, either individually or as a group, have the appropriate set of permissions. Identity Governance collects information from various identity and application data sources and guides the **authorized users** through the key phases of the governance process. You can install Identity Governance on premises or access it as a Service.

Figure 1-1 *Identity Governance Capabilities*



1.1 Understanding Installation and Configuration

You can install the components for Identity Governance in a distributed environment. Several of the components can also run in a high-availability cluster. You can also install Identity Reporting with Identity Governance. For information about installation and configuration, see the *Identity Governance 4.3.1 Installation and Configuration Guide*.

1.2 Understanding Key Administration and User Tasks

Identity Governance enables authorized users to:

- Collect identities, application, and application data
- Create application entities
- Transform, publish, and manage data
- Mine data and create technical and business roles
- Assign governance responsibilities
- Set risk thresholds and create SoD, data, and other policies
- Review users, accounts, technical and business roles, business role definitions, and relationships
- Request access and access removal
- Fulfill or deny requests, and verify changes
- Run analytics and gain governance insights
- Manage compliance and remediate violations

This guide provides detailed information about the various governance tasks and specific instructions about review owner, reviewer, requester, request approver, and fulfiller tasks.For information about how to log in to the Identity Governance application, see “How to Log in to Identity Governance” in the *Identity Governance 4.3.1 Installation and Configuration Guide*

NOTE: If you are logged in and your access token times out, a message appears stating that you must re-authenticate or log out of the application. If you re-authenticate, Identity Governance displays the login screen in a separate window or browser tab. You must log in again to continue working in the Identity Governance application.

1.3 Understanding Reporting

You can launch Identity Reporting from the Identity Governance application or access it directly from a browser. Identity Reporting enables you to generate reports about identity and application data, data collection and publication, reviews, and fulfillment status. Users with the Global, Customer, or Report Administrator role can create, run, and view the reports. For information about installing and configuring Identity Reporting, see the *Identity Governance 4.3.1 Installation and Configuration Guide*. For information about using Identity Reporting, see the *Identity Reporting Quick Start (https:/*

/www.netiq.com/documentation/identity-reporting/pdfdoc/rpt-quick-start/rpt-quick-start.pdf) and the *Identity Governance Reporting Guide (https://www.microfocus.com/documentation/identity-governance/4.3/pdfdoc/reporting-guide/reporting-guide.pdf)*.

1.4 Understanding Licenses

Qualified Identity Manager customers who have a limited access license for Identity Governance are entitled to install and use the identity catalog based features of Identity Governance to create and manage identities, accounts, groups, applications, permissions, and business roles. All other features are provided on a preview basis and cannot be fully enabled or used in production without the purchase of a full “per managed identity” license for Identity Governance 3.6 or later.

Some examples of Identity Governance features NOT covered by the limited access license are: Reviews, Review Settings, Coverage map loading for Reviews, Delegation, Risk policies, SoD policies, Certification policies, Data policies, Analytics settings and fact collections, and Governance Insights.

When the Limited License is installed you will see the following text in red at the top of the product page:

```
This feature requires a full Identity Governance license. Enter your
license in the About page to remove this message.
```

Enter your license in the About page to remove the message and get full access to Identity Governance features.

1.5 Understanding REST Services for Identity Governance

Identity Governance supports REST API functionality. The REST APIs use the OAuth2 protocol for authentication. The installation program deploys a special API WAR file, `apidoc.war`, which contains the documentation of REST services needed for Identity Governance. On Tomcat the `doc.war` file is automatically deployed when Identity Governance is installed.

The REST API documentation can be found at *protocol*://*server*:*port*/apidoc. For example, http://myserver.netiq.com:8080/apidoc.

NOTE: You should manually move or delete the API WAR files and folders from the Tomcat webapps directory in your production environment.

---

2 Adding Identity Governance Users and Assigning Authorizations

Individuals who can log in to Identity Governance are **Identity Governance users**. The authentication server for Identity Governance must include login information for all Identity Governance users. The source of data, or identity source, for these users could be your Human Resources directory or a CSV file. To ensure that users have a fixed set of permissions in Identity Governance, you can assign them to one of the built-in authorizations using the **Configuration > Authorization Assignments** menu.

2.1 Understanding Authorizations in Identity Governance

Identity Governance relies on authorizations to define a fixed set of access permissions. After installation of Identity Governance on premises and after deployment of Identity Governance as a service, the bootstrap administrator collects and publishes the initial set of identities and assigns a user as a Global or Customer Administrator who then assigns other authorizations. In SaaS environment, the Customer Administrator will work with a SaaS Operations Administrator to configure services and plan maintenance tasks. The SaaS Operations Administrator is a member of the SaaS team responsible for customer tenancy operations including data center configurations.

Identity Governance authorizations can be global or runtime:

- **Global authorizations** are constant within Identity Governance and assigned through the Identity Governance **Configuration** settings. Identity Governance maintains the set of privileges granted by the authorization. For more information, see Section 2.1.1, “Global Authorizations,” on page 20
- **Runtime authorizations** are those that users assume as needed to perform tasks specific to a governance area such as request, review, or fulfillment. For example, you assign a Review Owner as needed during an access review and validation cycle. You can reassign these authorizations with each review run. For more information, see Section 2.1.2, “Runtime Authorizations,” on page 23.

If a user does not have the required authorization or does not have an assigned task, the user will be redirected to the Access Request interface. For more information about requesting access, see Chapter 24, “Instructions for Access Requesters and Approvers,” on page 313. For more information about the bootstrap administrator, see “Understanding the Bootstrap Administrator for Identity Governance” in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

2.1.1 Global Authorizations

After collecting and publishing an initial set of identities, assign the Global Administrator authorization in an on-premises environment and Customer Administrator in a SaaS environment to one of these identities. The Global or Customer Administrator can then assign the rest of the global authorizations. For more information, see Section 2.3, “Assigning Authorizations to Identity Governance Users,” on page 27.

Customer Administrator (Identity Governance as a Service only authorization)

The Customer Administrator is the primary authorization for Identity Governance as a Service. This authorization is responsible for day-to-day business operations of the product and can:

- Perform all Identity Governance actions
- Assign all Identity Governance global and runtime authorizations for users in the enterprise

Global Administrator (Identity Governance on-premises only authorization)

The Global Administrator is the primary authorization for Identity Governance on-premises deployments. This authorization can:

- Perform all Identity Governance actions
- Assign all Identity Governance global and runtime authorizations

Access Request Administrator

The Access Request Administrator manages policies that define who can request access in your enterprise. This authorization can:

- Create, modify, and delete Access Request Policies
- Create, modify, and delete Access Request Approval Policies
- Edit the default Access Request Approval Policy
- Customize default request and approval forms
- Create and customize approval workflows
- Create custom request and approval forms for one or more permissions or applications

Auditor

The Auditor has read-only rights to the catalog, reviews, Separation of Duties (SoD) policies and violations, business roles, risk, certification policies, fulfillment statuses, and Governance Overview dashboard. However, this authorization can configure and run insight queries and an account assigned to the Auditor authorization might also be specified as a Review Auditor in a review definition. For more information, see Section 2.1.2, “Runtime Authorizations,” on page 23.

Business Roles Administrator

The Business Roles Administrator performs all administrative functions for all business roles. A Business Roles Administrator can delegate administrative privileges. This authorization can:

- Administer the business role schema under **Data Administration**
- Configure role mining settings
- Collect automated and business role mining metrics
- Mine for business roles and promote role candidates
- Create a business role

- Modify a business role
  - Add or change role owners, role managers, fulfillers, and categories
  - Add or change the business role approval policy
  - Add users and groups to the business role
  - Exclude users and groups from the business role
- Publish a business role
- Delete a business role
- Analyze business roles
- Configure the business roles default approval policy
- Create and modify business roles approval policies

Data Administrator

The Data Administrator manages the identity and application data sources. This authorization can:

- Create, add, modify, and review data sources
- Create custom metrics
- Create scheduled collections
- Execute data collection and publishing
- Create and map attributes in the catalog
- Review and edit data in the catalog
- Create custom request and approval forms for one or more permissions or applications
- Configure and run governance insight queries
- Delegate responsibility by assigning application administrators, application owners, or manual fulfillers to applications in the catalog
- Assign delegates for users
- View data collection, data summary, and system trends on the Governance Overview dashboard
- Perform data maintenance tasks including archiving and data cleanup

Maintenance Administrator

The Maintenance Administrator configures and performs data maintenance tasks such as archiving and data cleanup.

Governance Insights Administrator

The Governance Insights Administrator manages data queries. This authorization can:

- Configure and run governance insight queries
- Download and import insight queries

Fulfillment Administrator

The Fulfillment Administrator manages fulfillment and verification of requests that result from reviews. This authorization can access real time and historical data for provisioning activities, including fulfillment status and verification management.

Report Administrator

The Report Administrator can access Identity Reporting. This authorization can:

- Create, view, and run reports for Identity Governance
- Add, remove, and modify data sources on which you want to run reports

Review Administrator

The Review Administrator manages the review process but does not have access to data collection or fulfillment settings. This authorization can:

- Create, schedule, and start reviews in preview mode or live mode
- Modify a review schedule
- Assign all the runtime authorizations as part of a review, thereby delegating certain rights pertaining to the review to those authorizations
- View reviews in progress
- View the name of the person who started the review on demand, on schedule, or by micro certification
- View data summary and system trends on the Governance Overview dashboard
- View the **Catalog**, but cannot modify it

Technical Roles Administrator

The Technical Roles Administrator mines for technical role candidates and manages technical roles. A Technical Roles Administrator can delegate administrative privileges. This authorization can:

- Collect User to permission assignments metric
- Mine for technical roles and promote role candidates
- Create and delete technical roles
- Add or remove permissions from a technical role
- Add or remove categories
- Promote, activate, or deactivate technical roles
- Assign technical role owners
- Assign access request and approval policies
- Assign technical roles to users detected to have all the permissions included in a technical role
- Download or import technical roles

Security Officer

The Security Officer has read-only rights to the catalog and can:

- Assign authorizations for all functions in Identity Governance
- View data summary on the Governance Overview dashboard
- View the **Catalog**, but cannot modify it

NOTE: Ensure that the users assigned to the Security Officer authorization can also be trusted with global privileges in Identity Governance.

Separation of Duties Administrator

The Separation of Duties Administrator creates and manages SoD policies and violation cases.

Workflow Administrator

The Workflow Administrator creates and edits custom workflows. For additional information about their access rights in Workflow Administration Console, see the *Workflow Administration Guide*.

2.1.2 Runtime Authorizations

Assign runtime authorizations when you need them. For more information, see Section 2.3, “Assigning Authorizations to Identity Governance Users,” on page 27.

Access Requester

Access Requesters request application access, permissions, and technical role assignment. Identity Governance Access Request Administrator, Customer Administrator, and Global Administrator define the Access Request policy that specifies who can request access, what can they request, and for whom can they make their requests.

Access Request Approver

Access Request Approvers confirm whether to approve or deny requested access in the Request application. Identity Governance assigns this authorization if an Access Request Approval policy specifies approvers. Access request approvers can also reassign their task to another approver.

Application Owner

The Application Owner manages all assigned applications. This authorization can:

- View and manage the following information in the catalog:
  - The applications in the catalog for which they are an owner or administrator
  - The accounts associated with those applications
  - All identities in the system, but details of the identities are restricted to only the permissions and account for which they are an owner or administrator.
  - All groups
- Create custom request and approval forms for assigned applications and permissions under the assigned applications
- Perform data editing for assigned applications
- Review data and access within the assigned applications if assigned as a reviewer
- (Conditional) Review access entitlements or remediate access policy violations within the application if assigned this responsibility by the review definition

Application Administrator

The Application Administrator validates published data and performs data cleanup, or editing, for all assigned applications. This authorization can:

- Edit data within the scope of the data source
- Review data and access within the data source

- View the catalog but edit only items related to the assigned data source
- Create custom request and approval forms for assigned applications and permissions under the assigned applications

Business Role Owner

The Business Role Owner can review a business role and approve a business role depending on whether the assigned approval policy specifies **Approved by owners**. Business role owners cannot edit business roles, they can only view them. For more information about approval policies, see Chapter 19, “Creating and Managing Business Roles,” on page 229.

Business Role Manager

A Business Role Manager is an optional participant in the business role process. This authorization can:

- Edit assigned business roles
- Submit business role for approval, if approval is required based on approval policy
- Promote role candidates
- Publish roles
- Deactivate roles

NOTE: Role Managers cannot delete a role. Only Global or Business Role Administrators can delete roles.

Escalation Reviewer

The Escalation Reviewer is an optional participant in a review. All tasks not completed on time are forwarded to the Escalation Reviewer for resolution. Otherwise, the tasks are forwarded to the Review Owner. This authorization can:

- View user, permission, application, and account details in the context of the review
- Decide whether to keep, modify, or remove access privileges for a user under review
- Edit review decisions before submitting those items

Fulfiller

The Fulfiller performs manual provisioning for access changes. This authorization can:

- View the changeset, identity, permission, and application details for each fulfillment request
- View guidance from collected analytics data about the requested change
- View the reason for the requested change and the source of the request, such as a review run, business role fulfillment, or SoD policy
- Fulfill, decline to fulfill, or reassign requests

Review Auditor

The Review Auditor verifies a review campaign. Each review can have its own Review Auditor. This authorization can:

- Accept or reject the review after the Review Owner marks the review complete

- View the name of the person who started the review on demand, on schedule, or by micro certification
- View the data related to the review, but cannot modify the data

Review Owner

The Review Owner manages all assigned review instances. The Review Owner can view the details of any user, permission, or application entity within the context of the review. This authorization does not have general access to the catalog.

The Review Administrator who initiates a review automatically assumes the authorization of Review Owner if no Review Owner is specified.

NOTE: If you assign a new owner to a review, both the previous and new owners can access the review. The previous owner continues to see review instances run before the ownership change. The new owner sees only the instances run after the ownership change.

For an active Review, the Review Owner can:

- Start and monitor the review progress
- Resolve access policy violations in the review
- Reassign certification tasks within the review
- Run reports against the review
- Declare the review complete
- View the review status on the Governance Overview dashboard
- View **Quick Info** details about a catalog item
- View the fulfillment status of a review item
- View the run history

Reviewer

The Reviewer authorization reviews sets of access permissions or memberships as part of a review run. This authorization can:

- Decide whether to keep, modify, or remove access privileges for a user under review
- Decide whether to keep or remove the business role membership for a user under review
- Change the reviewer for any assigned review items
- View user, permission, application, and account details in the context of the review
- View a history of review decisions in the context of the review
- View guidance on how a permission is assigned, such as through a direct assignment or authorized by a role
- View current assignment details by clicking the review item links, if an administrator selected the assignment attributes as default columns to display for user and account access review
- Add a comment to a review item with the decision to keep or remove, individually or in a batch
- Edit review decisions before submitting them

SoD Policy Owner

The SoD Policy Owner is responsible for managing assigned Separation of Duties policies. This authorization can:

- Manage assigned policies
- Manage violation cases for assigned policies

Technical Role Owner

The Technical Role Owner is responsible for managing technical roles for which they are the owner. Owners cannot import, create, promote, delete, or assign access request policies to a role. This authorization can:

- Add or remove permissions from a technical role
- Add or remove categories
- Activate or deactivate technical roles
- Assign technical role owners
- Assign technical roles to users detected to have all the permissions included in a technical role
- Download technical roles

2.2 Adding Identity Governance Users

Until you collect data for your Identity Governance users, they cannot log in to the application. For more information about the bootstrap administrator account, see "Understanding the Bootstrap Administrator for Identity Governance" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

NOTE: In a test environment that does not also use Identity Manager, you might not have an LDAP authentication server to use for your data source. Instead, you can use a CSV file that contains login information for Identity Governance users. The CSV file must use UTF-8 encoding.

To add Identity Governance users:

1. Log in to Identity Governance with an Identity Governance Bootstrap or Global Administrator account.
2. Select **Data Sources > Identities**.
3. Under **Identity Sources**, select the LDAP authentication server specified during installation.

   Alternatively, you can specify a CSV file.

   NOTE: If Identity Governance does not list the authentication server, select **+** to add the identity source. For more information, see Section 7.4, "Creating Identity Sources," on page 90.

   ---

4. To collect the identities from the authentication server, select the icon for **Collect Now**. Later, you can set up scheduled collections to update your catalog.

   For more information, see Chapter 10, "Creating and Monitoring Scheduled Collections," on page 109.
5. When collection completes, select the icon for **Publish identities now**.

6 Assign Identity Governance authorizations to the appropriate identities that you collected.

For more information, see Section 2.3, "Assigning Authorizations to Identity Governance Users," on page 27.

2.3 Assigning Authorizations to Identity Governance Users

The method for assigning authorizations in Identity Governance depends on the type of authorization and your environment.

Authorization	Assignment Method	Assigned By
Access Request Approver	Access Request Approval policy	Access Request Administrator, Customer Administrator, or Global Administrator
All global authorizations	Authorization Assignment (**Configuration** > **Authorizations**)	Bootstrap Administrator, Customer Administrator, or Global Administrator
Application Administrator	Application in the catalog	Application Owner, Data Administrator, Customer Administrator, Global Administrator, or Security Officer
Application Owner	Application in the catalog or review definition	Data Administrator, Customer Administrator, Global Administrator, or Security Officer
Business Role Manager	Business role definition	Business Roles Administrator, Customer Administrator, Global Administrator, or Security Officer
Business Role Owner	Business role definition	Business Roles Administrator, Customer Administrator, Global Administrator, or Security Officer
Escalation Reviewer	Review definition	Review Administrator, Customer Administrator, or Global Administrator
Fulfiller	Application setup in **Fulfillment** > **Configuration** or Business role definition	Business Roles Administrator, Fulfillment Administrator, Customer Administrator, Global Administrator, or Security Officer
Permission Owner	Review definition	Customer Administrator, Global Administrator, Data Administrator, or Security Officer
Review Auditor	Review definition	Review Administrator, Customer Administrator, or Global Administrator
Review Owner	Review definition	Review Administrator, Review Owner, Customer Administrator, or Global Administrator

Authorization	Assignment Method	Assigned By
Reviewer	Review definition	Review Administrator, Customer Administrator, or Global Administrator
SoD Policy Owner	SoD policy definition	Separation of Duties Administrator, Customer Administrator, or Global Administrator
Technical Role Owner	Technical role definition	Technical Roles Administrator, Customer Administrator, or Global Administrator

2.4 Using Coverage Maps

Coverage maps allow administrators to map review or access request items to respective reviewers or approvers when creating a review definition or an access request approval policy. Coverage maps use one or more rules to specify:

- An entity type or attribute based on the item under review
- Different entity and attribute criteria in a single column
- Secondary or related entity or attribute of related entity referenced by entity-entity relationships

For more information, see:

- Section 2.4.1, “About Coverage Map Rules,” on page 28
- Section 2.4.2, “Using Criteria Definitions in Rules,” on page 29
- Section 2.4.3, “Using Operators, Conditions, Filters, Relationships, and Attributes in Rules,” on page 29
- Section 2.4.4, “Supported Relationships,” on page 29
- Section 2.4.5, “Creating Rules for Coverage Maps,” on page 30
- Section 2.4.6, “Creating a Coverage Map,” on page 31
- Section 2.4.7, “Coverage Map — An Example,” on page 32
- Section 2.4.8, “Exporting and Importing a Coverage Map,” on page 33
- Section 2.4.9, “Creating Coverage Map Using a CSV File,” on page 33
- Section 2.4.10, “Loading a Coverage Map CSV File,” on page 37
- Section 2.4.11, “Editing a Coverage Map,” on page 37
- Section 2.4.12, “Deleting a Coverage Map,” on page 38

2.4.1 About Coverage Map Rules

Coverage maps comprise one or more rules that define and specify the following:

- Reviewers of a **User Access** or **Account Review** definition

NOTE: To specify a coverage map as a reviewer for unmapped accounts, ensure that **All unmapped accounts** is selected for the review items, and then specify **Review by Coverage Map** as the reviewer.

- Approvers for requested access in the **Request** application

To create coverage map rules, Identity Governance uses an interface similar to the advanced filter for searches. The interface uses conditions and subconditions to define rules for coverage maps. You can also export the coverage map that you create, and import coverage maps that others have created.

2.4.2 Using Criteria Definitions in Rules

Criteria options in the rules interface correspond with the criteria that you define in your rules. For example, if you want to create a condition for your rule that specifies users with specific titles, select **User: Title**.

2.4.3 Using Operators, Conditions, Filters, Relationships, and Attributes in Rules

The rules interface uses the **operators** AND, OR, and NOT to create expressions that direct the rule definition to include, respectively, ALL of the conditions you define, ANY of the conditions you define, or NONE of the conditions you define in the search filter. Select one of these operators to start building a filter. The operator you select applies to every condition you create.

Conditions allow you to specify a criteria option as a criterion for a rule, and then use additional operators, such as “equal to,” “not equal to,” “equals one of,” “does not equal any of,” “greater than,” “less than,” and “greater than or equal to,” to define how the rule includes, or if it excludes, the defined item in the coverage map as a result of the condition.

Filters are subconditions that allow you to fine-tune a condition with additional AND, OR, and NOT statements.

Relationships and **attributes** appear as options only when you define reviewer or approver criteria. Relationships require that you also assign and define an attribute for the relationship.

2.4.4 Supported Relationships

Relationships can be nested in coverage maps. However, relationships cannot be referenced in the `ReviewItem` criteria cell; they can be accessed only from the `Reviewer` or `Approver` criteria cell.

The supported predefined relationships appear below:

Coverage Map Type(s)	Entity	Relationship	Related Entity
`REVIEW` and `REQUEST`	`USER`	`supervsior`	`USER`
`REVIEW` and `REQUEST`	`USER`	`affiliate`	`USER`
`REVIEW` and `REQUEST`	`APPLICATION`	`applicationOwners`	`applicationOwners` (table)

Coverage Map Type(s)	Entity	Relationship	Related Entity
REVIEW and REQUEST	applicationOwners	owner	USER
REVIEW and REQUEST	applicationOwners	groupOwner	GROUP
REVIEW and REQUEST	PERMISSION	permissionOwners	resolved_spermission_owner (table)
REVIEW and REQUEST	PERMISSION	permissionHolders	saccount_permission and saccount_user (tables)
REVIEW and REQUEST	resolved_spermission_owner	owner	USER
REVIEW and REQUEST	ACCOUNT	accountHolders	saccount_user (table)
REVIEW and REQUEST	ACCOUNT	accountOwners (account custodians)	resolved_saccount_owner (table)
REVIEW only	USER	riuser (user under review)	USER
REVIEW only	saccount_user	holder	USER
REVIEW only	resolved_saccount_owner	owner	USER
REQUEST only	ROLE_POLICY (technical role)	role_policyOwners	policy_owner (table)
REQUEST only	policy_owner	owner	USER
REQUEST only	policy_owner	groupOwner	GROUP

2.4.5 Creating Rules for Coverage Maps

Rule creation requires that you create expressions to define and add criteria for your coverage map. Click **Define Criteria** to define conditions that create expressions for one or more of the following review or approval items:

- User
- Account
- Permission
- Application

Click **Add Criteria** to define conditions or relationships that create expressions for one or more of the following reviewer or approver criteria:

- User
- Group

2.4.6 Creating a Coverage Map

When you create a coverage map, Identity Governance searches for a matching statement in the order defined in the coverage map. When one or more review items match all defined review item criteria, the users or groups matching the respective user or group criteria become reviewers for those items.

To create a coverage map:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Policies** > **Coverage Maps**.
3. Click the add icon (+).
4. Type a name and a description for the coverage map.
5. Specify the coverage map type.
6. (Conditional) Create the Review Type coverage map rules.
   - **6a** Select **Review**.
   - **6b** Click the plus icon (+).
   - **6c** Under **Review Item Criteria**, click **Define Criteria**.

     NOTE: You are not required to define review item criteria. A rule may contain only a reviewer criteria.

   - **6d** Click the plus icon (+) for the criteria you want to define, and then use operators, conditions, and filters available to create one or more expressions for each criteria.

     NOTE: Some condition expressions require 1:1 mapping. For example, if the condition "User: Display Name **equals** `<Account Holder Display Name>`" returns more than one possible result, Identity Governance displays an error message. You should configure "User: Display Name **equals one of** `<Account Holder Display Name>`."

   - **6e** Click **Save**.
   - **6f** Under **Reviewer Criteria**, click **Add Criteria**, and then select either **Define Criteria** or **Define Relationship**.
   - **6g** Choose the criteria you want to define, and then use operators, conditions, and filters to create one or more conditions for each criteria.
   - **6h** Click **Save**.

   Perform these steps for each rule you want to add to your Review Type coverage map.
7. (Conditional) Create the Request Type coverage map rules.
   - **7a** Select **Request**.
   - **7b** Click the plus icon (+).
   - **7c** Under **Approval Item Criteria**, click **Define Criteria**.

     NOTE: You are not required to define approval item criteria. A rule may contain only an approver criteria.

7d Click the plus icon (+) for the criteria you want to define, and then use operators, conditions, and filters available to create one or more conditions for each criteria.

NOTE: Some condition expressions require 1:1 mapping. For example, “equals” is not valid if the rule could return more than one possible result. In those cases, “equals one of” is a valid choice.

7e Click **Save**.

7f Under **Approver Criteria**, click **Add Criteria**, and then select either **Define Criteria** or **Define Relationship**.

7g Choose the criteria you want to define, and then use operators, conditions, and filters to create one or more conditions for each criteria.

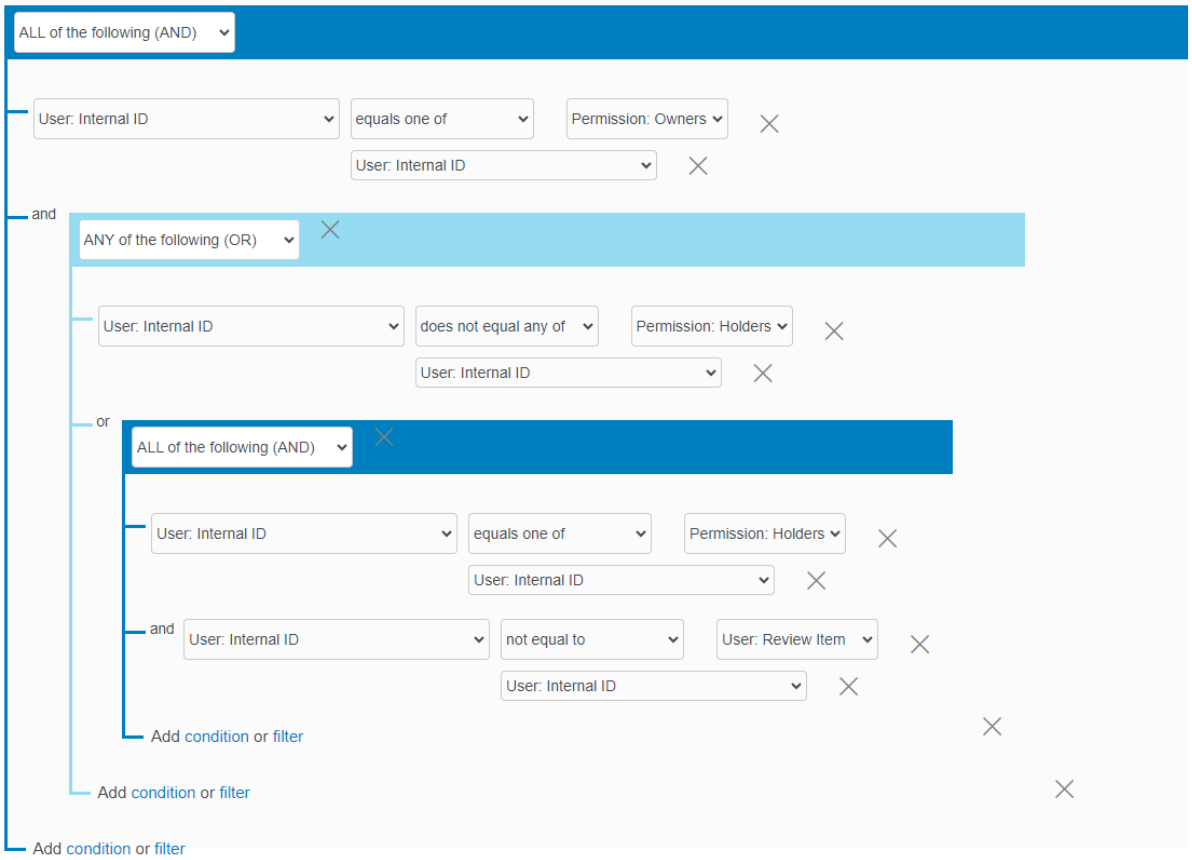
7h Click **Save**.

Perform these steps for each rule you want to add to your Request Type coverage map.

8 Click **Save**.

2.4.7 Coverage Map — An Example

Identity Governance provides the flexibility to create simple and complex coverage maps by selecting an entity, then defining additional criteria using advanced search filters. For example, you can use the advanced search filter to specify criteria as displayed below to create a review coverage map where reviewers can only be reviewers when they are the permission owner but not when the reviewer also has that permission and is not the user under review.



2.4.8 Exporting and Importing a Coverage Map

Identity Governance allows you to export one or more coverage maps to a file that you can download and share with others in your enterprise.

Identity Governance saves the following files to a ZIP archive in your browser download directory:

- A JSON file containing information for the coverage maps you chose to export
- A JSON file containing information for review definitions or access request approval policies (depending on the coverage map type) that use the coverage map(s)

You can share the downloaded file with others, who will extract the coverage map file before importing it. For more information about exporting and importing procedures, see Chapter 33, “Exporting and Importing,” on page 387.

NOTE: Before you run a review, verify all mappings in the review definitions to ensure the coverage map associations are correct.

2.4.9 Creating Coverage Map Using a CSV File

Identity Governance allows you to create coverage maps using CSV files, which you can then load into Identity Governance. You can use these files to map review or request items to respective reviewers or approvers by specifying:

- An entity type or attribute based on the item under review
- Different entity and attribute criteria in a single column
- Secondary or related entity or attribute of related entity referenced by entity-entity relationships

You should understand Identity Governance supported coverage map types, keywords, syntax, and entity-entity relationships to create and load coverage maps.

If you prefer to manually create a coverage map, you can create a CSV file with header and criteria cells. For greater flexibility use only keywords. For more information, see:

- “Supported Coverage Map Types and Keywords” on page 34
- “Supported Syntax for CSV Files” on page 34
- “About Relationships” on page 35
- “User Access Review Coverage Map Examples” on page 35
- “Account Review Coverage Map Examples” on page 36
- “Access Request Coverage Map Example” on page 37

Supported Coverage Map Types and Keywords

Identity Governance supports the following coverage map type attributes and keywords:

Type	Description	Keywords
REVIEW	Maps for user and group access and account review based reviews	◆ Reviewer ◆ ReviewItem
REQUEST	Maps for request based approver determination	◆ Approver ◆ RequestItem

Supported Syntax for CSV Files

Header and Criteria Cells Syntax

For	Syntax
USER or GROUP based reviewer header cell	<Reviewer.user|Reviewer.group>[.related user or group attribute key]
Review item header cell	<Approver.user|Approver.group>[.related user or group attribute key]
USER or GROUP based approver header cell	<Application|Permission|User]>[.entity-attribute-key]
Request item header cell	[RequestItem.]<Application|Permission|ROLE_POLICY|User>.<entity-attribute-key>
Keyword(s) only header	<Reviewer|ReviewItem> or <Approver|RequestItem>
Attribute based criteria cell	[<entity-name>.]<attribute-name> <Op> <value(s)>
Attribute and relationship based criteria cell	[<entity-name>.]<attribute-name> <Op> ReviewItem.<entity-name>.[<relationship-name>.]<attribute-name>

TIP: Specifying only keywords in the header column, and specifying other entity and attributes details in the criteria cells provides more flexibility than other formats.

Operator Syntax

Value entries for attributes that have numeric data types support the following list of comparison prefixes: >, >=, <, <=, !=, <>. For example: "Permission.risk","< 40".

Value entries for attributes with string data types support multiple values by using the pipe (|) symbol. For example, "Reviewer.user.displayName","Sue Smith|Jerry Jones|Tom Carter". Additionally, you can use the following operators:

- !IS_EMPTY! or !NULL!
- !IN!
- !CONTAINS!
- !MATCHES!
- !ENDS_WITH!
- !STARTS_WITH!
- !NOT!

Date Type

You can select date type attributes as conditions. The system evaluates date types in comparisons using ISO 8601 date and time format. The following are some examples of January 31, 2024:

- 2024-01-31
- 2024-01-31T10:00Z
- 2024-01-31T10:00-05:00

NOTE: Though the format allows for time to be specified, Identity Governance stores only the date in the catalog for date entity types.

About Relationships

The supported predefined relationships are listed in Section 2.4.4, “Supported Relationships,” on page 29.

IMPORTANT: When creating a CSV coverage map, any of the relationships that resolve to a table would need another segment to resolve to an ENTITY. For example, APPLICATION.applicationOwners is incomplete, because it resolves to a table. The complete expression should be: APPLICATION.applicationOwners.USER.<attributeName> or APPLICATION.applicationOwners.GROUP.<attributeName>

User Access Review Coverage Map Examples

USER based reviewer with risk and location as criteria

```
"Reviewer.user.displayName","Permission.risk","User.location"
"Sue Smith",">90","Boston"
"Charles Smith",">70","New York"
```

The first line is the header row and contains the column headers that identify the entity attributes that Identity Governance will use to determine reviewers.

The example uses the risk attribute from the permission entity and the location attribute from the user entity to match against review items. When a review item matches, the example uses the displayName attribute from the User entity to select a reviewer.

All the review item criteria columns must match for that row to be considered a match to the review item. In this example, the second line only matches a review item where the permission risk is greater than 90 and the user's location is Boston.

USER based reviewer with multiple criteria

```
"Reviewer.user.displayName","User.department"
"Armando Colaco","!STARTS_WITH! Opera"
"Charles Ward","!NOT! !MATCHES! Finance"
"Henry Morgan","!NOT! !NULL!"
```

The reviewer assignment attempts to perform a match on each row of the coverage map until a match has been found. The first line is the header row and contains the entity attributes that are being evaluated. The second row assigns Armando Colaco as reviewer if the department of the user under review starts with `Opera`. The third row assigns Charles Ward as reviewer for users who are not members of the Finance department. The fourth row assigns Henry Morgan as reviewer for users who are members of a department.

During coverage map processing, a matching row is searched for in the order they appear in the CSV file. After a match is found for a review item, the reviewers are assigned based on that matching row, and no further rows are processed for that review item.

NOTE: Any review items that do not find a match are assigned to the review exception queue.

Keywords only header with review item referenced in criteria cells

```
"ReviewItem", "Reviewer"
"user.department !IN! Transportation|Tours", "user.location ==
ReviewItem.user.supervisor.location"
"user.department !NULL!", "user.uniqueUserId !IN!
ReviewItem.application.applicationOwners.owner.uniqueUserId"
```

In this example, the header cells use only keywords, and the first criteria row uses relationships to assign a reviewer. Note that the `ReviewItem` is referenced within the `Reviewer` criteria cells. For users under review who are in the Transportation or Tours department, a reviewer is assigned based on the location of the supervisor.

The second criteria row specifies multiple reviewers based on the owners of the application under review if the department attribute is null.

Account Review Coverage Map Examples

Self and account owners as reviewers

```
"ReviewItem.account.relationToUserType","Reviewer.user.uniqueUserId"
"==SHARED","!IN!ReviewItem.account.accountOwners.owner.uniqueUserId
"==SINGULAR","!IN!ReviewItem.account.accountHolders.holder.uniqueUserId"
```

In this example, the header cells use keywords and the criteria cells uses relationships to specify that all shared accounts are reviewed by the account owner, and single assigned accounts are reviewed by the holder of the account (self).

Supervisors as reviewers

```
"ReviewItem.account.relationToUserType","Reviewer.user.uniqueUserId"
"==SHARED",
"!IN!ReviewItem.account.accountOwners.owner.supervisorUniqueId"
"==SINGULAR","!IN!ReviewItem.account.accountHolders.holder.supervisorUniqu
eId"
```

In this example, the supervisor of the account owner is specified as the reviewer for all shared accounts and the supervisor of the holder of the account is specified as reviewer for single accounts.

Access Request Coverage Map Example

Policy owners as approvers

```
"Approver.user.uniqueUserId","Approver.group.uniqueGroupId","RequestItem"
"!IN! RequestItem.role_policy.policyOwners.owner.uniqueUserId","!IN!
RequestItem.role_policy.policyOwners.groupOwner.uniqueGroupId","role_polic
y.risk > 30"
```

In this example, for access requests to technical roles, if risk is greater than 30, then the policy owner is assigned as the approver.

2.4.10 Loading a Coverage Map CSV File

To load a coverage map CSV File:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Policy** > **Coverage Maps**.
3. To load a new coverage map:
   - **3a** Click the load icon.
   - **3b** Select the coverage map type: **REVIEW** or **REQUEST**.
   - **3c** Type coverage map name and description.
   - **3d** Click the upload icon, and then browse for the coverage map CSV file.
   - **3e** Select **Save**.
4. Repeat the above steps to add additional coverage maps.

2.4.11 Editing a Coverage Map

Identity Governance allows you to edit your coverage maps as needed.

To edit a coverage map:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Policy** > **Coverage Maps**.
3. Click the name of the coverage map you want to edit.
4. Click **Edit**.

5 Make the desired changes.

6 Click **Save**.

2.4.12 Deleting a Coverage Map

You can delete coverage maps only if all the following conditions are met:

- Identity Governance purged all the associated review instances
- Authorized administrators either deleted and purged the mapped review definition or changed the mapping

To delete a single or multiple coverage maps:

1 Log in to Identity Governance as a Global Administrator.

2 Select **Policy** > **Coverage Maps**.

3 Click on the review definition column and view associated review instances.

4 Click the name of the coverage map that meets the conditions for deletion outlined above.

5 Click **Edit**.

6 Click the delete icon.

7 To delete multiple coverage maps:

7a Repeat Step 3 on page 38 for each coverage map that you want to delete.

7b Select the coverage maps that meet the conditions outlined above.

7c Click **Actions** > **Delete Coverage Map**.

3 Creating and Managing Delegation

Delegation enables a more consistent workflow for managing the reassignment of user tasks by allowing users and administrators to assign delegates for request and approval tasks.

3.1 Understanding Delegation

Authorized users can delegate their review and approval tasks. The Customer, Global, or Data Administrator can assign delegates for all users. The delegate then receives tasks and acts on them instead of the original assignee. If the original assignee acts in one of the review or access approval management roles, the delegate also has the proper access permissions to act in that role. For example, if the original assignee was review owner, review auditor, or access request approver, the delegate will also have the related access permissions.

Delegation is a one-to-one mapping between two active users in the catalog. While a user can have only one delegate at any given time, a user can act as delegate for multiple users. Delegate chains are allowed. For example, User A can have a delegate User B, User B can have a delegate User C. However, a cyclical chain, where User A’s delegate is User B, and User B’s delegate is User A, is not allowed and will cause the review startup to fail.

When a review is started, Identity Governance calculates reviewers by the active delegate mappings that exist at the start of the review. If a delegate exists for an original assignee, the delegate for all intents and purposes is now considered the reviewer. To prevent review startup failure related to a cyclical chain, administrators can use the **Validate delegate mapping** bulk action after mapping delegates. The only other times Identity Governance calculates delegates are when review items are escalated, and when a reviewer is reassigned using the **Change Reviewer** option. When using the **Change Reviewer** option during reviews, the option becomes inactive when a cyclical chain is detected. After a delegate reviews or approves an item, and after running an Insight Query, the delegate and their relationship to the user appears in the results list. For example, “Approved by User B (delegate for User A, the delegate will show up under 'Delegated From' column).

A delegation continues until it is terminated, a different user is assigned, or when the current date is not in the specified date range. When a delegation is terminated or modified, all future tasks are reassigned to the original assignee or the new delegate. If the delegation is terminated or modified when a review is in progress, outstanding tasks are not impacted. For purposes of historical audit, reviewer information and task activity in preview or live review tabs indicate that the task was assigned to a delegate in place of the original assignee.

3.2 Assigning and Managing Delegates for Yourself

1. Log in to Identity Governance.
2. In the title bar, select ***Your User Name*** > **My Settings**.
3. Expand the **Delegate Mapping** menu and click **Assign Delegate**.
4. Specify a delegate and select an assignment type.
5. (Optional) Select a reason and specify the start and end date of delegation.
6. Activate the delegate mapping.
7. Click **Save**. Identity Governance automatically checks your mapping and adds a green check mark icon in the Status column to indicate that your mapping is valid.
8. (Conditional) If you see a red error icon in the Status column, edit the mapping and fix the invalid mapping.

   NOTE: If you see a gray warning icon, no action is needed. The gray warning icon indicates that the current date is not in the date range you specified. The icon will automatically disappear when the data range becomes active.

   ---
9. (Optional) Repeat the above steps if you want to delegate a assignment type (for example, Request Approvals) to another user.
10. (Optional) Select **Edit** to modify the delegate, reason, effective dates, or status.
11. (Optional) Select **Delete** to terminate a delegation.

3.3 Assigning and Managing Delegation for All Users

1. Log in as a Global or Data Administrator.
2. Under **Policy**, select **Delegation**.
3. Click **+** to add a delegate.
4. Search and select a user, assign a delegate, and select an assignment type.
5. (Optional) Add a reason, specify the start and end date of delegation, and activate the delegation.
6. Click **Save**.
7. Repeat the above steps to add delegates for other users.
8. Select rows and then select **Actions > Validate delegate mappings** to ensure delegate mappings, if chained, are chained appropriately. Fix invalid mappings, if any.
9. (Optional) Select **Edit** to change a user, delegate, reason, or status.
10. (Optional) Select **Delete** to terminate a delegation.
11. (Optional) Select rows and then select **Actions > Activate** or **Actions > Deactivate** to change the status of multiple delegations.

NOTE: Review owners and review administrators can bypass delegation for the review management roles (review owner, escalation reviewer, and auditor) by editing the running review instance. These changes are made only for the running review instance. Delegates can also assign another user as a reviewer by using the **Change Reviewer** option on the review tabs. Request approvers can also bypass delegation for the approver role by reassigning approvers on the Approval page.

3.4 Exporting and Importing Delegation Mappings

Authorized users have the ability to export all or selected mappings to a zip file and import them to a different Identity Governance environment. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

4 Customizing and Configuring Identity Governance for Your Enterprise

You can customize the displayed names of attributes and risk levels in the Identity Governance interface. You can also customize the content in the templates for the email notifications.

4.1 Enabling and Disabling Auditing Events

A Global Administrator can select **Configuration > Audit Enablement** to enable and disable specified audit events for specified packages and event IDs.

When a Global Administrator enables auditing, Identity Governance can send audit event information to any combination of the following:

- An application server log
- A separate log file
- A syslog destination

Audit event logs allow you to provide evidence that you comply with regulations. The Global Administrator must first set the audit targets for selected modules, and then enable or disable audit event logging for specific packages or event IDs. Authorized administrators can also export and import audit settings.

NOTE: If you delete an audit log file while auditing is enabled and the server is running, a new audit log file will not automatically be generated. If you need to delete an audit log file while auditing is enabled, you must either first disable auditing and then enable it again, or you must restart the server.

You can also use the Configuration Utility to enable and disable auditing. For more information about the Configuration Utility, see “Using the Identity Governance Configuration Utility”in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

4.2 Managing Logging Levels

A Global Administrator can configure the logging levels for Identity Governance and the Identity Governance clients to provide a more granular view of the events occurring. Use the following information to enable or increase the logging levels for Identity Governance and Identity Governance clients.

4.2.1 Setting Logging Levels by Module and Package

Identity Governance allows Global Administrator to set logging levels for the packages in each available module and also import and export these settings. The product includes a short list of packages for each selected module to which an administrator can assign a logging level. They can also search for and add packages to each module, or delete packages from each module.

Identity Governance allows administrators to set the following logging levels for each package:

- Info
- Warning
- Error
- Fatal
- Debug
- Trace
- None

Identity Governance displays a list of packages associated with each module.

To set the logging level:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration > Logging Levels**.
3. From the drop-down list, select one of the following modules:
   - DaaS WAR
   - DTP WAR
   - Server WAR
   - RPT WAR
4. Specify the logging levels for the packages in the selected module.

   NOTE: You cannot change the logging levels for Client, CX, and Health modules using the user interface. To specify logging levels for these modules, you need to edit the respective xml files, then restart Tomcat. Contact your Technical Support team for more information about editing these files.
5. (Optional) Click the toggle to enable auditing for the packages in the selected package.
6. (Optional) Add an appender reference.
7. Next to each updated package, click **Save**.

8 (Optional) To add a logger package to a selected module:

8a Next to **Logging levels by module and package**, click the plus sign (+).

8b In the **Add New Logger** window, type the name of the package you want to add.

8c Select the logging level for the package you want to add.

8d (Optional) Click the plus sign (+) to select an appender reference for the package.

8e Click **Add**.

4.2.2 Setting the Exception Level

The exception level in Identity Governance specifies the level at which exception messages appear in the console. By default, the logging exception level is set to **Debug**. Global Administrators who want stack trace, should set the exception level to **Error**.

NOTE: The exception level applies to all modules and packages.

4.3 Changing Advanced Configuration Settings

After installing Identity Governance, you might need to change your default configuration settings under the guidance of support engineers. You can change the application configuration and enable features using the Identity Governance **Advanced** menu and configuration utilities.

WARNING: Changing advanced configuration settings can impact the performance, security, and overall function of Identity Governance. Some settings will require Tomcat Server restart. Consult Identity Governance support engineers for additional details.

To change configuration settings after installation using the Advanced menu:

1 Log in to Identity Governance as a Global Administrator.

2 Select **Configuration > Advanced**.

3 Search for a global configuration property key.

4 Click the edit icon to change the default value or to add a value.

5 Click the save icon.

6 (Conditional) Restart Tomcat Server. Consult support engineers about when you will need to do this.

7 (Optional) Click **+** to add a configuration property key and value.

For more information about the configuration utilities, see "Using the Identity Governance Configuration Utility" and "Using the Identity Governance Configuration Update Utility" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

4.4 Customizing Email Notification Templates

Identity Governance notifies users of tasks in their queue, as well as other review events, as specified in review definitions. Depending on your configuration, various events associated with functional areas, such as bulk data update, business role approval, request, review, Separation of Duties (SoD), and fulfillment, might trigger email notifications. For example, the Bulk Data Administrator can be notified when a bulk data template is generated and when a bulk data update occurs; and an SoD Policy Owner can be notified when a new SoD violation is detected after data source collection and publication. The application supplies default templates with preconfigured tokens for the email notifications and uses the templates as is unless you customize them for your environment.

Users must have a valid email in the Identity Governance catalog to receive notifications. If Self is specified as the recipient and a user affected by the policy has no email, the application will not send the notification to Customer, Global, or other authorized administrators. When an user has multiple email addresses in the catalog, Identity Governance will send notification to only one email address.

IMPORTANT: Make sure users have a valid email because tasks such as Data and Certification policy violation uses emails for remediations and review and request approval tasks are also communicated via emails.

TIP: When setting up and testing Identity Governance notifications or testing preview review notifications, make sure you are using a test email system or test email addresses. For example, use fake mail, mail catcher, or test corporate mail server. *Do not send emails to a live server while testing your system*. If you have real email accounts in your test system you can inadvertently send spam email to people in your company.

You can also customize the product name in email notifications to brand it for your organization. To change the product name, run the Identity Governance Configuration Utility in the console mode, and specify the product name you prefer on the **Identity Governance Server Details** tab. For more information, see "Using the Identity Governance Configuration Utility" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

For information about configuring Identity Governance to send email notifications, see "Enabling Email Notifications for Identity Governance" in the *Identity Governance 4.3.1 Installation and Configuration Guide*. For information about Review related notifications, see: Section 25.1.9, "Setting Review Notifications," on page 333.

4.4.1 Modifying Email Templates

Identity Governance allows you to modify an XML file that contains the email text in the languages supported for Identity Governance. You can edit the XML file with one of the following programs to customize it for your organization:

- XML editor

- Text editor
- Designer for NetIQ Identity Manager

To modify an email template content:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration > Notification Emails**.
3. Select a download option:
   - To customize all email templates in a single file, select **Download XML**. Depending on your browser settings, you might be prompted for the download path.

     NOTE: If prompted, do not rename the `EmailTemplates.xml` file. Identity Governance cannot upload a file that does not match the expected name.
   - To download the XML file for all the emails of a functional area in a single locale, select **Implemented Locale** from the **View functional area** drop-down list, then select the locale.
   - To download the XML file for a single email in all the implemented locales, select **Email** from the **View functional area** drop-down list, then click an email name.

     Optionally, select **Email source preview (en)** to view the template. Specify an email address to **Send notification preview**.

     Click **Download XML**.
4. Modify the content in the email templates you have downloaded.

   NOTE: Do not modify any text in the code strings in the file. Identity Governance might not function correctly if you change the code strings. For descriptions of the email tokens, see "Email Tokens" on page 47.
5. Save and close the files.
6. To submit the modified files, click **Import XML.**

Email Tokens

When customizing emails, be careful in handling the tokens. Identity Governance allows the use of entities and their attributes in your email templates. Entity tokens *must* appear in the `form:token-descriptions` section to be processed. If it only appears in the `<body/>` section of the template it will stay unresolved.

Some email templates expect only certain processing and entity tokens. Therefore, the product might not be able to replace a token with a value in some situations. For example, when an unexpected token is present in the template, a entity token is evaluated as `null` during notification preview, or an entity attribute was not collected and was resolved as `null`, the generated email might contain blank values or might contain token as-is. Notifications sent during review preview mode that enable administrators and review owners to preview notifications, might not always replace tokens with values, and names seen in the preview might not be the name that is sent in the live mode email.

The email templates use the following processing tokens:

Token	Notes
applicationId	Application ID, unused in the Certification External Provisioning Start Error template
applicationName	Application name
appName	Application name
approverName	Business role approver
certifierFullName	Reviewer's full name
certifyTaskLink	Link to task
changesetId	Unused in the Certification External Provisioning Start Error template
content	Used in the generic email template
curatorFullName	Bulk data feed curator
error	Fulfillment error
errorMessage	Error message text
externalPrdLink	Unused in the Certification External Provisioning Start Error template
feedName	Bulk data update definition
fulfillerName	Full name of the fulfiller
host	The workflow hostname
inputFile	Bulk data CSV file
link	URL link
message	The output message from a system process.
newTaskType	Used in the Certification Auto Provisioning Start Failed template
ownerName	Owner of the SoD policy
permissionsToLose	List of application permissions
prdName	Workflow name used in the external fulfillment template
prevReviewerFullName	User that the task was reassigned from
productName	Configured product name, such as Identity Governance or Access Review
reassignedByFullName	User who reassigned the task
reassignComment	Optional comment entered at reassignment
retryCount	Number of fulfillment items in a retry state
reviewLink	URL link to review
	NOTE: Do not use this token in notification emails to users, such as reviewers who have limited access to reviews. Instead use the certifyTaskLink token.

Token	Notes
reviewName	Name of the review
reviewOwner	Review owner’s name
reviewOwnerPhone	Review owner’s phone number
roles	List of business approval roles
subject	Found in Certification Started and Certification Changed email templates with no reference to the token in the templates.
taskTimeoutDays	Task timeout in days
theTerminator	The user that terminated a review
userFullName	Identity Governance user's full name
violations	Used in the Detected SoD Violation email template.

NOTE: Instances where there are multiple review owners, and the review uses any one of these listed templates:

- Certification Approval Task Pending Reminder
- Certification Approval Task Pending
- Certify Task Past Due
- Certify Task Pending Reminder
- Certify Task Pending
- Certify Task Reassignment

Identity Governance sends the email notification with the primary and the additional review owner’s phone numbers for the token $reviewOwnerPhone$ and their names for the token $reviewOwner$. If the $reviewOwnerPhone$ token is not present in the template, then Identity Governance lists the names of the review owners.

The email templates use the following entity and role-based tokens:

Entity Token	Entity Type	Notes
ADDRESSEE	USER	Primary (TO) address. Resolves to one of the following role: ◆ Review Owner ◆ Reviewer ◆ Auditor ◆ Escalation Reviewer
REVIEW	REVIEWINSTANCE	Review instance
REVIEWDEF	REVIEW_DEFINITION	Attributes for the review definition

Entity Token	Entity Type	Notes
REVIEWER	USER	Task owner of a current review instance. Used only in notifications to task owners.
PAST_REVIEWER	USER	Reviewer of the previous review instance. Used only in task reassignment notifications.

The following table shows the current attribute definitions for the review based entity types.

Entity Type	Attributes
REVIEWINSTANCE	◆ certificationDate ◆ endDate ◆ expectedEndDate ◆ startDate ◆ lastStatusChange ◆ validToDate ◆ taskCount ◆ taskCompleteCount ◆ itemCount ◆ itemCompleteCount ◆ itemApproveCount ◆ statusComment ◆ auditorComment ◆ startMessage ◆ approvedBy ◆ canceledBy ◆ approvedByPolicy ◆ status ◆ owners ◆ auditor

Entity Type	Attributes
REVIEW_DEFINITION	◆ name ◆ description ◆ activeFromDate ◆ activeToDate ◆ latestValidToDate ◆ startDate ◆ isActive ◆ duration ◆ escalationTimeout ◆ validFor ◆ repeat ◆ expirationExtension ◆ reviewType ◆ durationUnit ◆ escalationTimeoutUnit ◆ validForUnit ◆ repeatUnit ◆ expirationExtensionUnit ◆ owners ◆ auditor

4.4.2 Adding an Image to the Email Template

In addition to modifying an email template, you can also add an image or logo to the email template.

To add an image to the email template:

1. Select the image you want to add to the template and encode it in base64 string format.

   TIP: Use the base64encode website or similar encoders to encode the image.

2. Download the email template.
3. Add the `<img src=" %base64-value% "/>` tag where you want the image to appear. For example, `<p>Powered by <img src="..."/></p>`.
4. Upload the modified email template.

4.4.3 Deleting a Custom Email Template

When you no longer want to use a custom email template, you can delete the custom template by clicking the custom email template name on the Notification Emails page, then clicking **Delete**.

4.5 Customizing the Collector Templates for Data Sources

A collector template typically includes predefined attribute mappings and value transformation policies suitable for the target data source. To create a custom collector template, you can download and edit an existing template. Collector templates use JavaScript Object Notation (JSON) format to specify the collection behavior. You can use a JSON formatter or text editor to modify the content of the template file.

When you import a new or modified template for an application source, you must specify whether the template is designed for collecting accounts or permissions from the source. If a new or customized template replaces an existing template, you can disable the template that you no longer need.

1. Log in to Identity Governance as a Bootstrap, Global, or Data administrator.
2. Select **Configuration**.
3. Expand the **Identity Source Collector Templates**, **Application Source Collector Templates**, or **Application Definition Source Collector Templates** section.
4. (Conditional) To customize an existing template, complete the following steps:
   - **4a** Select the template that you want to customize.
   - **4b** Click **Download**.
   - **4c** Specify where you want to save the downloaded file.
   - **4d** Edit the template and save the JSON file.
5. (Conditional) To import a new or modified collector template, select **+** and then specify the template that you want to import.
6. (Conditional) To disable a template that you do not use or to enable an older template, complete the following steps:
   - **6a** Select the template that you want to disable or enable.
   - **6b** Select **Actions**.
   - **6c** **Disable** or **Enable**.

4.6 Creating and Assigning Categories

Identity Governance allows you to set up categories to organize applications, permissions, business roles, and technical roles. You can define these categories in Identity Governance and assign them to entities. You can also customize your categories and assignments offline and upload them in bulk, and you can export a JSON file, edit it, and import it. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

1. Log in to Identity Governance as a Global or Data Administrator.
2. Select **Configuration** > **Categories**.
3. To add new categories, select **+** and specify a name and description for the category.
4. Assign the category to entities:
   - **4a** Select **+** next to **Assign entities**.
   - **4b** Select the entity type and then select specific entities to assign the category to.

4c When you have selected all the entities, select **Add**. A tab for each entity type with list of entities is displayed.

4d Select and remove the category assignment, if needed.

NOTE: You can also assign categories to permissions, applications, or technical roles in the Catalog by editing an entity.

---

5 Select **Save** and then close the window.

4.7 Disabling Review Email Notifications

Identity Governance enables you to customize and set up various event notifications. Administrators can also disable notifications during access governance life cycle using the Identity Governance Configuration Utility.

To disable review email notifications:

1 Stop Tomcat. For examples, see "Starting and Stopping Apache Tomcat" in *Identity Governance 4.3.1 Installation and Configuration Guide*.

2 Launch the Identity Governance Configuration Utility in console mode. For more information, see "Using the Identity Governance Configuration Utility" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

3 Specify suppress commands for the emails you want to disable as shown in the following examples.

WARNING: Disabling review notifications is a global change and is applied to *all* reviews.

3a To stop review termination notifications being sent out to the Review Owner and Reviewers when a running Review is terminated type the Configuration Utility console mode command: `add-property GLOBAL com.netiq.iac.reviews.suppressReviewTerminationEmail true`.

3b To disable losing permission notification from being sent to the employee that is about to have a permission revoked type the Configuration Utility console mode command: `add-property com.netiq.iac.reviews.fulfillment.suppressLosingPermissionEmail true`.

4 Exit the console mode.

5 Delete the `localhost` folder from the `tomcat/work/Catalina` directory.

6 Start Tomcat. For examples, see "Starting and Stopping Apache Tomcat" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

4.8 Extending the Identity Governance Schema

Identity Governance contains a default schema for entities that you collect in the catalog. If the default schema provided does not meet your needs, you can extend the Identity Governance schema. Extending the schema is a simple process.

To extend the schema, add attributes to the default schema. You can view the default schema for Identity Governance in the console. Log in as a Global or Data administrator to view the schema, which is listed under the **Data Administration** menu.

4.8.1 Adding or Editing Attributes to Extend the Schema

Identity Governance provides a simple way to extend the schema for the different entities. You can add additional attributes and define properties. You can also download attributes as JSON files to edit the properties. After editing, you can import the attributes to the page that lists all attributes for a given entity.

1. Log in to Identity Governance as a Global or Data Administrator.
2. Under **Data Administration**, select the entity where you want to add or edit the attribute.
   - **Identity**
   - **Account**
   - **Permission**
   - **Business Roles**
   - **Application**

   NOTE: Identity Governance does not allow you to extend the schema for groups and permission assignments.

   ---

3. Select the plus sign **+** to add a new attribute or select an existing default or custom attribute to edit the properties.
4. Add or edit the attribute by configuring the following:

   NOTE: Some values might not be editable, depending on factors such as the Attribute Behavior settings and collection status.

   Attribute name and Key

   Specify the attribute name and key. Use the same value for both fields. The attribute name must be unique to your Identity Governance environment.

   Data Type

   Select the type of attribute you want to create. Attribute data types are **String**, **Boolean**, **Double**, **Long**, **Date**, and **Locale**. Attribute data types cannot be edited after collection.

IMPORTANT: Boolean and Locale type attributes do not support multiple values. Do not change these data types to another data type after saving the attribute. If you do, the attribute might still display that multiple values are not allowed. We recommend that you delete the custom attribute and recreate it when you need to change an attribute data type from Boolean and Locale to another data type.

Maximum size

Specify the number of characters allowed for the value of this attribute.

Truncate to size

Enable to allow the system to handle values longer than the attribute's maximum size. If you do not enable this option, and the value is longer than the maximum size, an error will occur and the record is not collected.

Attribute Behavior

Select the behavior of the attribute. The attribute can be required, allowed to change, allowed to have multiple values, or allowed to have a static value. Static values enclosed in double quotes allow you to provide the same attribute value for all collected objects. For example, to set the same values of `cost = 10`, `type = regular`, and `privileged = false` for all collected Accounts, configure the account collector with the static values in double quotes for these attributes. This is a great way to set a default value that you can override using collector transforms or by editing the attributes as needed after collection.

Listable Options

Select how you want the attribute displayed in Identity Governance.

Display in Quick Info views

Allows anyone with rights to view reviews to see the attribute. This option does not allow the attribute to be changed.

Display in lists and detail views

Allows administrators to view and change the information in the Identity Governance console.

Sortable in table columns

Allows administrators to store the attribute in the table columns.

Allow to be reviewed

Allows administrators to specify which attributes to review when creating User Profile Review definition.

Searchable Options

Select how you want the new attribute to be searched for in Identity Governance.

- Available in catalog searches. Changes take effect after publication.
- Display as refine search option.
- Display in review item selection criteria.
- Display in business role selection criteria.

IMPORTANT: For all attributes that you have configured for authentication matching rules using the Identity Governance Configuration Utility, ensure that you enable the following list and search options for identity attributes:

- Display in lists and detail views.
- Available in catalog searches. Changes take effect after publication.

5 Select **Save**.

4.8.2 Adding Attributes to a Collector

If a collector you use does not contain the schema you need, you can add attributes to extend the schema of the collector. You must have already created and configured the collector before performing the following steps.

1 Log in to Identity Governance as a Global Administrator.
2 Select **Data Sources**.
3 Select **Identities**, **Applications,** or **Application Definitions**.
4 Select ***Your Data Source***.
5 In the collector page, select the collector name to view details.
6 Based on your collector, select **Collect Identity**, **Collect Permission**, or **Collect Application**.
7 Scroll down the list of parameters and click **Add attribute**.
8 Configure parameters to define the attribute.
9 Select **Save**.

4.8.3 Viewing Available Attributes in Business Roles

When you create a business role, you define a membership expression that searches for all users who meet a certain criteria to be added to the business role. For more information, see Section 19.2, “Creating and Defining Business Roles,” on page 236.

The **Membership expression** lists all of the available attributes you can match under the **Title** field. This list matches the list displayed under **Data Administration** > **Business Roles**. If you want to add more items to this list, you must add a new attribute to the business roles schema.

NOTE: Only Bootstrap, Customer, Global, Data or Business Role Administrators have rights to administer the business role schema. For more information, see Section 4.8.1, “Adding or Editing Attributes to Extend the Schema,” on page 54.

4.9 Customizing Download Settings

Identity Governance enables you to export and download data related to various functional areas as ZIP files. Based on your authorization, you can download items such as data sources, review, role, and policy definitions, reviewer, review item, and business roles lists, and technical and business roles. The download is performed asynchronously, and users can continue to work on the page or

switch to a different page and not affect the download process. You can also export and import your download settings. For more information about exporting and importing and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

TIP: For description of the internal ENUM values from the database that might appear in the downloaded files, see the *Identity Governance ENUM Values Technical Reference (https://wwwtest.microfocus.com/documentation/identity-governance/4.3/tech-refs/IDGov_ENUMS_Technical_Reference.pdf)*.

All your downloads are staged to a designated download area. When you download an item from the Identity Governance download area, the file is stored on your local hard drive. The file on your local hard drive is basically a copy of the data that is stored in the database. The data in the database is retained for the interval specified in the **Configuration > Download Settings** menu. Use the download icon on the Identity Governance title bar to download files and also manually delete data from the download area in the database before the end of the retention interval.

Use the **Configuration > Download Settings** menu to view the default download settings and optionally customize:

- Attributes used to *uniquely* identify Identity Governance users, groups, permissions, or accounts when references to these entities are exported with other entities or definitions such as review definitions, request policies, SoD policies, and roles.

  NOTE: You should select an attribute that appears in the type ahead list, is enabled as **Available in catalog searches** in the **Data Administration > *Entity* Attributes > *Attribute*** definition page, and has unique relationship with the entity. Additional attributes might exist in the system but they cannot be used as uniqueness attribute. For example, you can select attributes such as Permission ID Digest which has a 1-1 relationship with permission. However, attributes such as titles, job codes, or departments would not be good candidates since they do not uniquely identify the entity.

- Number of hours to retain downloads before they are deleted from the download area in the database (**Download retention period**)
- Delimiter used to separate multi-valued attributes in the CSV (**CSV Multi-value Delimiter**)

4.10 Customizing Access Request Landing Page

The default Access Request landing page is Current Access page. To change the default landing page, use the following steps:

1. Log in to Identity Governance as a Global Administrator.
2. From the Identity Governance home page, click **Configuration** > **General Settings**.
3. Under **General Settings**, select the desired landing page for **Access Request landing page**.
4. Click **Save**.

5 Using Advanced Filters for Searches

If you have a large data set, a simple search could return a list of results too large to be helpful or relevant to your needs. Many Identity Governance search fields include an advanced filter option that allows you to create search filters that include one or more conditions and subconditions.

5.1 Using the Expression Builder to Create Advanced Filters

The filter icon, where available for searches, appears to the right of the search field. Click the filter icon to activate an expression builder, which lets you create advanced filters by selecting and combining search attributes, operators and expressions, values, and filters that Identity Governance uses to create a focused list of search results.

5.1.1 Choosing Search Attributes

The search attributes available from the drop-down list varies across searches, depending on the data columns available to select for display in the results list. For example, if you want to create a search for specific Business Role approval policies, you can choose from the following search attributes:

- Name
- Changed By
- Created By
- Description
- Name
- Type

5.1.2 Using Operators, Conditions, and Filters

Advanced search filters use the **operators** AND, OR, and NOT to create expressions that direct the search to include, respectively, ALL of the conditions you define, ANY of the conditions you define, or NONE of the conditions you define in the search filter. Select one of these operators to start building a filter. The operator you select applies to every condition you create.

Conditions allow you to specify search attributes including dates and use additional operators, such as “equal to,” “not equal to,” “equals one of,” “does not equal any of,” “greater than,” “less than,” “greater than or equal to,” “subset of,” “superset of,” “intersects,” and “same as” to define how or if the search item appears as a result of the condition.

Filters are subconditions that allow you to fine-tune a condition by further filtering results using additional AND, OR, and NOT statements.

NOTE: When you use “Not equal to” as a condition, the search function will not evaluate identities with a null value. For example, the condition "is not equal to manager" will result in all Identities that has a title that does not equal manager. It will not include identities that have no value for title. To include null values the advanced search would also need to include the condition “title is empty”: User: Title not equal to manager or User: Title is empty. Also, when using Boolean attributes, you need to account for null values. Follow database search best practices when using advanced searches.

5.2 Creating and Saving an Advanced Filter — Example

Filters can be as simple or complex as needed. For example, the procedure below creates a simple filter that narrows the list of Business Role approval policies by searching for and listing:

- All the Business Roles approval policies that include the word “Approval,” and
- Were created by either of two specific people in your organization, but
- Are not the policy named “Default approval policy.”

To create a search filter for the example:

1. Click **Policy** > **Business Roles**.
2. Click the **Approval Policies** tab, then click **Approval Policies**.
3. Click the Filter icon to the right of the search field, then select **New Filter**.
4. Create a condition with the following options:
   - **4a** Select **ALL of the following (AND)** as the operator.
   - **4b** Select **Name** and **Contains**, then type `Approval` in the catalog attribute field.
   - **4c** Click **Filter**, to use the OR operator and add a subcondition to narrow results to two specific people.
   - **4d** Click **Condition** at the root layer of the expression and select **Name**, **not equal to**, then type `Default approval policy` in the catalog attribute field.
5. To apply the advanced search filter, click **Apply**.

NOTE: Some advanced filters allow you to save the filter for future use. If the save option is available, type the filter name, then click **Save**.

5.3 Using and Managing Saved Filters

When you save an advanced filter, it becomes available for use when you click the filter icon, along with options to manage saved filters and to create a new filter.

5.3.1 Using a Saved Filter

To use a saved filter:

1. Click the Filter icon, then select the filter you want to use.
2. (Optional) Make changes to the filter.
3. Click **Apply**.

5.3.2 Managing Existing Filters

Identity Governance provides a Manage Filters window, which looks like the expression builder to make changes to or delete your saved filters.

To edit a saved filter:

1. Click the Filter icon, then select **Manage saved filters**.
2. In the Manage Filters window, click **Filter**, then select the filter you want to edit.
3. Make the desired changes to the saved filter.
4. Click **Save**.

TIP: If you want to create a new saved filter from an existing filter, you can change the name of the saved filter as part of your edits.

To delete a saved filter:

1. Click the Filter icon, then select **Manage saved filters**.
2. In the Manage Filters window, click **Filter**, then select the filter you want to delete.
3. Click the Delete icon.

6 Understanding Data Administration

After installing Identity Governance, the bootstrap administrator collects and publishes an initial set of identities and provides global authorization to one of these users. Alternately, the bootstrap administrator can also have the global authorization. The Customer Administrator or Global Administrator assigns users other authorizations such as the data administration authorization.

As a Data Administrator, you are responsible for the entire data administration process including the key phases of data preparation, collection, publication, and management. Data collection and publication is the first critical step in the governance process, and it is an ongoing process that is needed to ensure that the access information that is being reviewed is up to date.

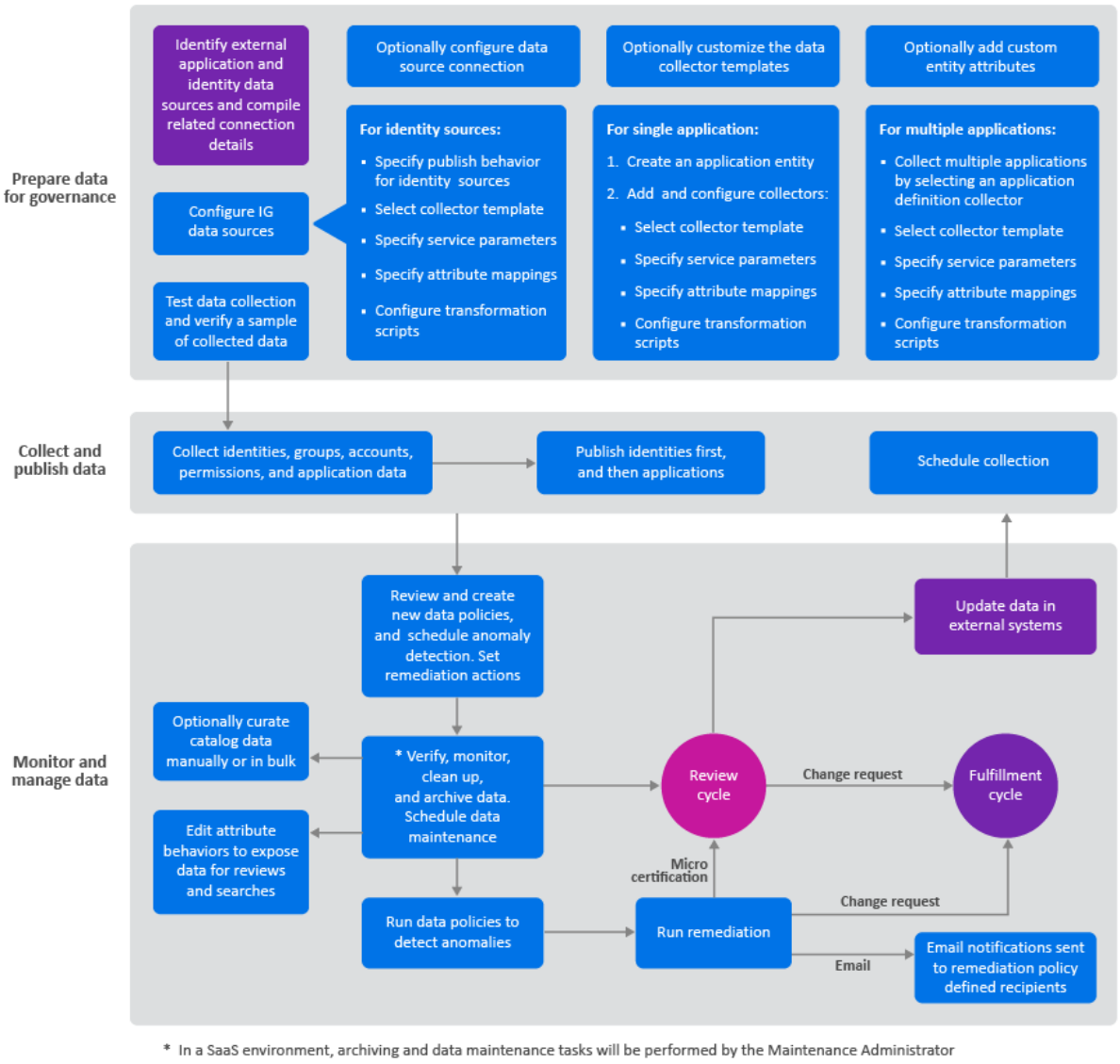
Identity Governance processes require clean, up-to-date data obtained from a variety of sources such as Identity Manager, Active Directory, and other enterprise applications in the data center and the cloud. Identity Governance can obtain the data by directly connecting to the systems through protocols such as LDAP, SCIM, and JDBC, or it can simply periodically extract the data from a file such as a Comma Separated Value (CSV) formatted file. The features and processes Identity Governance uses to retrieve, validate, and format entity (Identity, Group, Application, Account, and Permission) data from desired data sources is referred to as **data collection** and the collection templates you use to collect data are referred to as **collectors**.

Data Publication refers to the processes used to transfer the collected data to the Identity Governance **catalog** which makes the data available for governance operations.

Identity Governance provides default collector templates to get you started with the configuration process for data collection. However, each environment has custom requirements that might require unique transformation and configuration options.

As a Data Administrator, you need a thorough understanding of the sources from which the data is retrieved, as well as the Identity Governance data administration concepts and tasks. The following figure provides a brief overview of the data administration process.

Figure 6-1 *Data Administration Process Overview*



For additional information about the data collection and publication concepts and an overview of related tasks, see the following sections:

- Section 6.1, “Checklist for Collecting, Publishing, and Managing Data,” on page 65
- Section 6.2, “Understanding Collection and Publication Configuration Utility Settings,” on page 66
- Section 6.3, “Creating an Integration Account,” on page 67
- Section 6.4, “Understanding Notifications,” on page 67
- Section 6.5, “Understanding the Identity Governance Catalog,” on page 67
- Section 6.6, “Understanding Data Sources,” on page 69
- Section 6.7, “Understanding Cloud Bridge,” on page 70
- Section 6.8, “Collecting Data Using Cloud Bridge,” on page 70
- Section 6.9, “Understanding Collectors,” on page 72

6.1 Checklist for Collecting, Publishing, and Managing Data

	Checklist Items
❑	1. Ensure that you understand your data sources and Identity Governance concepts and processes. In addition, we recommend that you create an integration account.
❑	2. Identify external data sources from which data must be imported into the Identity Governance catalog and determine which entity data you want to retrieve.
❑	3. Compile information needed to collect data from each source such as server DNS name or IP address, server connection ports, administrative account user name and password, and the type of data you want to collect. **NOTE:** You can use the default collector templates as a guide for the type of information you need to gather.
❑	4. Select data sources and appropriate collector templates.
❑	5. (Optional) If the Identity Governance default templates do not meet your needs, download and customize collector templates. For more information, see Section 4.5, “Customizing the Collector Templates for Data Sources,” on page 52.
	6. (Optional) If the Identity Governance schema does not meet your needs, create custom attributes as needed to map entities. For more information, see Section 4.8.1, “Adding or Editing Attributes to Extend the Schema,” on page 54.
❑	7. Configure collector options for your data source. For more information, see Chapter 7, “Collecting Identities,” on page 83 and Chapter 8, “Collecting Applications and Application Data,” on page 95.
❑	8. (Conditional) If your data is not in the correct format, configure transformation scripts. For more information, see Section 6.9.2, “Transforming Data During Collection,” on page 75.
❑	9. Test the data collection and preview the raw or transformed data. For more information, see Section 6.9.3, “Testing Collections,” on page 76.
❑	10. Collect data.
❑	11. Publish data. For more information, see Chapter 9, “Publishing the Collected Data,” on page 105.

	Checklist Items
❑	12. (Optional) Schedule collection and publication. For more information, see Chapter 10, “Creating and Monitoring Scheduled Collections,” on page 109.
❑	13. Create and run data policies to compare collection metrics, validate data, and detect anomalies. For more information, see Section 11.3, “Creating and Editing Data Policies,” on page 115 and Section 11.6, “Comparing Collections and Publications,” on page 118.
❑	14. Run remediation to resolve anomalies. For more information, see Section 11.8, “Detecting and Remediating Violations in Published Data,” on page 119.
❑	15. (Optional) Run Insight Queries to examine your data. For more information, see Section 12.5, “Analyzing Data with Insight Queries,” on page 134.
❑	16. (Optional) Edit (curate) data manually and in bulk. For more information, see Section 12.3, “Editing Attribute Values of Objects in the Catalog,” on page 127.
❑	17. (Optional) Create custom metrics for data analysis. For more information, see Section 31.4, “Creating Custom Metrics,” on page 377.
❑	18. Plan and execute data maintenance activities such as archive and cleanup. For more information, seeSection 6.11, “Understanding Data Cleanup and Archiving,” on page 80 and Chapter 13, “Database Maintenance,” on page 137.

6.2 Understanding Collection and Publication Configuration Utility Settings

The following settings in the Identity Governance Configuration Utility allow you to control the collection and publication of the data sources. For information about the Configuration Utility, see “Using the Identity Governance Configuration Utility” in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

6.2.1 Collection and Publication Batch Sizes

These settings allow an administrator to tune the size of the record chunks that Identity Governance uses for the data collection and publication operations to achieve optimal performance in each environment.

6.2.2 Collection and Publication Settings

Do not clear **Clean DAAS Configuration post collection**. The **Max supported Depth of permission relations** field prevents loops of relationship mappings in deeply nested permissions environments. The default setting should be best for most environments.

6.3 Creating an Integration Account

Connectors are components that can connect to external systems and collect (pull) data from and fulfill (push) data to that system. Businesses can authorize administrators to perform integration activities. However, we strongly recommend that you create a dedicated account for the integration activities performed by the Identity Governance connectors (collectors and fulfillers) for collection or fulfillment. This would ensure that integration authorization is not associated with a specific user but associated with an account for business continuity and auditing purposes.

Based on the desired integration, specific capabilities for the integration account user might be required. For guidance related to procedures for creating the integration account, refer to the documentation of your systems that you want to integrate with Identity Governance. For example, you can refer to the Salesforce knowledge article to create an integration account for Salesforce. For a Workday integration account, refer to your Workday documentation (https://doc.workday.com/).

6.4 Understanding Notifications

Identity Governance notifies users when a collection or publication of identities or application fails or is canceled. Identity Governance sends email notifications to groups and individual owners. If an application has an owner, Identity Governance sends the email notifications to the Application Owner. Otherwise, Identity Governance sends the email notifications to the Data Administrator. The Data Administrator also receives all notifications related to identity sources. In the absence of an Application Owner or a Data Administrator, Identity Governance sends the notifications to a Global or Customer Administrator.

Email notifications include a link that enables recipients to navigate back to the identity or application source page where they can view additional details regarding the failure or cancellation. For information on customizing email notification, see Section 4.4, “Customizing Email Notification Templates,” on page 46.

6.5 Understanding the Identity Governance Catalog

The Identity Governance **catalog** is the repository of all collected data. The catalog reflects the current state of the operations database. It includes information about the following entities:

- **Identities**

  Identities, also referred to as Users, represent the people who are at the core of the processes within Identity Governance. They are the *who* in the review process of “*who* has access to *what*.” Identities also represent the people who manage and perform the reviews, or who serve as the administrators of Identity Governance.

  Identities are the first part of the catalog. Identity Governance can collect, correlate, and publish the identities. Plus, if you integrate with Identity Manager, you can leverage all the capabilities of Identity Manager to provide a synchronized, composite view of the people or things in your organization from multiple changing systems of record. Identity Governance can collect identities from multiple sources but it logically publishes the identities to a single name space in the catalog.

Identity Governance maps the identity and entitlement data to a minimum standard schema. The schema can be extended to include custom attributes to match the shape of your identity and entitlement data.

- **Groups**

  Groups, also referred to as User Groups or Identity Groups, are comprised of collected identities and are a useful entity for assigning administrative roles or reviews to a set of people without incurring the administrative overhead of direct assignment.

- **Applications**

  Applications in Identity Governance are the source of information about accounts and permissions. Identity Governance provides application definition templates to collect applications.Also, the Identity Manager Advanced Edition Permission collector gathers entitlement-enabled Identity Manager driver objects as applications.

  Applications have their own namespaces. Identity Governance can collect and publish the application data (accounts and permissions) per application in parallel. Identity Governance uses the latest published identities in the catalog to map who has what access to permissions in each application when it is published.

- **Accounts**

  Accounts generally represent entities that provide access to applications. If you log in to Netflix, you are using an account. If you log in to Gmail, you are using an account. Accounts are *not* identities. They are the representation of system, application, or data source accessed *by* an identity. Accounts often specify the type of permissions granted to a user.

  In some scenarios, such as system or administrative accounts which are not linked to identities custodians are assigned. You can collect this data directly from the application source, then map and join it to identities while configuring the account collector. If you cannot collect the data, Identity Governance allows you to edit the account and assign one or more custodians from the identities available in the catalog.

- **Permissions**

  Permissions, from an Identity Governance perspective, have multiple facets. Permissions can describe any of the following:

  - Actions that you can take within an application

    For example, finance department employees have access to the SAP Finance application (accounts). One employee has the rights granted to run Accounts Payable functions; another employee has the rights granted to run the Accounts Receivable functions. Both have accounts, but different permissions within the same application. This is a case where the Permissions (Accounts Receivable, Accounts Payable) are granted to the application user (account).

  - Items that you possess to access things

    For example, all employees have an electronic badge that allows them access to their office building. These employees do not have an account on the Building Access application to which they must log in, They simply have the access granted to their person via the badge. This is a case where the Permission (badge) is granted directly to the Identity (person).

  Permissions can be inherited in the case of hierarchical relationships. For example, for parent-child hierarchy permissions, when a user has an assignment for a child permission, they may also optionally be given an assignment for the parent permission. In such scenarios, the Assignment Type becomes INHERITED for the parent permission. Note that the Assignment Type can be INHERITED as well as DIRECT for the parent permission if the option **Nested**

members in membership query is configured in eDirectory. For more information see, Nested Group (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/fbabihje.html#b7lygte) in the NetIQ eDirectory Administration Guide (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

You can view details of all permission assignments in the Identity Governance Catalog by clicking the **Assignment details** link on the **Accounts** and **Permissions** tab. The assignment details indicate how it was assigned, such as direct or inherited, if the assignment can be revoked or not, the assignment start and end time, or the assignment value.

- **Roles (Technical Roles)**

  Technical roles allow business owners to simplify the review process by grouping permissions, and reduces the number of items for business leaders to review. For example, a role called *Sales Employee* might have permissions associated with sales software applications and financial data and one or more permissions that apply to all employees, such as *Garage Access*, *Building Access*, and *Read Access to Company Intranet*.

  Technical roles can be detected if the user has all the permissions defined by the role. Technical roles can also be directly assigned to users and groups. Identity Governance does not collect technical roles.

NOTE: Technical roles can be authorized by business roles. Business roles are higher-level roles focused around common access requirements for business role members. For example, a manager in the Sales Department might need all the permissions associated with a *Sales Employee* technical role, and need access to the management resources. Identity Governance provides details of business role associated with identities, applications, permissions, and technical roles as separate tabs in the catalog view.

6.6 Understanding Data Sources

To certify that your users have the appropriate levels of access to resources and applications, you need to populate the Identity Governance catalog with the identities, applications, application accounts, and application permissions that exist in your environment.

Data sources are data repositories located on-premises or on the cloud from which Identity Governance collects data using collector templates. Identity Governance uses these sources to collect and merge data from a variety of sources and adds them to the catalog to facilitate governance operations.

Identity Governance supports the following types of data sources:

- **Identity data sources** to collect, merge, and publish identities and groups.
- **Application data sources** to collect and publish accounts and permissions from a single application source using one or more collector templates.
- **Application definition sources** to collect application entities. Application definition data sources collect application records, but do not collect application data such as accounts and permissions. When you publish an application definition data source, the associated applications appear in the catalog. The application definition data source itself does not appear in the catalog. To collect and publish the associated applications' data (accounts and permissions), you will need to configure collectors on the application source.

Before collecting from the data source, you might need to prepare your data. If a date attribute in your data source uses a non-Java format, Identity Governance does not recognize the data as a date. For example, if the StartDate attribute uses "YYYY/MM/DD" fixed-length format and you want to collect it in date format, the collection will show an error. Identity Governance uses only the default format for Oracle Java for date attributes. In this scenario, you might "clean" the data by converting the attribute values to Java's default date format, which uses the number of milliseconds that have elapsed since midnight, January 1, 1970. Alternately, you could collect the date value in string format so that you will be able to see the native value. This method also guarantees that the data does not have to be "clean" to be collected.

6.7 Understanding Cloud Bridge

NOTE: Micro Focus supports Cloud Bridge only in Identity Governance as a Service deployments.

In Identity Governance as a Service environments, **Cloud Bridge** is a data transfer bridge between Identity Governance in the cloud and data sources in on-premises environments. The **Cloud Bridge agent** (CBA) is the entity that responds to the Identity Governance collection and fulfillment commands and directs them to the proper data source for execution. In the SaaS environment, the configuration and persistence of service-parameters identified as credentials are performed in the Cloud Bridge agent. For a high-level overview of your SaaS environment with Cloud Bridge, see the *Identity Governance as a Service Quick Start*.

The Cloud Bridge Data Center are configured as part of your Identity Governance tenancy based on the information you provide in the technical questionnaire. **Data Centers** are conceptual representation of your CBA instance. Install the Cloud Bridge agents on your local systems, and then configure Identity Governance Data Source Connections and Data Sources as needed to connect to your on-premises data sources. If you need to collect data from multiple data centers, you will need to install a Cloud Bridge agent in each on-premises data center.

Before enabling Cloud Bridge agent to collect data from on-premises data centers, authorized administrators will need to install Cloud Bridge, add credentials, and configure the data source connections. For more information about Cloud Bridge agent installation and configuration procedures, see the *NetIQ Cloud Bridge Agent Installation and Administration Guide (https://www.microfocus.com/documentation/identity-and-access-management/iam-services/cloud-bridge-agent-admin/bookinfo.html)*.

For information about procedures related to configuring data source connections and enabling the connection in Identity Governance, see Section 6.8, "Collecting Data Using Cloud Bridge," on page 70.

6.8 Collecting Data Using Cloud Bridge

After configuring data source connections, Customer or Data administrators must enable the connection to collect data using the Cloud Bridge.

NOTE: Micro Focus supports Cloud Bridge only in Identity Governance as a Service deployments.

6.8.1 Configuring Cloud Bridge Data Source Connections

NOTE: Micro Focus supports Cloud Bridge only in Identity Governance as a Service deployments.

1. Log in as a Customer or Data Administrator.
2. Click **Data Sources > Data Centers**.
3. Synchronize data centers to view previously configured data centers.

   For successful synchronization, make sure the cloud bridge agent is configured correctly and running.
4. Test connection to verify settings.
5. Create data source connections:
   - **5a** Select **Data Sources > Data Source Connections**.
   - **5b** Click **+**.
   - **5c** Add a name and description.
   - **5d** Use the **Data Centers** drop down to select the data center in which the Data Source Connection resides.
   - **5e** Save the data source connection. Note that each data source connection has a unique ID.
   - **5f** Copy the unique ID.

   or
6. Click **Import Data Source Connections**.
   - **6a** Select the JSON file to import.
   - **6b** Specify the data center.
   - **6c** **Import**.

   NOTE: You can import and export multiple data source connections. You can import new or overwrite existing data source connections, but for new connections you must specify a data center. When you select **Export Data Source Connections**, Identity Governance exports the data centers as part of the export file. Identity Governance also exports the data centers and data source connections when you export the identity or application data sources.
7. Create credentials for the data source connection in Cloud Bridge. For information about adding credentials, see“Adding Credentials for the Data Source Connection”section in the *NetIQ Cloud Bridge Agent Installation and Administration Guide (https://www.microfocus.com/documentation/identity-and-access-management/iam-services/cloud-bridge-agent-admin/bookinfo.html)*.

   For information about adding credentials for specific collectors or fulfillers, see Chapter 17, “Understanding Variations in Collector and Fulfillment Target Configurations,” on page 183.

6.8.2 Enabling Cloud Bridge Connection

NOTE: Micro Focus supports Cloud Bridge only in Identity Governance as a Service deployments.

Customer or Data administrators must enable use of Cloud Bridge, specify a data source connection, and specify unique parameters when required to collect data from on-premises and Cloud data sources to the Identity Governance as a Service catalog and when fulfilling change requests.

NOTE: Ensure that you have configured your data source connection before enabling the cloud bridge connection in your collector or fulfillment target template.

To enable Cloud Bridge Data Source Connection:

1. Log in as a Customer or Data Administrator.
2. Click **Data Sources > Identities** or **Data Sources > Applications**.
3. Click + and select a collector template.
   - **3a** (Conditional) Click **Upgrade** if a higher version of the collector template is available.
4. Enable the Cloud Bridge connection and specify a data source connection. Note that the **User Name** and **Password** are no longer configurable except in collectors and fulfillment target templates such as SCIM and REST GitHub which can be authenticated with different authentication methods.
5. (Conditional) When using a template that allows authentication method configuration, specify the authentication method.
6. Click **Test Connection** to verify your settings and connection.
7. Specify other fields as required and save the template.

   For information about configuring specific collectors or fulfillers, see the Chapter 17, “Understanding Variations in Collector and Fulfillment Target Configurations,” on page 183.

6.9 Understanding Collectors

Identity Governance provides templates to simplify the collection of data. Collection templates or **collectors** are the default mappings of identity, account, or permission data from identity and application sources to the core Identity Governance schema. Your systems might use different terms for the same type of objects. Collectors enable you to map your system-specific objects from various sources to the Identity Governance objects in order to collect and publish them to the Identity Governance catalog.

Each collector has one or more views that allow you to:

- Specify which data you will collect from your identity or application source
- Describe how that data will be linked together in the catalog

The collector views describe the characteristics of the data source that you could collect. The views are different for identity and application sources. For example, the JDBC Identity (Oracle) collector template can collect data for users, groups, group-to-group associations, and group-to-user associations. Collectors for application sources gather either account or permission data.

For each collector, you can collect data from on-premises data centers by enabling Cloud Bridge connection.

- Section 6.9.1, “Understanding Collector Configuration,” on page 73
- Section 6.9.2, “Transforming Data During Collection,” on page 75

6.9.1 Understanding Collector Configuration

Identity Governance provides a large set of collector templates that contain default data and configuration settings for many common enterprise and cloud data sources. Each template can be customized to connect to associated data sources.

NOTE: Customization of templates might require additional knowledge of connected systems, and all modifications are the responsibility of the customer. For further guidance, contact support or professional services.

Every collector has the following common elements:

Collector template

Collector templates include predefined attribute mappings and value transformation policies for specific data source types. Select a template that best suits the data source. For example, select **AD Identity** to collect identities from Active Directory. The templates support the following types of data sources:

- Active Directory
- Azure Active Directory
- CSV file
- eDirectory
- Google Apps
- Identity Manager AE
- IDM Entitlements
- JDBC, such as Oracle or PostgreSQL
- Resource Access Control Facility (RACF)
- Salesforce
- SAP HR

  NOTE: Identity Governance does not currently support SAP collectors in the SaaS environment.

- SAP User Management
- SCIM
- ServiceNow
- SharePoint
- Workday

NOTE: You can have one ore more templates for each data source. Template names indicate that they are permissions or accounts collectors. Template names that end in **with changes** can be enabled for processing incremental change events.

To see all the data source types, select **Collector Template** when you create the data source.

Service Parameters

These are the configurable parameters that allow the collector to connect and, if required, authenticate to the target data source. Depending on the connector, these service parameters can vary and might include, file locations, server host and port specifications, or service URLs. If you make changes to any service parameter that connects to the target data source, then Identity Governance will prompt you to re-enter the password.

After initial configuration, you must always update credentials and other service parameters in each template as needed. For example, when connecting to applications that use access tokens for authentication, such as SCIM-compatible applications, you must change the token when they expire and reconfigure the template to use the current access token.

This view also includes Cloud Bridge related parameters, authentication related parameters, and a **Test connection** button to verify the settings.

NOTE: Micro Focus supports Cloud Bridge only in Identity Governance as a Service deployments.

Cloud Bridge Connector The **Use Cloud Bridge connector?** option enables you to collect data from on-premises data centers when using Identity Governance as a Service. After enabling a Cloud Bridge connection, you must select the data source pertaining to your data center for credentials to be passed through automatically based on the data source unique ID.

NOTE: Once you enable a Cloud Bridge connection, typically you do not need to specify user name and password for the data host server as credentials will be passed through automatically based on your data source unique ID. However, for collectors such as the SCIM, Identity and Manager AE Permission collectors, you might need to specify ordinals for additional authentication methods. For more information about Cloud Bridge procedures for unique collectors, see Chapter 17, “Understanding Variations in Collector and Fulfillment Target Configurations,” on page 183. Always verify that you configure the service parameters correctly by testing the connection.

Collect Views

Each collector is comprised of one or more collector “views” that can be customized to match the characteristics of the data source being collected. These views enable you to map attributes and add transformation scripts. When collecting identities, they also enable you to select match rule when publishing and merging.

TIP: If you want to map attributes to static values, enclose the value within double quotes while configuring the collector templates. This applies the static value to each collected record.

For information about identity collect views, see Section 7.1, “Understanding Collector Templates for Identity Sources,” on page 83 and for information about application (account and permission) collect views, see Section 8.2, “Understanding Collectors for Application Data Sources,” on page 96.

Transformation Scripts View

This view in the collector template allows you to view transformation script usage information. For information about using transformation scripts, see Section 6.9.2, “Transforming Data During Collection,” on page 75.

Test Collection and Troubleshooting

This option allows you to preview data before running a full collection, preserve the configuration for a data source, or create an emulation package for a data source. You can use generated files to validate and troubleshoot collections, send results to support engineers, and to import data source configurations to a different environment.

For more information about test collections and troubleshooting, see Section 6.9.3, “Testing Collections,” on page 76 and Section 6.9.4, “Creating Emulation Packages,” on page 77.

For more information about configuring data source collector templates, see:

- Chapter 7, “Collecting Identities,” on page 83
- Chapter 8, “Collecting Applications and Application Data,” on page 95
- Chapter 17, “Understanding Variations in Collector and Fulfillment Target Configurations,” on page 183

6.9.2 Transforming Data During Collection

Because each application might have its own format for the data that you plan to collect, you might need to transform the data during the data collection process. For example, the application might store dates as a string (`20151202`) that needs to be converted to the Identity Governance date format, which is the Java Date format in milliseconds. Also, an application might use field lengths that do not match the field length in Identity Governance. These variations in collected data affect your ability to use the data or merge it with data collected from other sources.

Transformation scripts may be added to any mapped data field in any data collector by clicking on the ‘{}’ icon next to the field mapping. This will expand the dialog to allow you to either upload a transformation file or paste in transformation text. If required, you can also delete a transformation script after removing all references to the script from the attribute mapping(s) that use it.

The transforms are done through Nashorn-compatible Javascript. Within the Javascript, you can access the collected value by creating a variable name `inputValue`. After manipulating the collected value, you can return the value to Identity Governance by assigning the value to a variable name `outputValue`.

The following example translates the values `true` and `false` from the connected system to `active` and `inactive` in the Identity Governance catalog.

```
if (inputValue == 'true') {
    outputValue = 'active';
}
else {
    outputValue = 'inactive';
}
```

To add or delete a transformation script:

1. Log in as a Globalor Data Administrator.

2 Select a configured data source, and then expand a collector view to view related attributes.

3 Click '{}' icon next to the field mapping to add a script.

or

4 Delete a script.

NOTE: You must remove all references to the script from the attribute mappings to delete a script.

4a Expand the Transformation scripts view of the data collector to see its usage.

4b Expand the collector view(s) mentioned in the usage information.

4c Click '{...}' icon next to the field mapping and choose **Select a script...** to clear the script usage from the attribute mapping.

4d Repeat the above step to remove all usage of the script.

4e Expand the Transformation script view and select the delete icon to delete the script.

For more information about transformations, see the *Collected Data Transformations reference*.

6.9.3 Testing Collections

When creating, updating, or troubleshooting data collectors, you can test all or part of the collections without publishing the results to the catalog. When you test a collection, you either ensure that the collector is correctly configured, or you have the ability to change the collector configuration and quickly test again to check the results.

You can view the collected data as soon as the test collection completes, or you can download the results to view later. Results of test collections remain available in the Identity Governance database until you delete them or they expire.

When you run a test collection, you have some options for the test data:

- All records
- Some records

  When you select a subset of records to collect, you cannot control which records to collect. You could use this option if you want to quickly spot check a collector configuration rather than waiting for all the data to be collected.

- Raw data

  Raw data contains attribute names from the native application. These attributes have not yet been transformed based on the mappings in the collector. Testing the raw data collection lets you verify that you are collecting the data you intend to collect before Identity Governance transforms it.

- Transformed data

  Transformed data contains attribute names that you have mapped from the native application to the attribute names you are using within Identity Governance. Testing the transformed data collection lets you verify that your mappings within the data collector meet your expectations.

To test a sample collection from a data source:

1 Log in as a Global or Data Administrator.

2 Select a data source.

NOTE: Test connection is not supported when the CSV collector is accessed via an HTTP or HTTPS connection.

3 Click **Test Collection and Troubleshooting**.

4 On the Test Collection tab, select the collectors, then:

4a Click **Run Test Collection**.

4b Select the specific entities to collect.

4c (Conditional) To collect a subset of records, type the number of records to collect.

4d (Conditional) To collect all records, make no changes to the default **All** value.

4e Start raw data or transformed data collection.

5 To view the test collection results, select **Actions > View**.

6 To download the test collection results to your local computer:

6a Click **Actions > Test collection results**.

6b Enter a meaningful description.

6c Click **Download**.

6d Click the download icon on the Identity Governance title bar to download test collection results to your local computer.

6e (Optional) Delete the test collection results from the download area in Identity Governance.

If you do not manually delete the test collection results from the download area, Identity Governance will automatically delete the data from the database based on your default download retention day settings. For information about customizing download settings, see Section 4.9, “Customizing Download Settings,” on page 56.

7 (Optional) On the Test Collection tab, click **Actions** > **Delete** to delete the test collection.

Identity Governance will automatically delete the test collection based on your default download retention day settings.

6.9.4 Creating Emulation Packages

You can more easily troubleshoot collection configuration outside your production environment by creating emulation packages for data source collectors. An **emulation package** contains CSV files with the raw collected data from the data source and a CSV file containing data source configuration details. Emulation packages remain available in the Identity Governance database until you delete them or they expire.

To create an emulation package:

1 Select a data source.

2 Select **Test Collection and Troubleshooting**.

3 Under **Download and Emulation**, select **Create emulation package**.

4 Click **Test Collection and Troubleshooting**.

5 On the Download and Emulation tab, click **Create emulation package**.

6 To view the emulation records, select **Actions > View**.

7 To download the emulation package to your local computer:

7a Click **Actions** > **Download emulation package (data source and raw collected data)**.

7b Enter a meaningful description.

7c Click **Download**.

7d Click the download icon on the Identity Governance title bar to download the emulation package to your local computer.

7e (Optional) Delete the emulation package from the download area in Identity Governance.

If you do not manually delete the emulation package, Identity Governance will automatically delete the data from the database based on your default download retention day settings. For information about customizing download settings, see Section 4.9, “Customizing Download Settings,” on page 56.

8 (Optional) On the Download and Emulation tab, click **Actions** > **Delete** to delete the emulation.

Identity Governance will automatically delete the emulation based on your default download retention day settings.

6.9.5 Downloading and Importing Collectors

The ability to download and import collectors helps you manage your environment in several ways.

- Back up a working collector
- Replicate an environment
- Update collector details in a text editor
- Troubleshoot collections

Configuring collectors can take time, and you might go through several iterations of trial and error. When you have configured a collector that achieves the results you want, you should download it and save it with your other backup files. You can also use downloaded collectors to replicate an environment, either in a test environment or to use in another office location.

You could decide that you need to change the predefined attribute mappings and value transformation policies of a template to meet your specific environment. If you find that you need to customize a collector template, rather than only editing the values in a collector, you can download and import collector templates under **Configuration** in Identity Governance. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

NOTE: To correctly import data, you must download data sources from the current version of Identity Governance.

When you download a data source, the zipped file has the name of the data source. For example, `AD_Identities.zip`. The files within the zipped file are generically named in English and can include the following files:

- `Identity_Source.json` or `Application_Source.json` file (depending on type of data source) which contains the configuration of the data source and all of its collectors.

- `DataCenter_datacentername.json` and `DataSourceConnection_datasourceconnectionname.json` files when the collector uses Cloud Bridge connection.
- Attribute files containing the schema elements used by the collectors within the data source. For example, `USER_Attributes.json`, `PERMISSION_Attributes.json`, and `APPLICATION_attributes.json`.
- Template files containing the collector template name and version used to create the collectors in the data source. For example, `Template_AD-Account_4.0.0.json`.
- `Categories.json` file when categories are applied to the source.

To download data source and associated files:

1. Select a data source, then select **Test Collection and Troubleshooting**.
2. Select **Download and Emulation**.
3. Click **Download Data Source Configuration**.
   - **3a** Type a meaningful description such as the collector name.
   - **3b** (Optional) Download included templates, assigned categories, and associated attribute definitions.
   - **3c** Select the download icon on the top title bar to access the saved file and download the file.

   TIP: We recommend creating a folder for *each* data source zipped file and extracting the contents into that folder. This ensures that the similarly named files from different sources are not mixed together or overwrite those from other sources.

To import associated files and data source:

1. (Conditional) If your data source has custom schema or categories associated with it, import the previously downloaded schema files or category files before importing the data source. To import attributes definitions, navigate to the respective attribute page under **Data Administration** and import respective attribute file. To import categories and templates, select respective options under **Configuration**.
2. Under **Data Sources**, select **Identities** or **Applications**.
3. Select **Import an identity source** or **Import an application source**.
4. Based on the type of data source, select the `Identity_Source.json` or the `Application_Source.json` file.

6.10 Upgrading Collectors

Identity Governance allows you to upgrade the collector template when:

- You have upgraded Identity Governance
- You have imported an older collector template
- You have an old collector template which you want to convert to one that accepts change events

While upgrading, Identity Governance allows you to compare the parameters of the two versions, and preserve the configurations and scripts from the old version or make changes as needed. If you decide to use Cloud Bridge for data transfer, you must first create a data center or import the data center JSON file, then configure a data source connection. You can restore to the previous template if needed.

To upgrade the collector template:

1 Under **Data Sources**, select **Identities** or **Applications**.

1a Click **Import an identity source** or **Import an application source**. If you import an identity or application source that was created with an older version of the collector template, click the imported collector, then expand the collector view.

Or

1b (Conditional) If you have upgraded Identity Governance, but have an older version of the collector template, then select the existing identity or application source and expand the collector view.

2 Make necessary changes and save.

3 Click **Upgrade**

4 Compare configurations and make changes as needed.

5 Click **Upgrade**.

6 (Optional) **Restore to Template Version** *number* if you want to revert to the older template.

Identity Governance continues to display the restore link until you dismiss the option.

6.11 Understanding Data Cleanup and Archiving

Identity Governance enables authorized system administrators to perform archiving and cleanup using the Database Maintenance menu. It is essential that you have an effective data cleanup, archiving, and maintenance strategy. Effectively managed cleanup can reduce the volume of data that needs to be archived or backed up. You also must consider dependencies before purging your data. For example, you must consider active instances before snapshots when determining which data to retain and which to purge.

You must cleanup your operations database (by default, `igops`) on a regular basis for efficient performance of your system. Identity Governance archive database (by default, `igarc`) is meant for historical and analytical purposes. It is not intended for disaster recovery and is recommended for use only in development environments. Data restoration should primarily rely on external archive database copies created by the DBA on a regular basis (typically, every week).

We recommend that you do the following to improve performance and reduce data administration costs:

- Create an external archive destination in your stage and production enviorments. This will allow for yearly rotation and free up space when maintenance occurs.
- Create a maintenance schedule to automate cleanup.
- Rotate your archive. When creating a new archive, make sure to change the archive name. Otherwise, all previously archived data will be deleted.

Adjust your data archiving and maintenance schedule based on your system environment. When you fail to archive and cleanup as needed, your data will require additional resources and maintenance.

For more information about the Identity Governance maintenance, cleanup types, and archiving see Chapter 13, “Database Maintenance,” on page 137.

7 Collecting Identities

To certify that your users have the appropriate levels of access to your resources and applications, you need to populate the Identity Governance catalog with the identities, application accounts, and application permissions that exist in your environment. Identity Governance organizes data according to their type of source: identity or application. When you create a data source, you also configure the settings for data collection.

Identity Governance must collect information about users from identity sources. After Identity Governance collects this information, you must publish the information to populate the catalog. You can then assign these users administrative authorizations in the product. For more information, see Section 2.2, “Adding Identity Governance Users,” on page 26.

7.1 Understanding Collector Templates for Identity Sources

Identity collectors populate the catalog with identities and group data. Identities are at the core of the functions of Identity Governance. All collectors share some common elements and features. In addition, identity collectors also include identity specific collector views and publication behavior settings.

7.1.1 Understanding Identity Collector Views

Each identity collector comprises one or more of the following views that you can customize to match the characteristics of the data source being collected.

Collect Identity

To ensure that you can create a unique identity from the data that you collect, you can tell Identity Governance how to map the data collected from an application to the data that you collect from identity sources. Collect as much information as you need to fulfill your business needs. Also ensure that you collect enough information to allow application account and permission data to be joined to your identities. Some common join attributes that are available from most application sources include `email address`, `workforceId`, and `name` attributes.

Collect Group

Identity Governance always uses the `userID` attribute for an identity to join to the membership of collected groups. If a data source does not support group collection, Identity Governance does not allow you to configure this option.

An identity in the catalog can have attributes for one or more organizational group. For example, you might group employee identities by their department, such as Finance or Human Resources. You can use the collected group attribute to set the scope of a review, such as reviewing employees only in the Finance group. For example, Active Directory, eDirectory, and Identity Manager support this type of collection.

Collect Group to User Membership

Collects the relationship that joins users to groups from identity sources that maintain these relationships separate from the basic group information. For example, the JDBC Identity collector runs a SQL query that parses the table that contains the links between groups and users.

Collect Parent Group to Child Group Relationships

Collects the relationship that joins groups to subordinate groups from identity sources that maintain these relationships separate from the basic group information. For example, the eDirectory Identity collector uses this view to obtain nested group members of groups.

TIP: To optimize results, enable these views only when you want to get appropriate data and mapping information. You can disable these views if your data source does not contain identity group collection. For example, the Active Directory collector collects group, user member, and child group member information from the **Collect Groups** view. So, the other views can be disabled.

7.1.2 Understanding Publication Behavior

When you create an identity source, you can specify a publication option. The catalog contains data collected from multiple data sources. To create a unified identity for each person, you need to merge, or unify, the different sets of collected information. Merging occurs during the publication process. For each identity source, you can specify one of the following publication option:

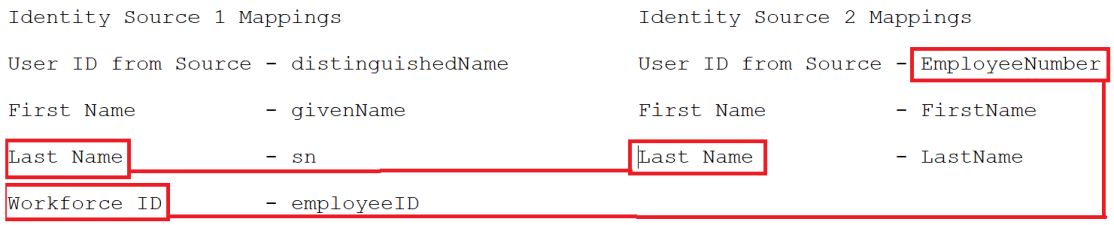
Publish and merge

Use this option when you collect data for the same identity from different data sources. For example, both Active Directory and Salesforce.com have the same `first_name` and `last_name` attributes for Jane Smith. This option allows you to combine the duplicate attributes from the sources into one identity for Jane in the Identity Governance catalog.

When identity sources are merged to create combined published users, there are scenarios where a user collected from an identity source will not merge with a user from another identity source. By default, Identity Governance will create a new user when it cannot merge a collected user with an existing user. However, there are some identity sources where it is not desirable for a new user to be created. These identity sources are only intended to add information to existing users, and are not meant to create new users. You can specify whether a merged identity source should be allowed to create new users, or must always merge with a user collected from another identity source by enabling or disabling **New User Creation**.

When you edit the configuration of a publish and merge collector, the schema mapping user interface presents a **Match rule** check box next to each attribute mapping row. *You must select at least one matching attribute before you can save the configuration*. By specifying the matching attribute you can merge the collected data from an identity source to the existing data. For example, the Workfore ID is used as the matching attribute to map EmployeeNumber to Workforce ID and Last Name to LastName.

Figure 7-1 *Attribute Matching*



NOTE: You must specify unique values for the attributes you want to match during merging. In addition, do not use an empty (null) value as a matching attribute value. If a matching attribute has a null value, the record from the second source is discarded.

You must also specify the rules for merging. Only one of your data sources can be an authoritative source for each identity attribute. To help you specify the **attribute authority**, Identity Governance numbers the data sources within each collection. The first source listed becomes the default authoritative source for all attributes in the collection. However, you can reorder the priority of the data sources or override the default setting for specific attributes. For more information, see Section 9.1, “Publishing Identity Sources,” on page 105.

Publish without merging

Use this option if you have only one identity source or your data sources do not contain the same identities. Since Identity Governance does not perform any merging activities during publication, you might observe faster performance. However, if your sources do contain the same identity, Identity Governance will treat those identities as separate people.

Do not publish

Use this option when you are configuring the identity source. For example, you might not want to publish any collected data when you are testing the process.

7.2 Understanding the Variations for Identity Sources

In Identity Governance, you associate user identities gathered from identity sources to the accounts and permissions assigned in the application sources. Many user identities are categorized by groups and have parent-child relationships with other identities or accounts. However, some application sources might define groups or parent-child relationships in a different way than Identity Governance. Also, some identity sources might be configured to generate incremental change events.

For more information about variations in service parameters and collect view procedures, see Chapter 17, “Understanding Variations in Collector and Fulfillment Target Configurations,” on page 183.

7.3 Collecting from Identity Sources with Change Events

NOTE: We do not support using the Identity collector with changes when you merge idenity sources.

Full collection and publication includes data collection, provisioning technical and business roles, and SoD and risk calcuations and might take more processing time and memory when compared to incremently collecting changes. **Identity sources with change events** provide incremental change events for user and group data from certain identity sources to incrementally update the identity catalog and improve processing time and reduce database growth.

Always monitor processing times, system memory usage, and database growth and evaluate if full collection or change collection will be the best option for your environment. For example, if Active Directory is your LDAP source and by default you collect Last Login attribute, collecting only change events might also take as much as time as a full collection. In that scenario, change events collection might not be the optimal option.

IMPORTANT: The identity source with change event collectors is not intended to handle large-scale changes to the source directory, such as changes to the user population resulting from mergers or spin-offs, major changes to group memberships, or major reorganizations of any kind. In such cases, you should disable event processing and enable it after the major changes.

To periodically pull change events and incrementally make changes to your identity catalog, the following conditions must be met:

- An identity source has a collector which can be configured to provide change events, either by having created an identity source from a suitable template, or by having migrated a non-event-aware identity source by using the Identity Governance Migration Utility and selecting enabling event collection. For more information, see “Creating Identity Sources” on page 90 and Section 7.3.3, “Converting an Identity Collector to a Change Event Identity Collector,” on page 89.
- The identity source is the primary identity source. For example, it is either the sole identity source or an unmerged identity source.
- The identity event source has been collected and published.
- The configuration of the identity source and its collector has not changed since the last publication.
- Identity event source collection, identity publication, or application publication is not in progress.
- (Conditional) For eDirectory, the Change-Log module must be installed to support event processing. For more information, see “Installing the Change-Log Module on a Remote eDirectory server ” in the *NetIQ Driver for Bidirectional eDirectory Implementation Guide*.
- (Conditional) For Identity Manager, the Identity Gateway Integration Module must be installed on the target Identity Manager server. Using Designer, install the following packages to support event processing:
  - Identity Gateway Integration Module Base

- Identity Gateway Integration Module Default
- Identity Gateway Identity Governance Integration Package

For more information, see the *NetIQ Identity Manager Driver for Identity Gateway Integration Module Implementation Guide*.

Identity Governance allows you to configure multiple non-merging identity source collectors to collect change events. You can set the polling interval and maximum polling time in minutes for each collector so that they can function independently. *We do not recommend setting the polling interval time to less than 35 minutes.*If you do not set the polling values while configuring the collector, Identity Governance uses the globally set preconfigured values to determine the polling frequency. However, the polling values set at the collector level takes precedence over the globally set values. Identity Governance uses the global configuration parameters: `com.netiq.iac.rtc.event.polling.interval` and `com.netiq.iac.rtc.max.polling.timeout` to set the polling values.

You must perform at least one collection and publication before Identity Governance launches into the polling cycle, or the **Enable change event processing** flag will remain blocked.

The **Identity Change Event Productions** allows you to see details of the change events that occurred during the polling time, such as, entities that were added, modified, or deleted. Depending on your requirement, you can select or sort the columns, or use event data to search events. You can also filter event data based on specific event type.

If you collect for one of the data sources after enabling event collection, Identity Governance suspends polling for that source but continues polling for the other identity sources with change event collection. Polling for the suspended source does not resume until the collection is published by the next identity publication.

NOTE: When an identity publication is in progress, polling for all identity sources change event collectors is temporarily suspended until the publication completes.

Typically, events are collected in batches of up to 100 events. However, if the identity source's **Batch Size Limit** as configured in the **Service Parameters** is less than 100, then that batch size is the upper limit for event collection.

During event collection, Identity Governance treats a user record move in the underlying LDAP tree from *outside of* to *inside of* the scope of the configured Search Base as an ADD event. Likewise, Identity Governance treats a user record move to the *outside of* the Search Base scope as a DELETE event. The **Data Sources > Activity** page reports the number of events of each type that were processed in the most recent event processing period as part of the detail of the most recent collection for that collector.

For more efficient event processing, Identity Governance does not generate change events for any dynamic changes in eDirectory or Identity Manager dynamic groups. Also, removing a member from an eDirectory or Identity Manager group will not remove that member from any of the group's super groups if those groups have been configured to report nested members in membership query.

If you have upgraded from a previous version of Identity Governance, use the Identity Source Migration utility to update your Active Directory data collector, eDirectory data collector, and Identity Manager data collector to accept change events.

- Section 7.3.1, “Understanding Change Event Collection Status,” on page 88
- Section 7.3.2, “Supported Attribute Syntaxes for eDirectory and Identity Manager Change Events Collection,” on page 88
- Section 7.3.3, “Converting an Identity Collector to a Change Event Identity Collector,” on page 89

7.3.1 Understanding Change Event Collection Status

The event collection displays the following status:

Change Event Collection Status	Description
DISABLED	Event processing is not enabled for this collector and identity source. If event processing is enabled from this state, the state becomes BLOCKED, and the identity source must be collected and published before it can become READY.
BLOCKED	Event processing is enabled, but cannot proceed because the preconditions for processing change events were not met. For more information, see Section 7.3, “Collecting from Identity Sources with Change Events,” on page 86.
READY	Event processing is enabled and not blocked, but awaiting scheduling to proceed.
IN_PROGRESS	Events are being polled for and processed. **NOTE:** Event processing will be in progress either until a polling request returns no events or until the configured maximum event processing time is reached.

7.3.2 Supported Attribute Syntaxes for eDirectory and Identity Manager Change Events Collection

Identity Governance supports the collection of the following attribute syntaxes during eDirectory and Identity Manager change events collection:

- `Boolean`
- `Case Exact String`
- `Case Ignore List`
- `Case Ignore String`
- `Class Name`
- `Counter`

- Distinguished Name
- Integer
- Integer 64
- Interval
- Numeric String
- Object ACL
- Octet String
- Path
- Postal Address
- Printable String
- Telephone Number
- Time
- Typed Name
- Unknown

7.3.3 Converting an Identity Collector to a Change Event Identity Collector

Identity Governance allows you to convert an existing identity collector to one that accepts change events. While converting, you can compare the parameters of the two versions and make changes to the fields as required. You can convert the following identity collectors:

Collector	Convert to
AD Identity	AD Identity with changes
eDirectory Identity	eDirectory Identity with changes or IDM Identity with changes
eDirectory Identity with changes	IDM Identity with changes
Identity Manager Identity	IDM Identity with changes

To convert an identity source to one with changes:

1. In Identity Governance, select **Data Sources** > **Identities**.
2. Select the identity source, then expand the view of the collector.
3. (Conditional) If a higher version of the collector template is available, then Identity Governance provides the option to upgrade the template. To upgrade:
   - **3a** Specify details as necessary and save.
   - **3b** Select **Upgrade**.
   - **3c** Compare configurations and make changes as needed.
   - **3d** Select **Upgrade**.

3e Select **Back to data source page**.

3f (Optional) **Restore to Template Version** number if you want to revert to the older template.

4 To convert the template to with changes, click **Convert**.

5 Review the following updates:

- Identity Governance changed the template name to **with changes** template corresponding to the one prior to the update.
- The **Service Parameters** section prompts to re-enter the password.
- Under **Collect Identity** and **Collect Group** (the user view):
  - (Conditional) For Active Directory identity change event source, Identity Governance has added the new parameter **LDAP Identity Changes Search Filter**, with the value `(objectClass=user)`. This parameter identifies events in Active Directory DirSync or AD Connect that the connector delivers in this view to Identity Governance. Only modify this parameter if you have other object classes in the local AD that correspond to users and only by adding other `objectClass` terms to an LDAP expression.
  - (Conditional) For Active Directory identity change event source, Identity Governance has added the new parameter **AD Object Categories for Changes**, with the value `user`. You can modify this value if needed by adding other object category names in a comma-separated list.
- The option **Enable Change Event Collection** is checked and requires input for the following fields:
  - Polling interval

    We do not recommend setting this to less than 35 minutes.
  - Maximum poll time
  - Last poll time

6 Click **Convert**.

7.4 Creating Identity Sources

Identity sources provide the information to build a catalog of the people within your organization. The information that you collect from your data sources can add as much personally identifiable information as you need to create the unique identity for each person.

NOTE: When you create identity sources, keep the following in mind:

- If you are using the Identity Manager Identity collector, it must always be first in the list of collectors. Otherwise user authorizations will fail. For more information, see Section 7.5, “Assigning Identity Manager as the Primary Identity Source,” on page 92.
- If you collect data from two or more identity sources that have duplicate information for the `Primary Supervisor ID from Source` attribute, Identity Governance cannot merge or publish the data. After collecting each identity source, you must define extended attributes,

such as `Source1_userID` and `Source2_userID`, for the `Primary Supervisor ID from Source` attribute. Then, to merge the information, specify the extended attributes as the "Join to" attribute for `Primary Supervisor ID from Source`.

- Identity Governance provides Custom Collector SDK to create collectors. For more information about installing the Custom Collector SDK, see *Identity Governance Release Notes*.

To create a identity source and collect identities and groups:

1. Log in to Identity Governance as a Global or Data Administrator.
2. Select **Data Sources**.
3. (Conditional) To create an identity source collector, select **Identities**.
4. Select **+** to create an identity source collector from a template.

   or

   Select **Import an Identity Source** to specify a JSON file to import.

   IMPORTANT: To import a data source, you must first export the data source from the current version of Identity Governance. Data source files exported from earlier versions of Identity Governance do not import correctly to the current version. Hence, the data source must be recreated in the current version of Identity Governance.

   ---

5. (Conditional) To collect from a CSV file, specify the full path to the file.

   The CSV collector supports TSV files. To use a TSV file, enter the word `tab`, in uppercase, lowercase, or any combination in the **Column Delimiter** field.

6. (Conditional) To configure an identity source with change events collector, select a template name ending in **with changes** and observe the conditions listed in Section 7.3, "Collecting from Identity Sources with Change Events," on page 86. For more information, see "Understanding Change Event Collection Status" on page 88 and "Supported Attribute Syntaxes for eDirectory and Identity Manager Change Events Collection" on page 88.

   NOTE: A change to the collector configuration suspends change event processing, which does not resume until a full batch collection and publication completes.

   IMPORTANT: For large scale changes, disable event collection, and enable it only for incremental change events.

   ---

7. Specify all the mandatory fields for the data source.

   For more information, see the following content:

   - Section 6.9.1, "Understanding Collector Configuration," on page 73
   - Section 7.1, "Understanding Collector Templates for Identity Sources," on page 83
   - Section 7.2, "Understanding the Variations for Identity Sources," on page 85

8. Configure publication behavior.
9. (Conditional) If you select **Publish and Merge** as your publication behavior, enable or disable **New User Creation**.
10. (Conditional) To merge the collected data from an identity source, specify which attributes to match by selecting **Match rule** check box.

As each identity source collector configured for publish and merge can potentially create new Identities in the catalog, you should always ensure that the mandatory **User ID from Source** attribute mapping is configured to collect an acceptable unique identifier that is appropriate for the catalog.

IMPORTANT: When collecting identities using the publish and merge setting, matching attributes are mandatory for Identity Governance to include the user when publishing. If a secondary identity source has users that do not have the matching attribute defined in the collector, they will be collected, but they will not be published. For information about merging examples, see the *Data Collection and Publication Technical Reference (https://wwwtest.microfocus.com/documentation/identity-governance/4.3/tech-refs/Collector-Data-Transformation.pdf)*. For information about setting merge rules before publishing identities, see Section 9.1.2, “Setting the Merge Rules for Publication,” on page 106.

---

11 Save your settings.

12 Select **Test Collection and Troubleshooting**.

12a To ensure your settings are correct run test collections. For more information, see Section 6.9.3, “Testing Collections,” on page 76.

12b (Optional) To preview data, create emulation package. For more information, see Section 6.9.4, “Creating Emulation Packages,” on page 77.

13 Select Collect now icon on the Identities page individually.

14 (Optional) Schedule a collection. For more information, see Chapter 10, “Creating and Monitoring Scheduled Collections,” on page 109.

The first time you set up Identity Governance, you must collect and publish data after creating your data sources so that your catalog contains the data. For information about publishing identities, see Section 9.1, “Publishing Identity Sources,” on page 105.

7.5 Assigning Identity Manager as the Primary Identity Source

You must assign Identity Manager as your primary identity source. If Identity Manager is not assigned as the primary identity source, user authorizations will fail with the following error:

```
You are authenticated and logged in, but you do not have access to the
Identity Governance application. This means you logged in as a user who was
valid in your authentication source, but has never been collected in
Identity Governance or does not have access to the Identity Governance
application.
```

Identity Governance expects the Identity Manager Collector to be the first collector in the list of Identities Collectors.

You can use one of the following workarounds to resolve this issue:

Workaround 1

1 Log in to Identity Governance as the Bootstrap Administrator.

2 Select **Data Sources** > **Identities**.

3 Expand the **Merging Rule**.

4 In the LDAP Distinguish Name field, change the value from **None** to **Identity Manager Collector**.

5 Click **Save**, and then publish the change.

Workaround 2

1 Log in to Identity Governance as the Bootstrap Administrator.

2 Select **Data Sources** > **Identities**.

3 Drag and drop the Identity Manager Identities Collector to be first in the list.

4 Click **Save**, and then publish the change.

8 Collecting Applications and Application Data

Identity Governance enables Data Administrators to separate the process of defining an application in the governance system from collecting the data for the application. You can configure application definition data sources to collect application entities from a CSV file or a Configuration Management Database (CMDB) using an application definition template. You can also configure application data sources to collect accounts and permissions data using account and permission collectors.

8.1 Understanding the Application Definition Template

Identity Governance uses an **application definition template** to create application entities. This feature enables you to collect application configuration items from ServiceNow, Identity Manager, and a CSV file. You can include information about one or more applications or drivers, such as their name, description, risk, classification, and vendor in a CSV file, or add ServiceNow or entitlement drivers and add the applications or drivers as an application source on the **Data Sources > Applications page**. You can then configure any of the applications to collect data from one or more applications. Each application source and its collectors can then be exported and imported as needed.

NOTE: The IDM Entitlement application definition template collects only Identity Manager applications and creates an application data source for each supported driver. You can rename or delete a driver from the Application Sources page as needed. For the list of supported drivers, refer to *Technical Requirements*.

For more information about defining an application and collecting from application sources, see Section 8.8, “Collecting Application Data for Multiple Applications,” on page 101 and Section 8.7, “Collecting Application Data from a Single Application Source,” on page 100.

8.2 Understanding Collectors for Application Data Sources

An application collector can be a single-application collector or a multi-application collector. To configure an application as a multi-application collector, you must specify a unique ID when configuring the application source. If you do not specify a unique ID, Identity Governance will create a unique ID and recognize it as a single application data source. For an application to be eligible for collection using the multi-application collector:

- The subordinate applications must have no collectors.
- The application must have a unique ID (Application ID from Source).
- The permissions of the application must not be collected by any other application.

Account and permission collectors are the two types of collectors available within an application source. In general, application data stores do not maintain personal information about the account holders since it is not needed for the operation of the application. These applications might hold basic information such as an Account Identifier (or login ID), a password, and the set of permissions that have been granted to the account users (group memberships, roles, ACLs, and so forth). In a typical enterprise, there will also be some account attribute (or combination of them) that can be used to associate (or join) the account to the identity that uses the account. However, this is not true for all accounts. Many applications have admin or system accounts that IT staff and administrators use to maintain the application, grant access to others, and so forth. Often, these admin or system accounts are granted the greatest level of permissions for the application. Additionally, sometimes these superuser accounts are shared by a group of individuals. As a result, it is very important to collect and review *all* accounts from the data source whether they can be joined to an identity or not. Identity Governance enables you to collect and publish accounts, then view both mapped and unmapped accounts in the Accounts catalog.

Account collectors gather information about the application users, such as their name, account ID, login name, and login time. Permission collectors gather information about the application access rights of the account users. Since there is no universal method for linking accounts and permissions to identities, these collectors also provide the attributes and optional views necessary to join application accounts to Identity Governance identities and to join application permissions to either Identity Governance identities or the application accounts as needed.

NOTE: *The source type of application connectors does **not** have to be the same*. For example, there may be an attribute on User accounts in Active Directory (for example, myAppRoles) that is used to assign permissions for an enterprise application. Although the accounts are collected from Active Directory, permissions may be collected from a JDBC database, a CSV file, or some other source.

Some permission collectors can collect nested permission assignments. For parent-child hierarchy permissions, when a user has an assignment for a child permission, they may also optionally be given an assignment for the parent permission. To allow the creation of these nested permission assignments, you must enable the option **Populate Nested Permission Assignments** while configuring the service parameters. The **AD Permission** and the **eDirectory Permission** collector templates include this option by default, but you can create a custom template and include the option to collect nested permission assignments.

IMPORTANT: When **Populate Nested Permission Assignments** is enabled, the assignment type attribute on collected permission assignments will show as DIRECT even if the value supplied by the collector is different. Identity Governance ignores the assignment type attribute value supplied by the collector.

- Section 8.2.1, “Understanding Account Collector Views,” on page 97
- Section 8.2.2, “Understanding Permission Collector Views,” on page 97

8.2.1 Understanding Account Collector Views

Depending on the type of data that you want to collect, the account collector template might provide the following elements:

Collect Account

Accounts represent entities, such as a system, application, or data source, that an identity might access. For example, your employees might have an account that lets them log in to your company email system. An account in Identity Governance is similar to an association in Identity Manager.

Accounts can also have custodians. Some application sources such as eDirectory and Active Directory supports the concept of custodians which can be collected directly from the application. Once you collect the data, you can configure the account collector template to map the Account custodian attribute and join it to identity available in the Identity Governance catalog.

Identity Governance uses the **Account-User Mapping** attribute to join the accounts with the identities available in the catalog. You must specify the value for **Account-User Mapping** and the **Map to attribute** for Identity Governance to do the association.

Collect Provisioning Applications

Applies only to Identity Manager AE data sources.

Collect Connected Accounts

Applies only to Identity Manager AE data sources.

8.2.2 Understanding Permission Collector Views

Permission collectors gather the following types of information and create a catalog of permissions for the Application source:

- The set of permissions and descriptive attributes for each permission type
- The hierarchical relationship (if any) among permissions
- The data that will allow Identity Governance to join permission assignments to identities or accounts

There are a great number of variations in the way that permissions and their various relationships are described within each application source. To accommodate this variety, Identity Governance provides many ways to configure permission collectors by using views. The primary purpose of these views is to get the detailed information about the permission objects or values of a selected permission type.

Collect Permission

Used to collect the available permission values and descriptive information about the permission. If the permission schema contains the information needed to establish permission hierarchy and join permission values to Identities or Accounts, this view can be utilized to perform those functions also – with the benefit of configuration simplicity and better performance. Some examples of applications that utilize this type of combined view are the Active Directory and eDirectory `Group` permission collectors.

Sometimes a permission might have a owner assigned to it to review the access, evaluate the risk, or confirm decisions before removing permissions. You can collect the data directly from the application source and configure the permission collector template to map the Permission Owner attribute to identities or account holder. To map identities and groups as permission owners, specify a value for the **Permissions-owners-mapping** attribute, then select either **User ID from Source** or **Group ID from Source** or select both.

Collect Holder to Permission Mapping

Used when the information about assigned permissions is contained within a source that has the holder-to-permission relationship defined on the holder (Account of Identity) records. Some examples of applications that use this method exclusively are Salesforce.com and SAP. An example of this relationship would be the `memberOf` attribute on Active Directory User objects.

Collect Permission to Holders Mapping

Used when the information about assigned permissions is contained within a source that has the holder-to-permission relationship defined on the permission records. An example of this relationship would be the User `members` attribute on eDirectory Group objects.

Collect Permission hierarchy based on parent to child view

Used to collect top-down permission relationships. An example of this relationship would be the Group `members` attribute on eDirectory Group objects.

Collect Permission hierarchy based on child to parent

Used to collect bottom-up permission relationships. An example of this relationship would be the Group `memberOf` attribute on eDirectory Group objects.

8.3 Understanding Variations for Application Sources

All collectors share some common elements and features. In addition, collectors might include unique configurations. For information about additional service parameter and collect views configuration procedures, see Chapter 17, “Understanding Variations in Collector and Fulfillment Target Configurations,” on page 183.

Identity Governance also provides unique hybrid collections and supports change event processing for application sources. For more information see, Section 8.4, “Understanding Hybrid Permission Collectors,” on page 99and Section 8.9, “Understanding Change Event Processing,” on page 102.

8.4 Understanding Hybrid Permission Collectors

Identity Governance includes two hybrid collectors: eDirectory and Active Directory (AD). Hybrid collectors are used to collect:

- Permissions not related to application resources
- Applications that use eDirectory or Active Directory for authorization but do not utilize groups to assign the application permissions
- More details about the permissions that cannot be obtained from the simple assignment information maintained in eDirectory or Active Directory

  For example, Active Directory may represent access to an application by assigning attribute values to some custom attribute (for example, myAppAssignments) on the Active Directory account records. We collect those permission assignments using an LDAP collector (with a permission holder mapping to the custom attribute). However, the details of the permission objects (such as name and description) are not available as Active Directory objects; they are records in a CSV file. In that situation, we need to collect the Permission entities using a CSV collection method, and the Permission to Holder relationships using LDAP.

In a standard permission collector, the permissions and holder assignments must be collected using the same application connection method. The hybrid permission collectors allow the permission data to be collected from a CSV file, and the holder assignment data to be collected using LDAP. Note that for the CSV permission collections, just as with other CSV collections, data administrators need to generate the CSV and make it available to the Identity Governance service through a file share, http, or local file system.

8.5 Creating an Application Source

Application sources provide the information to build a catalog of the permissions and accounts within your organization. These data sources are configured with one or more collectors to gather the information from that source.

Identity Governance enables you to create application sources in the following ways:

- Using the application definition templates provided with Identity Governance

  Application definition source templates enable you to create an application that can collect permissions from other eligible applications as well as collect accounts and permissions from a variety of application sources.
- Manually creating an application
- Importing a JSON file

To create an application source using the application definition template:

1. Log in to Identity Governance as a Global or Data Administrator.
2. Select **Data Sources > Applications Definitions**.
3. Specify a name and description.
4. Select an application definition template such as ServiceNow or CSV.
5. Specify all the mandatory fields.

6 Save your settings.

7 Select **Application Definition Sources**.

8 Click the Collect icon.

9 Select a publication option.

9a To publish all applications click the **Publish** icon.

9b To publish only the changes, select the **Apply Changes** icon.

10 Select **Data Sources > Applications**.

11 Check that all the defined applications are listed as applications.

To create an application manually:

1 Log in to Identity Governance as a Customer or Data Administrator.

2 Select **Data Sources > Applications**.

3 Select **+** to create a data source.

4 Specify a name.

5 (Optional) Specify other fields as needed.

6 Save the settings.

7 Select **Data Sources > Applications** and configure the newly collected application.

To create an application by importing a JSON file, select **Import an application source** on the Applications page and import the application JSON file.

IMPORTANT: To import data sources, you must first export the data source from the current version of Identity Governance. Data source files exported from earlier versions of Identity Governance do not import correctly to the current version. Hence, the data source must be recreated in the current version of Identity Governance.

8.6 Exporting and Importing an Application Source and Collectors

Authorized administrators can import and export the data source and the included collectors. If an application source has multiple account or permission collector configured within it, Identity Governance provides the option to export and import each collector independently. The exported folder contains the collector template, attribute files, and if the collector has Cloud Bridge connection configured, the data center and the data source connection JSON files. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

8.7 Collecting Application Data from a Single Application Source

You can configure the default collector templates to collect application data from an application.

To create a application source and collect accounts and permissions:

1. Log in to Identity Governance as a Customer or Data Administrator.
2. Select **Data Sources > Applications**.
3. Edit an application.
4. Select **+** to create a data source collector from a template.

   NOTE: You can select and configure more than one account or permission collector for application collection.

   ---

5. Specify all the mandatory fields for the data source.

   NOTE: If you are collecting with the PAM collector, you should specify the permission type you want to collect User Role and Resource Pool. Additionally, indicate whether you intend to collect disabled permissions.

   For more information, see the following content in:

   - Section 6.9.1, "Understanding Collector Configuration," on page 73
   - Section 8.2, "Understanding Collectors for Application Data Sources," on page 96
   - Section 8.3, "Understanding Variations for Application Sources," on page 98
6. Save your settings.
7. (Optional) To preview all or part of the data, select **Test Collection and Troubleshooting**. For more information, see "Testing Collections" on page 76.
8. Select **Collect Now** icon for each data source on the Applications page.
9. (Conditional) When allowed, select the type of publication.

   NOTE: The ability to publish only changes will depend on your collection and publication scenario. For additional information about change event processing, see Section 8.9, "Understanding Change Event Processing," on page 102.

   9a To publish all collected accounts and permissions, select **Publish**.

   9b To publish only the changes, select **Apply Changes**.

   9c Click **OK**.
10. Publish data.
11. When you see that publication has completed, go to **Catalog** to view the collected information.

8.8 Collecting Application Data for Multiple Applications

When collecting permissions or accounts for a multi-application collector, you must collect the Unique Application ID attribute. The value collected for this attribute will determine the application the collected permission or account will be assigned to. Identity Governance searches for an application whose Application ID From Source attribute matches the collected Unique Application ID value.

To create a multi-application collector:

1. Log in to Identity Governance as a Customer or Data Administrator.

2 Select **Data Sources > Applications**.

3 Edit an application source or create an application manually.

4 Specify Unique Application ID.

5 Save the changes.

6 Enable the data source to collect permissions or accounts from multiple applications.

7 Add eligible applications.

NOTE: For an application to be eligible for collection using the multi-application collector, the subordinate application must have no collectors, must also have a unique Application ID (Application ID from Source), and its permissions must not be collected by any other application.

---

8 Specify all the mandatory fields for all the data sources.

9 Save your settings.

10 (Optional) Select + and add collectors. For more details about collecting accounts and permission data see, Section 8.7, “Collecting Application Data from a Single Application Source,” on page 100.

8.9 Understanding Change Event Processing

After you create your application source and perform a full collection and publication, you can apply only the changes that happened in any Application or Application Definition data sources since your last publication. You can apply the changes any number of times and as frequently as you want, but a full collection must always be followed by a full publication.

Always monitor processing times, system memory usage, and database growth and evaluate if full collection or applying changes will be the best option for your environment.

When you apply changes, Identity Governance collects the latest raw data and compares the data with the previously collected raw data. Identity Governance then publishes only what has changed. This saves space in the database because Identity Governance updates the current snapshot with only the changes. However, note that the overall applying changes process might take longer time than a full collection and publication.

IMPORTANT: Applying changes is not intended to handle large-scale changes to the source directory, such as changes to the user population resulting from mergers or spin-offs, major changes to group memberships, or major reorganizations of any kind. In such cases, we recommend a full collection and publication.

Note that Identity Governance will not allow you to apply changes in the following scenarios:

- When you collect data for a full publication but do not publish
- When you add a new collector to an existing application source
- When you have one or more collectors disabled during a collection, or a collection could not collect from all the collectors.

When you apply changes, Identity Governance goes through two phases: collects the raw data, and then processes the change events that were detected as a result of the collection. You can cancel applying changes regardless of the phase it is in, but if you cancel before the changes are applied you will not be able to perform a full publication after cancellation. You have to either perform a new collection, or complete the apply changes action. You can resume to apply the changes.

NOTE: In an application you can collect, publish, or apply changes at any time.

Once the changes are applied, click the **Show All Collect and Publish Productions** link to view the collection and publication details. You can see the steps of that publication as well as the number of entities that were added, modified, or deleted at each step. If you want the publication to save detailed information about the changes that were made so that you can review the changes later or see exactly what has happened, a Global, or a Bootstrap Administrator must first enable these global properties:

`com.netiq.iac.pce.save.add.events`

When set to `true`, Identity Governance save events that added entities, or relationships between entities. You can see details of new entities and relationships that were created.

`com.netiq.iac.pce.save.modify.events`

When set to `true`, Identity Governance save events that modified entities, or relationships between entities. You can see what the entities or relationships looked like before and after they were modified.

`com.netiq.iac.pce.save.delete.events`

When set to `true`, Identity Governance save events that deleted entities, or relationships between entities. You can see details of entities or relationships that were deleted.

8.10 Collecting Application and Application Definition Data Source Change Events

Understand how change event processing works, then evaluate if full collection or applying changes will be the best option for your environment.

To apply changes, select **Data Sources** > **Applications** or **Application Definitions**, collect data and publish, then apply changes. Note that the option to apply changes might not always be available. Identity Governance evaluates the collection scenario and makes a determination regarding the ability to perform change event collection.

You can hover the cursor over each status icon on the Application Sources and the Application Definition Sources pages to see the current status of your action. Click the date and time link to view more details about the current collection.

9 Publishing the Collected Data

Publication makes the most recently collected data, and the relations among that data, available in the catalog. When you publish identity data, you can configure Identity Governance to merge the attributes of a unified identity. Application publication uses the most recent identity publication to resolve permission and account holder relationships. Identity Governance always publishes the current snapshot of the collection. For example, if a collection is in process, Identity Governance publishes the previously collected data.

9.1 Publishing Identity Sources

Identity Governance publishes all identity sources concurrently to ensure that each unified identity receives the latest merged information. Identity sources always get published before application sources.

9.1.1 Planning for Publishing and Merging Identities

When using the Publish and merge option for your Identity Collectors, you will need to plan the following actions:

- Specify the order in which your identity sources will be published
- Specify the attribute(s) that will be used to match records from each source to identities in the catalog
- Designate which identity source will be used as the preferred (authoritative) source for the attributes that will be used to match records
- Decide if you want to allow or prevent new user creation when users from an identity source cannot be merged with an existing user from another identity source

For information about setting the merge rules, see Section 9.1.2, “Setting the Merge Rules for Publication,” on page 106.

9.1.2 Setting the Merge Rules for Publication

Merge rules allow you to control which values will be stored when multiple identity sources provide information for the same fields. For example, if two sources provide an email address, data from the selected source will be saved as the primary value. If you do not select a identity source as the authoritative source for merging, Identity Governance uses the first collected value.

Once you set the merge rules, you can export the rules as a JSON file, and import the file in another Identity Governance environment. The JSON file includes the merge order for the identity sources and the authoritative source for the identity attributes. While importing the merge rules, Identity Governance tries to match the identity data sources between the two systems based on ID or name and makes the best decision it can. However, before you import, you can change that decision or resolve any difference such as different mergeable identity sources or different identity attributes between the two systems.

If you delete any identity source or authoritative source from the system where data is imported and import the same file, Identity Governance displays only the current mergeable data present in the system regardless of the data being present in the exported file.

IMPORTANT: When collecting identities using the publish and merge setting, matching attributes are mandatory for Identity Governance to include the user when publishing. If a secondary identity source has users that do not have the matching attribute defined in the collector, they will be collected, but they will not be published. For information about merging examples, see *Data Collection and Publication Reference (https://wwwtest.microfocus.com/documentation/identity-governance/4.3/tech-refs/Collector-Data-Transformation.pdf)*.

---

1. Log in to Identity Governance as a Customer or Data Administrator.
2. Select **Data Sources > Identities**.
3. Drag and drop the identity sources to their desired positions to set their priority for merging the published attributes. In general, it is desirable to place your most complete and authoritative source in position 1.
4. To use a specific identity source as the attribute authority, complete the following steps:
   - **4a** Under Publish and merge, expand **Set merging rules**.
   - **4b** For the attribute that you want to modify, specify the identity source.

     The **None (first collected value)** option instructs Identity Governance to use the first identity source as the attribute authority.

     NOTE: You must specify unique values for the attributes you want to match during merging. In addition, do not use an empty (null) value as a matching attribute value.

     ---
5. (Optional) Click **Export merging rules** or **Import merging rules**.
6. Select the **Save** icon.
7. Publish your pending changes.
8. Verify the changes that you published to the catalog.

9.1.3 Publishing the Identity Sources

Since the Identity Governance catalog is comprised of the data contributed by all published sources of Identity data, you must perform a publication of Identity data only after you have performed a collection from all sources. The publication process will unify your collected data sources and populate the catalog.

If you have a scheduled collection, Identity Governance publishes the collected identities at the end of the run. You can also manually publish the identity sources.

Identity Governance uses a red diamond icon to indicate that an identity source has been collected but not published. Identity Governance shows any collection errors or warnings on the **Identities** and **Applications** data source pages.

To manually publish the identities:

1. Log in to Identity Governance as a Customer or Data Administrator.
2. Select **Data Sources > Identities**.
3. Make sure you have collected all the identities.
4. Select the Publish identities now icon.
5. When you see that publication has completed, go to **Catalog** to view the collected information.

9.1.4 Viewing Merge Histories

Identity Governance enables you to keep track of the merge events that cause unique user IDs to be created, assigned, or changed during the publication of identities. It also tracks events where merging could not happen. The merge process might result in events such as:

- The collected user fails to merge and does *not* create a new user
- A collected user that was previously merged no longer merges and new user creation is not allowed
- A previously merged user is split into different users, and a new user is created with a new unique user ID
- A collected user that used to merge with one user now merges with another user, which changes its unique user ID

You can view these merge events to investigate how identities were merged and why a certain user ended up having a certain unique user ID.

To view merge histories:

1. Log in to Identity Governance as a Customer or Data Administrator.
2. Select **Data Sources > Identities**.
3. In the upper right, select **Merge Histories**.
4. Select a tab to investigate merge events.
5. Select the Settings icon to add and delete columns.
6. Based on your analysis and needs, change your publication options. For support with troubleshooting issues, contact your Customer Support team.

9.2 Publishing Application Sources

If you have a scheduled collection, the scheduled run publishes the collected application data at the end of the run. You can also manually publish the application data source independently from other application data sources. However, before publishing an application data source, you must publish your identity sources.

To manually publish applications:

1. Log in to Identity Governance as a Customer or Data Administrator.
2. Publish your identity sources.

   For more information, see Section 9.1.3, “Publishing the Identity Sources,” on page 107.
3. Select **Data Sources > Applications**.
4. For each application source that you want to publish, select a publication option.

   NOTE: The ability to publish only changes will depend on your collection and publication scenario. For additional information about change event processing, see Section 8.9, “Understanding Change Event Processing,” on page 102.

   4a. To publish all collected accounts and permissions, click the **Publish** icon.

   4b. To publish only the changes, select the **Apply Changes** icon.

TIP: You might intermittently experience extended delays in publishing eDirectory permissions due to hardware, operating system performance, database performance, disk space, network speed, or other environmental factors. If you experience significant delay, cancel the current publication and start a new publication of the same source. In most cases, the new publication will complete as expected.

10 Creating and Monitoring Scheduled Collections

You can collect data on individual sources at any time. To enhance the collection and publication process, you can schedule collections to run at regular intervals. Each collection can contain one or more identity and application sources. For example, you might want to update identities associated with your human resources application every week. Instead of manually collecting and publishing those identities, you can create a scheduled collection.

To see the status of all recent and pending collections, go to **Data Sources > Activity**.

NOTE: After each run of a scheduled collection, Identity Governance automatically publishes the data.

10.1 Creating a Scheduled Collection

You can schedule collections to run at regular intervals. For example, if you want to collect data from Workforce and SAP identity sources every week, specify the start and end dates for the collection and how often it repeats. Alternatively, you can specify a custom string to run the scheduled collection on a specific set of dates. If you want to collect and publish only the changes that have happened in any application and application definition data sources, you can set the schedule based on your requirement, such as, daily, weekly, hourly, and enable **Publish Only Changes**. You can create schedules to publish changes, as well as schedules to do full publications.

NOTE: The option to Publish Only Changes is only available for schedules that include one or more application sources. This option does not apply to identity sources, only application sources. Schedules that include both identity sources and application sources will always perform a full publication of the identity sources, whether you enable or disable the Publish Only Changes option.

---

1. Log in as a Global or Data Administrator.
2. Under **Data Sources**, select **Schedules**.
3. (Conditional) When adding a new scheduled collection, complete the following steps:
   - **3a** Select **+** to create a new schedule.
   - **3b** Specify a name and description.
   - **3c** Specify the identity and application sources for collection.

NOTE: You cannot schedule a collection for applications without collectors.

3d Enable **Publish Only Changes** if you want application sources to only publish changes.

4 (Conditional) To modify an existing scheduled collection, select its name.

5 (Optional) To customize the interval for running the collection, complete the following steps:

5a For **Repeat**, select an interval or specify **custom**.

IMPORTANT: If using the hourly interval, specify at least 24 hours between collections to avoid errors when a new collection starts before a previous one completes.

5b Specify values for the starting and ending dates and the time zone.

5c For **Custom**, use the following syntax to indicate the collection time:

```
second minute hour day_of_month month year
```

For example, `0 20 10 ? * *`. For more information about specifying the parameter values, see Section 10.3, "Understanding the Cron Expression for a Custom Interval of Collection," on page 110.

6 (Optional) To see a list of the first 10 scheduled runs, select **Preview**.

7 To ensure that the schedule runs, select **Active**.

8 Save the schedule.

10.2 Monitoring Scheduled Collections

The **Data Sources > Schedules** page provides an overview of each scheduled collection. You can find the times for the most recent and next activity of the collection. If a scheduled collection is inactive, Identity Governance displays the collection in a gray field.

To observe the details of a scheduled collection, select its name. Identity Governance lists the settings for the collection. You can modify the settings, such as adding and removing sources. Alternatively, you might want to deactivate the scheduled collection. If you modify the settings, ensure that you save the change.

To review the details for a recent run of the specified collection, select the run. Identity Governance indicates the success and time of collection and publication for each data source. If you select a data source, Identity Governance takes you to the details page for that source or an overview, if a group of sources. For example, if your schedule collects data from all identity sources, Identity Governance displays the **Identity Sources** overview page.

10.3 Understanding the Cron Expression for a Custom Interval of Collection

Identity Governance uses a cron expression to create the custom schedule. The cron expression is a string of parameters in the following syntax:

```
second minute hour day_of_month month year
```

For example:

```
0 20 10 ? * *
```

Use the following values to specify the parameters in the expression:

n

Specifies a numeric value for the parameter. For example `12` for `day_of_month` or `2015` for `year`.

*****

Specifies that the parameter uses all available values. For example, to run at 10:20 AM every day in July 2015, specify `0 20 10 * 7 2015`.

-

Specifies a range of values. For example, to run the collection during consecutive months, specify `0 20 10 ? MAR-OCT *`.

/

Specifies that you want to run the collection at a particular interval. Use the following syntax: `first_instance/increment`. For example, to run the collection on the first day of the month and every third day after, specify `0 20 10 1/3 * *`.

?

Applies only to `day_of_month`

Specifies that `day_of_month` does not have a specific value. For example, to run the schedule at 10:20 AM on any day of May, specify `0 20 10 ? MAY *`.

L

Applies only to `day_of_month`

Specifies that you want to run the collection on the last day of the month. For example, `0 20 10 L * *`.

To specify multiple values for a parameter, use commas. For example, to run the collection every six hours at specific days during specific months, specify `0 0 0/6 5,7,21,24 MAR-JUN,OCT *`. The schedule runs on the 5th, 7th, 21st, and 24th days of March, April, May, June, and October. This example also combines values to specify the month: `MAR-JUN,OCT`.

11 Creating and Managing Data Policies

Data policies and controls can help you prove to auditors and internal risk management partners that the data collected and published into the Identity Governance catalog is complete and accurate. Having data policies and controls in place can promote confidence in your data collection processes, help you with decision support, and show others that your processes and configurations comply with a set of standards.

11.1 Understanding Data Policies

Administrator with Customer, Global, or Data administrator authorizations can use data polices to make informed governance decisions. They can use default data policies or specify criteria and create additional data policies to generate collection and publication details or monitor identity life cycle events. Data policies enable administrators to:

- Detect data with specific conditions such as permissions with permission assignment end date as today or accounts with privileged account status
- Monitor identity life cycle events such as employees who join or leave the company, as well as those who move to a different department or location, or changes job title or supervisor.
- Detect anomalies or inconsistencies in the published data such as detect users without supervisors or permissions with risk > 100
- Generate statistics such as number of groups in collected data or number of permissions without owners
- Monitor changes to specific attribute values such as cost or risk
- Monitor whether any attribute was changed
- Monitor changes to entities such as 25% increase in number of accounts or number of users added to the catalog since last collection or publication
- Monitor technical role assignment changes such as addition or removal of detected or assigned users, role permissions, and role owners

- Initiate remediation action for anomalies or inconsistencies such as email alerts, micro certification, change request, or workflow process
- Compare collection and publication details from the same data source at two different full collection or publication times

Scenario 1: To discover accounts that are not being used actively, an administrator can create an account data policy and specify that the policy should detect any accounts that have a last logged in date which is earlier than a desired time period and that an immediate micro certification review should be done for these accounts.

Scenario 2: To detect permissions that are being inherited in applications, an administrator can create a permission assignment data policy and specify that the policy should detect application permission and add condition that the permission assignment type should be inherited. To narrow results they can add other conditions such as permission name, permission unique application ID, or permission risk. Administrators can also trigger change requests for these inherited permissions if needed.

Scenario 3: To detect any changes to user attributes, permission attributes, or account attributes, an administrator can create a publication data policy that includes a condition that specifies whether a user, permission, or account attribute was changed in any way.

Scenario 4: To detect users who have joined the company, left the company, or changed departments, and call a workflow process to remediate the data policy violation, an administrator can use one of the following default data policies, then select an existing **Workflow** as the **Remediation/Action Type** to address the detected life cycle event as needed:

- Deactivated identities in last 24 hours
- Identities Created in last 24 hours
- Identities Started in last 24 hours
- Title, Department, Location, Supervisor changes

NOTE: Only one workflow process runs for each detection. You can view the workflow process in the **Detected Items** column for the specific data policy on the **Publication Data Policies** tab.

11.2 Understanding Data Policy Detections

Detections of policies and controls can be triggered by manually running detections, by predefining a schedule, or by specifying events. Authorized administrators can specify collection, publication, and user curation as the events that trigger detections.

Based on the data policy, administrators can define remediations for violations. The number of detections will vary depending on event types and factors such as:

- Frequency of the events

  For example, when you select user curation, each user curation will trigger a data policy detection. In the case of two curations with very little interval between them, two detections will be started sequentially. This might result in zero violations or a fewer number of violations because the previous detection might have already calculated it as a violation and saved that record to the database.

- Remediation status

  The Last Detected Items and Open Items columns on the Data Policy Collection or Publication tabs might not present the latest counts when remediation runs automatically after detection. Remediation takes time to process and update counts. For example, if 10 items were detected and remediated automatically after detection, then it will be 10 last detected items and 0 open items after a remediation run. If remediation was not set, then it will be 10 last detected items and 10 open items. If 2 of the detected items were resolved manually, then it will be 10 detected items and 8 open items.

- Processing time of Identity Governance calculations

  For example, when you manually run a technical-role-changes data policy after adding or removing entity types such as owners or permissions from a technical role, the number of detections might be inaccurate, if the technical role calculations had not completed. However, when you configure the data policy to be triggered automatically by the technical role detection event, the number of data policy detections will be accurate and remediation will run correctly.

Authorized administrators can delay data policy detections and remediation runs that are automatically triggered after User, Permission, or Account curation using `com.netiq.iac.datapolicy.detection.trigger.delay.minutes` and `com.netiq.iac.remediation.run.delay.minutes` configuration properties. Note that these properties should be in minutes.These properties will not impact variations in number of detections caused by calculations in progress such as technical role calculations. You must wait for the calculations to be completed before triggering detections.

We recommend that you periodically refresh your page for more accurate counts of the last detected items and open items on the Data Policy page. You can view all previous detections by editing a policy and clicking **Show All Detections**. You can also view the most accurate count of all open and resolved items by clicking the data policy name, then clicking **Show open and resolved items**.

11.3 Creating and Editing Data Policies

Identity Governance provides default collection data policies and publication data policies. In addition, it enables you to create and edit data policies.

To create and edit data policies:

1. Log in as a Global or Data Administrator.
2. Select **Data Administration > Policies and Controls**.
3. (Optional) Click the gear icon to customize display settings for collection and publication data policies. For example, you could choose to display Analysis Type column.
4. In the **Collection Data Policies** or **Publication Data Policies** tab, select **+** to create a new policy.
5. Select the type of metric you want to run:
   - **Any attribute changes** to detect any changes to a selected attribute value.

     For example: If you want to start a user profile micro certification when the “Supervisor” attribute for a user changes, select **Identity** as the **Data Source Type**, then configure the criteria to **User: Supervisor**, then select **is changed**.

NOTE: Even though you can create and edit data policies at any time in your governance processes, we recommend that you create policies that use Any Attribute changes metric immediately after installing Identity Governance. If the policy is created later when there is existing data, the policy will look at the data from the beginning of time to current time and find all instances of changes to the attribute. To set the current data as the baseline, define the policy without specifying remediation, run the policy, resolve all the violations manually, then configure remediation.

- **Attribute changes with criteria** to monitor changes to attribute values based on your specified criteria in published data.

  If you configure only **Entities which changed to match the following criteria**, the simple criteria policy returns all entity types that match the criteria.

  For example: “All users whose location is Boston.”

  You can **Add optional criteria** to this data policy to configure **Entities which changed from the following criteria** and narrow the results to list only changes from a specified value.

  For the previous example: If you also configure the optional criteria to specify users whose location changed from Chicago, the policy returns only “Users currently located in Boston who previously were located in Chicago.”

- **Criteria** to detect and monitor user, permissions, or accounts based on your specified criteria in collected or published data.

NOTE: Data collection policies use only collected values, and exclude curated values from the policy. To include data for extended attributes, you must first collect that data.

- **Entity changes** to detect changes such as addition or removal of entities such as identities, accounts, and permissions, and permission assignments, or monitor changes based on the number of entities in collected or published data.
- **Statistics** to detect the number of specified entities such as users, groups, permissions, or accounts in collected or published data.

NOTE: You cannot calculate violations for these types of statistics and the number of entities is displayed in the **Data Sources > Activity** page.

- **Technical role changes** to detect changes such as addition or removal of detected or assigned users, role permissions, and role owners, or monitor changes based on the number of entities.

6 Select detection type such as violation or event.

7 Select trigger method for detections.

  7a (Conditional) When selecting events as trigger, select one or more events.

  7b (Conditional) When selecting schedule, if you had not previously created a schedule, create a schedule after saving the data policy.

8 Select the desired data source type, analysis type, entity type, and operation for the policy, and specify additional criteria. The required selections will vary based on the type of metric you selected in Step 5 on page 115.

NOTE: When specifying criteria, press Enter after typing a value for it to be included as a parameter in data policy analysis and calculations.

8a (Conditional) If you select entity analysis type and choose to analyze permissions and account changes in application sources or to analyze user changes in identity sources, add and remove respective data sources as needed to expand or constrain analysis.

TIP: When selecting dates, in addition to selecting a specific date using the date picker, you can also create date formula that calculates the date based on your criteria.

9 (Optional) Click **Estimate impact** when available to show estimated violations for the policy.

10 Save your settings.

11 Select **Data Administration > Policies and Controls**.

12 (Optional) Select the policy, then select **Edit** to edit the policy.

13 (Optional) Click **Show All Detections** to view previous detection instances.

11.4 Scheduling Data Policy Calculations

After creating data policies, you can schedule data policy calculations or calculate data metrics including violations on demand.

To schedule data policy calculation:

1 Log in as a Global, Review, or Data Administrator.

2 Select **Data Administration > Policies and Controls**.

3 Select **Schedule** tab, add or remove appropriate policies, and set the schedule.

NOTE: By default, all data policies will be included in the scheduled detection process. However, once you remove a policy from the schedule, Identity Governance will detect anomalies (violations) only for the policies included in the schedule. To detect violations of other policies, you can either manually calculate policy violations or add the policy to the schedule.

4 Select **Active** and then select **Save** to activate the schedule.

11.5 Manually Calculating Publication Data Policy Metrics

In addition to scheduling data policy calculations, you can also manually calculate publication data policy metrics including violations. Collection data policies cannot be run manually and need to be scheduled.

To manually calculate data policy violations:

1 Log in as a Globalor Data Administrator.

2 Select **Data Administration > Policies and Controls**.

3 Select **Publication Data Policies** tab.

4 Select one or more policies, and then select **Actions > Calculate Policy Violations**.

NOTE: You can cancel calculations in progress by selecting **Cancel** next to the progress status.

5 Observe numbers of violations and click the number to view the list of violations with additional information such as violation detection time, and last action performed on the item.

11.6 Comparing Collections and Publications

Identity Governance supports both partial and full collections and publications. Full collections are collections that collect all raw data and transform the data whereas partial collections collect only the changes since the last collection and do not transform the data. Partial or change events collections and publications, collect and merge changes. To determine changes between each collection whether full or partial, check the status of a collection or publication on the Data Sources page. Optionally, enable syslog to log all events in the database, and access the history records in the database.

To prove or verify that you have complete and accurate data, by comparing full collection and publication details from the same data source at two different collection or publication times, use the default data policies or create additional data policies and compare the results on the Data Activities page.

To compare full collections and publications:

1 Select **Data Sources > Activity**.

2 (Optional) To focus the list on a specific time period, select the calendar icon.

3 (Optional) To show a longer list, change the number of rows per page.

4 To quickly compare a collection or publication with the previous collection or publication, select the item from the **Date and status** column.

5 (Optional) In the comparison view, to view or open the applicable data policies, complete the following:

- **5a** Select the Refine comparison options gear icon.
- **5b** Select or clear listed policies to change your comparison results.
- **5c** Select **Edit Policies** to open the **Data Administration** > **Policies and Controls** page.

6 To compare two collections or publications from non-consecutive times:

- **6a** Group data sources.
- **6b** Select a data source name to view list of activity.
- **6c** Select two listed collections or publications using the check boxes.
- **6d** Click **Compare**.
- **6e** View changes and select links to view additional information about the changes. For example, if the number of changes is not zero, that number is a link. Selecting that link opens a quick view of the items that changed.

7 (Optional) Select **Overview** on the top navigation bar to view Data Policy Status details. For more information, see Section 32.7, “Viewing Policies and Controls Status, Violations, and Trends,” on page 385.

NOTE: The Governance Overview dashboard data summary numbers such as the number of permissions will not always match the number of collected and published objects in the Activity page. The Activity page shows the number of objects collected or published by Identity Governance. The Data Summary widget shows only the number of objects that are visible in the catalog. Based on your collector configuration, Identity Governance might exclude objects such as Users who are flagged as inactive or permissions objects that represent items like resource parameters from the catalog resulting in a different number of objects than the number of collected or published objects.

11.7 Manually Resolving Detections

Generally, you can define remediation when creating policies, then schedule a policy run. However, for publication data policies that detect any attribute changes, you can also manually resolve the detections.

To manually resolve Any Attribute Changes detections:

1. Click the number of open items.
2. (Optional) Set the maximum number of rows per page to 100.
3. Select specific items or select all items.
4. Click **Resolve**.
5. Repeat steps 3 and 4 on each page of open items.
6. Click the Refresh icon to refresh the list of open and resolved items.

11.8 Detecting and Remediating Violations in Published Data

Identity Governance enables you to check your collected and published data using data policies. In addition to looking at statistical information, you can also take remediation action for data policy violations (anomalies) in published data by:

- Sending an email notification
- Reviewing items in violation by creating a micro-certification review instance
- Creating a change request
- Creating a workflow

NOTE: Workflow remediation can only be utilized for publication policies where the entity type is User. Workflow remediation is not an option for publication policies for Account or Permission entity types.

Once a micro certification is complete, a change request is fulfilled, or a workflow is executed, you can select one or more publication data policies and **Actions** > **Run Policy Detection** to recalculate the number of data policy violations. For more information about micro certification and fulfillment, see Section 25.2, “Understanding Micro Certification,” on page 340 and Chapter 15, “Instructions for Fulfillers,” on page 175.

If, after the initial remediation type selection, administrators would like to change the remediation type for future violations then they can select the link under the Remediation column on the Data Policy page and edit the remediation setup. Note that the last remediation event is listed below the name in the Remediations column.

To remediate data policy violations:

1. Log in as a Global or Data Administrator.
2. Select **Data Administration > Policies and Controls**.
3. Select the **Publication Data Policies** tab.
4. Select **+** to add a remediation action to a violation.
5. (Optional) Enable **Run Remediation on new violations when calculated**.
6. Specify a name for the remediation.
7. Specify and configure one of the following Remediation/Action types:
   - If you selected **Email Notification**:
     - Select **Email source**.
     - Specify a user, group, or role (such as supervisor or permission owners) as the recipient of the email. If a role has no user assigned to it, then email will be sent to Data Administrator. If a user has not been assigned as a Data Administrator, then the email will be sent to the Global Administrator.
   - If you selected **Change Request**, select violation types, and provide instructions for fulfilling the change requests generated for selected violation types. Based on your policy type, additionally, select **Modify** or **Remove**.
   - If you selected **Micro Certification**, configure the following settings:
     - **Review Definition**: Search and select a review definition from the selection dialog or specify the review definition name. Note that Identity Governance applies filters based on data policy and enables the selection of only relevant review definitions.
     - **Review Name**: Specify a name for the micro certification.
     - **Start Message**: Specify the message that will be displayed in the header area of reviews describing why the review was started.
     - **Review Period**: Leave this blank if you want to use the duration specified in the review definition. Otherwise, specify a duration.
   - If you selected **Workflow**, based on your violation, search for, and specify, an existing workflow.

     NOTE: If no existing workflow is relevant for the current data policy violation, a Workflow Administrator has the option here to click **Create Remediation/Action Workflow** and provide the requested information to create a workflow that remediates the data policy violation.

     ---
8. Save and apply the remediation.
9. Repeat the above steps to add multiple remediations.
10. Run individual or multiple remediations.
    - **10a** To run all the specified remediations, select **Actions > Run Remediation/Action**.
    - **10b** To run individual remediation, hover over a remediation name, then click **Run**.

11 (Optional) Hover over a remediation name, then click **Edit** or **Delete** as needed. Note that you can also directly run the remediation or delete a remediation from the Remediation settings window.

NOTE: If the remediation name specifies a workflow, you will see an additional option you can click to run the workflow.

If you selected **Create Remediation/Action Workflow** in Step 7 above, or if you want to edit an existing workflow, perform the following steps to open the Workflow Builder to create the remediation workflow:

1 On the Data Policies and Controls page, click the **Publication Data Policies** tab.

2 In the Remediations/Actions column, hover over the name of the workflow remediation you created in Step 7 above, and click **Edit**.

3 Next to the **Workflow** field, click **Edit**.

4 Use the Workflow Builder to create the remediation workflow for the data policy. For more information about creating workflows, see *Workflow Service Administration Guide*.

11.9 Monitoring Data Policy Detections and Remediations Results

Identity Governance enables authorized administrators to look at the progress and results of data policy detections. The application provides the ability to view all previous detection instances and monitor the results of data policy detections and remediations.

The data policy detection results will vary based on detection triggers, remediation status, and schedules. We recommend that you periodically refresh your page for more accurate counts of the last detected items and open items on the Data Policy page. To view more accurate counts and details about the detected, open, and resolved items, use the following procedure.

To monitor data policy detection and remediation results:

1 Log in as a Global or Data Administrator.

2 Select **Data Administration > Policies and Controls**.

3 In the **Collection Data Policies** or **Publication Data Policies** tab, to view the most accurate number of the last detected items and open items:

3a (Optional) View Statistic, Criteria, or Changes related policies by selecting respective option or options.

3b Click the number of open times to view the Open and Resolved Items window that displays last detected items, open items, and resolved items.

3c Alternatively, click on a policy name to view additional details, then

click **Show open and resolved items**.

11.10 Exporting and Importing Data Policies

Once you have created your data policies based on your business requirements, you can easily export the data policies and publication policies related review definitions as a zipped file and save it with your backup files. You can also use exported policies in another location or environment. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

12 Managing Data in the Catalog

The Identity Governance catalog contains all of the identities and permissions in your organization that you choose to collect. You use this information to create a unified identity for each person in your organization so you can review the permissions assigned to them.

To manage the Identity Governance catalog, you must have Bootstrap, Customer, Global, or Data Administrator authorization.

Identity Governance helps you create a unified identity for each user that combines all permissions that have been assigned by your identity and application sources. To build the unified identity, Identity Governance must know how to map incoming identity attributes. The catalog needs at least one identity source, such as Active Directory, and at least one application source. Otherwise, you cannot map identity attributes to permissions. When using a comma-separated value (CSV) file as a data source, the file must use UTF-8 encoding.

12.1 Configuring the Data Source for Post Authentication Matching

A user is a valid Identity Governance user when the user is authenticated by a One SSO provider (OSP) and has been mapped to a published Identity Governance catalog user. The post authentication mapping occurs based on the User Mapping configuration.

IMPORTANT: Identity Governance evaluates only collected attribute values for the authentication matching rules, not edited values. For more information, see “Changing the Values for Authentication Matching and Identity Governance Services” in *Identity Governance 4.3.1 Installation and Configuration Guide*.

You can also add your own custom attributes to the catalog. For example, if your data source is eDirectory, you must extend the schema for the catalog because eDirectory contains more attributes than are built into the catalog.

By default, all Identity Governance users must have the **LDAP Distinguished Name** attribute mapped in the attribute catalog. Identity Governance uses this attribute to authenticate users who log in to the application.

1. Log in to Identity Governance as a Globalor Data Administrator.
2. Select **Data Sources > Identities**.

3 Select the authentication server that you specified during installation.

4 Ensure that you have collected data from the data source and it is enabled for user view. For more information, see Section 2.3, “Assigning Authorizations to Identity Governance Users,” on page 27.

5 Scroll down to the **Collect User** or the **Collect Identity** section.

6 For **LDAP Distinguished Name**, specify the attribute in your identity source that you want to map to the login attribute for Identity Governance users.

For example, your identity source points to a container in Active Directory. Users log in to your network with an AD attribute called `username`. For **LDAP Distinguished Name**, specify the `username` attribute. Identity Governance maps `username` to the **LDAP Distinguished Name** attribute in the catalog.

7 (Optional) Map the other attributes in your identity source to the built-in attributes in the catalog.

8 (Optional) To add custom attributes, complete the following steps:

8a Select **Add Attribute**.

8b Specify the settings for the new attribute, and then select **Save**.

8c Specify an attribute from your identity source that you want to map to the new custom attribute.

8d Select **Save**.

9 (Optional) Add the new login users to authorizations in Identity Governance. For more information, see Section 2.3, “Assigning Authorizations to Identity Governance Users,” on page 27.

12.2 Understanding Identity, Application, and Permission Management

This section discusses changing identity, application, and permission information:

12.2.1 Managing Identity Information

Identity information includes:

- The attributes and relationships you collect through the identity collectors
- Status in Identity Governance, such as role assignments and risk factors
- Identity source information, such as the collector mappings, and curated and effective values for the identity attributes

To view or edit identity details:

1 Navigate to **Catalog > Identities** and select a user. For example, Lisa Haagensen.

2 View basic information about that user, and select **More** to see more details.

3 Select available tabs to view items such as group membership, role assignments, and source for the user information.

4 (Optional) Select the **Edit** icon next to the user.

5 Modify the available attribute values, and then select **Save**.

12.2.2 Managing Application Information

Application information includes:

- The application photo, name, and description
- The identities of the application owner and administrators
- The method for fulfilling changeset items

You can also specify the risk level for the application and whether reviews include the permission hierarchy of the application.

To manage the application information:

1 Navigate to **Catalog > Applications**.

2 Select the name of an application. For example, `Safe Financials`.

3 Select the **Edit** icon.

4 Modify the application settings, such as:

Risk

Specifies the importance of the application in terms of limited access and security.

For example, you might want to review access to applications with a **high** risk more often than applications with a **mild** risk.

Administrators

Specifies users who can access the Catalog and can manage data.

Tags

Specifies a string that creates a new tag or shows existing tags from another application that match the string.

Owners

Specifies a user who is responsible for reviews where the review definition references the Application Owner.

Show permission hierarchy in review

Specifies whether you want to see the permission that was assigned in a permission hierarchy of relationships when this application is included in a review.

Show account name in review and fulfillment details

Specifies whether you want to hide account names.

You can use this setting in review definitions as criteria for permissions to be included in the review. For example, if the collected accounts names are obscure names, you might not want to use them.

Permission ID for granting accounts

Specifies whether you want to use an autocompleter of permissions published in the system.

12.2.3 Reviewing Application Fulfillment Settings

Identity Governance allows you to specify a fulfillment target for each application. In the catalog, you can see the fulfillment settings for each application.

To review current fulfillment settings:

1. Log in to Identity Governance.
2. Under **Catalog**, click **Applications**, and select an application.
3. Under **Fulfillment Information**, view the fulfillment type and details.

For information about configuring fulfillment, see Section 14.2, “Configuring Fulfillment,” on page 157.

12.2.4 Managing Permission Information

Permission information includes:

- The permission photo, name, and description
- Identity of the permission owners
- The risk level for the permission

You can also observe permission relationships if the permission contains other permissions, has holders, or is part of Separation of Duties (SoD) policies.

When you save changes, Identity Governance displays an icon next to a changed setting. Select the icon to reset the setting to the originally collected value.

To manage permission information:

1. Navigate to **Catalog > Permissions**.
2. Select a permission.
3. Select the **Edit** icon.
4. Modify the permissions settings, such as:

   Risk

   Specifies the importance of the permission in terms of limited access and security.

   For example, you might want to review access to permissions with a **high** risk more often than permissions with a **mild** risk.

   Permission Owner

   Specifies one or more users responsible for reviews where the review definition references the Permission Owner.

   Hide Permission from Review

   Specifies whether you want to exclude this permission from reviews.

12.3 Editing Attribute Values of Objects in the Catalog

After you have published data, you can view the items, such as users and applications, along with their attributes, such as a user's phone number. Identity Governance attribute values are generally displayed as plain text. The **Description** field includes the option to display text in HTML. For example, when HTML or markdown elements are collected, curated, or entered when creating a permission, the description will render as HTML, and other fields will display as plain text in the catalog and within other functional areas such as reviews and policies.

To view the attributes of a specific item in the catalog, click **Catalog**, the type of data you want to view, and the object you want to view.

To edit attribute values individually, click the pencil icon for that item. Identity Governance displays any attributes that the Data Administrator has designated as editable, along with the current attribute value. When you edit the data, you override the originally collected content, and Identity Governance displays an icon next to the value to indicate the change. Any attribute that you edit will be persisted through subsequent collection and publication, even if the original value for the attribute changes. You can later reset the attribute value to its collected value. You can also associate tags, or metadata, so you can more easily identify the information when you create and perform a review.

To edit multiple attributes at the same time, see the following sections:

- Section 12.3.1, "Understanding Bulk Data Update," on page 128
- Section 12.3.2, "Configuring the Identity Governance Database Method for Bulk Update," on page 128
- Section 12.3.3, "Configuring the File System Bulk Update Method," on page 129
- Section 12.3.4, "Editing Attribute Values in Bulk," on page 130

NOTE: ◆You can edit only the attributes that are marked as editable.

- You cannot import attributes that have a different data type than the target system even when the attribute has not been collected.
- You can add new external attributes each time you collect data from a data source. However, after you publish the data for that collector, you cannot remove the attributes.
- When you specify a string type for a new extended attribute, Identity Governance always truncates the string at 2000 characters.
- You can reset only the attribute values that are collected. Attributes that are configured such as Last Account Review Date or Last Unmapped Account Review Date cannot be reset.
- If you edit any permission records to set the `excludeFromCatalog` attribute to `true`, the only way to see these records in the catalog again is to manually change the `permission` table value back to `false`. If bulk editing was used to set the `excludeFromCatalog` attribute to `true`, copy the Bulk Data Update CSV file that made the original edits, and change the edited value to `UNDO_CURATION`.

IMPORTANT: Identity Governance evaluates only collected attribute values for the authentication matching rules, not edited values.For more information, see "Changing the Values for Authentication Matching and Identity Governance Services" in *Identity Governance 4.3.1 Installation and Configuration Guide*.

12.3.1 Understanding Bulk Data Update

Before you edit attribute values in bulk, you must determine the bulk upload method you want to use, and a Global Administrator must have configured bulk update for that method. The available bulk upload methods are:

- **Identity Governance database:** The Global Administrator might use the Identity Governance Global Configuration feature or the Identity Governance Configuration Utility to configure the correct global property for this bulk update method.
- **File system:** The Global Administrator creates a bulk data update base folder, which contains the `input` and `output` subfolders, on the Identity Governance server, provides the Identity Governance service read/write access permission to the subfolders, generates access credentials, then specifies the parameters using Global Configuration, or the Identity Governance Configuration Utility.

12.3.2 Configuring the Identity Governance Database Method for Bulk Update

Before you can use the Identity Governance database to update attribute values in bulk, a Global Administrator must have configured the following properties using the Identity Governance Global Configuration feature or the Identity Governance Configuration Utility:

Base Folder

Identity Governance creates the CSV data template file in Identity Governance database and makes it available for you to download and edit.

Batch Size

(Optional) Specifies the maximum number of CSV data rows processed at one time. This option is useful for tuning the memory usage of the bulk update process. The default value is 1000.

To configure the base folder property:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration > Advanced**.
3. Search for the `com.netiq.iac.bulkdataupdate.csv.basefolder` property, then click the **Edit** icon.
4. In the **Value** field, type `DB://`.
5. Click **Save**.

To specify the number of CSV data rows processed at one time:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration > Advanced**.
3. Search for the `com.netiq.iac.bulkdataupdate.batchsize` property, then click the **Edit** icon.
4. In the **Value** field, type the number of CSV data rows you want to be processed at one time. The default is 1000.
5. Click **Save**.

12.3.3 Configuring the File System Bulk Update Method

To use this method, the Global Administrator needs access to the file system on the Identity Governance server. The Global Administrator must create a bulk data update base folder that contains the `input` and `output` subfolders, provide the Identity Governance service read/write access permission to the subfolders, generate access credentials, then configure the following properties using the Identity Governance Global Configuration feature or the Identity Governance Configuration Utility:

Base Folder

Identity Governance creates the CSV data template file in the `output` subfolder, and you must copy the updated file to the `input` subfolder.

Batch Size

(Optional) Specifies the maximum number of CSV data rows processed at one time. This option is useful for tuning the memory usage of the Bulk Update process. The default value is 1000.

To configure the base folder property:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration > Advanced**.
3. Search for the `com.netiq.iac.bulkdataupdate.csv.basefolder` property, and click the Edit icon.
4. In the **Value** field, type the path for the bulk update folder. For example, `/ig/bulkupdate`.
5. Click **Save**.

If you want to specify the number of CSV data rows processed at one time:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration > Advanced**.
3. Search for the `com.netiq.iac.bulkdataupdate.batchsize` property, and click the Edit icon.
4. In the **Value** field, type the number of CSV data rows you want processed at one time. The default is 1000.
5. Click **Save**.

When you copy the CSV file to the `input` folder during the process for Editing Attribute Values in Bulk, Identity Governance changes the file extension as it processes the file. Here are the different extensions and processes the file goes through during the bulk process:

File Extension Name	Process
`.csv`	Identity Governance starts the bulk process. It is the name on the file when you add it to the `input` folder.
`.ph1`	Phase 1 of the bulk process.
`.fail`	If the bulk process fails, the file name becomes `.fail`.
`.done`	If the bulk process succeeds, the name becomes `.done`.

12.3.4 Editing Attribute Values in Bulk

You can edit *attribute values* for multiple objects at the same time by importing the data into Identity Governance using a CSV file. For example, you might want to add photos for users in the catalog. When adding multiple values to a single attribute, separate the values with the pipe sign (|).

NOTE: When importing a bulk update file, ensure that the file matches a bulk update policy in the system. The generated bulk file that the user edits has an ID in the file that must match a bulk update policy in the system. In addition, that policy must have the same attributes, decision context attributes, and mapping attributes. If the ID and attributes do not match, the bulk update will be rejected.

To edit a number of attribute values:

1. Under **Data Sources**, select **Identities** or **Applications** depending on the type of data you want to edit.
2. In the upper right, select **Bulk data update**.
3. Click **+**.
4. Specify all the mandatory fields.
5. Click **+** next to **Attributes to update** and select the attributes.
6. (Optional) Click **+** next to **Decision context attributes** and select the attributes that will provide context for update decisions.
7. (Optional) Click **+** next to **Mapping attributes** and select the attributes that will be used to identify Identity Governance users by attribute values from other systems.
8. (Optional) Click **+** next to **Attributes to update** to select the attributes you want to update in bulk.
9. Save your settings.
10. Click the **Generate bulk update template now** icon.
11. (Conditional) If bulk update is configured to use the Identity Governance database method to generate a CSV template file, perform the following steps:
    - **11a** On the Identity Governance menu bar, click the **Your Downloads** icon.
    - **11b** On the Your Downloads window, select the template you generated, then click the download icon to download the template to the browser Downloads folder.
    - **11c** Open the browser download folder, then open the CSV template file.
    - **11d** Make any necessary changes, then save the file.
    - **11e** Click the Identity Governance upload icon.
12. (Conditional) If bulk update is configured to use the file system method to generate a CSV template file, perform the following steps:
    - **12a** Log in to the Identity Governance server, and locate the `output` subfolder of the bulk update folder.
    - **12b** Edit the CSV template file as needed.
    - **12c** Copy the CSV template file to the `input` subfolder.

    Identity Governance automatically detects updated files and applies the updated information to your data.

NOTE: If you have a large data set, the CSV template file could take longer than expected to generate and upload.

You can also undo an edited value or explicitly set a value to null. Identity Governance recognizes certain keywords in cells that perform specific actions:

- **UNDO_CURATION:** Removes any previously edited values for this attribute.
- **SET_NULL:** Sets the appropriate null or empty value on this attribute.

After you perform the bulk attribute update action, you can verify the changes by selecting **Catalog** > **Identities** or **Catalog** > **Accounts** to see if the attribute changes you made appear in the Catalog.

12.4 Searching for Items in the Catalog

Identity Governance provides several ways to find the information in your catalog. All catalog tables support a quick lookup of items by name or description. Some catalog tables also support an advanced filtering capability where users can build complex expressions based on searchable attributes. These complex expressions allow users to add attribute conditions to the search criteria or to add sub-expressions, known as filters, which can contain attribute conditions as well as other filters to refine the search results. Users can also save these filters for future searches. Both the quick lookup and filter expressions search are limited to a specific table. Insight Queries provide flexibility in searching for entities in your system, including searching across entity relationships.

- Section 12.4.1, “Supported Wildcards and Handling Wildcards as Literal Characters,” on page 131
- Section 12.4.2, “Searching within Catalog Items,” on page 133
- Section 12.4.3, “Using Advanced Filters for Searches,” on page 134

12.4.1 Supported Wildcards and Handling Wildcards as Literal Characters

Identity Governance supports the following wildcards in searches and advanced filtering:

- Underscore (_) for single characters
- Asterisk (*) and Percent (%) for multiple characters such as any sequence of zero or more characters

NOTE: The behavior of the wildcards differs based on the type of database and location of the search field or advanced filter. For example, PostgreSQL does not support wild cards for `equal` operations, but it does support wild cards for `like` operations.These wildcards are not supported in typeahead controls.

Table 12-1 *Examples of Valid Wildcards for Advanced Filters and Insight Queries*

Type	To Find
%	All results
*	All results
an%	All results that contain “an”
an*	All results that contain “an”
a_i	All results that have an “a”, followed by any character, then an “i”

You can also use other wildcards and expression capabilities supported by backend databases when searching Identity Governance entity tables. Identity Governance passes them in the search string to the databases. Refer to your database documentation for details about these additional wildcards and expressions.

When using these wildcards as literal characters, you must precede the special character with an escape (\) character in searches and advanced filtering when using the following operators:

- `contains`
- `starts with`
- `ends with`
- `matches`

You must also precede the wildcards with \ when using typeahead searches.

Operators in advanced search values such as `equal to` or `not equal to` do not need to be preceded by an escape character.

Table 12-2 *Examples of Special Character Usage in Search Strings*

Type	To find
%Admin%	Results that contain Admin, such as Administrative Assistant or Global Administrator.
J_n	Entities where the first character is J and the third character is n, such as Jane Smith or Brad Jones.
Jo\%Doe	Entities that match Jo%Doe, such as Jo% Doe or Jo%Doe Admin.
Acct_AD	Entities that match Acct_AD, such as Acct_AD_01 or Acct_AD Admin.

12.4.2 Searching within Catalog Items

You can search for specific items in the catalog by selecting the type of item under **Catalog**, such as **Users** or **Groups**. Then type your search criteria in the search box, and select the search icon.

Identity Governance attempts to complete your search entry as you type. To ensure that users can more easily find a group, always include a description of the group that matches what users might use as a search term. For example, "Finance Team" for your financial group.

You can add additional criteria to the search by clicking the filter icon, where available, and using the expression builder. The expression builder gives you the ability to use AND, OR, and NOT expressions with the additional search criteria. You can save and reuse filters that you have defined.

The application or owner control provides a type-ahead feature to select applications or users in the system. Searching for applications, groups, or users requires selecting the catalog item.

TIP: You can configure the application wait time in milliseconds after the last time you press a key and before the application performs a typeahead search by selecting **Configuration > General Settings > Typeahead Delay**.

The attributes that appear in the refinement list are fixed for Technical Roles. However, you can configure them for other catalog items.

To add or remove user attributes from the refinement list:

1. Select **Data Administration** and then select the type of catalog item, such as **Identity Attributes**.
2. Select an attribute to edit the attribute definition.
3. Select the desired searchable option for the attribute to have it displayed in the catalog or not:

   Available in catalog searches. Change takes effect after publication.

   Select this option to enable the attribute for quick searches. If the option is selected, the attribute is available in the catalog list for searches. This means the search is performed against this column even if this column is not shown in the catalog list.

   Display as refine search option

   Select this option to enable the attribute for advanced searches.

   Display in review item selection criteria

   Select this option if you want to display the attribute in review items. For more information, see Section 25.1.4, “Adding Selection Criteria for Review Items,” on page 329.

   Display in business role selection criteria

   Select this option if you want to display the attribute when creating a business role membership expression. The membership expression contains the search criteria for membership in a business role.
4. Select **Save**, then publish the changes to the catalog.

12.4.3 Using Advanced Filters for Searches

Where available in Identity Governance, you can add additional criteria to searches by clicking the filter icon and using the expression builder. The expression builder gives you the ability to use AND, OR, and NOT expressions with a set of attribute conditions or sub-expressions and filters that can be used to filter the result set based on specific values. The expression builder also calculates date based on the provided date formula.

If you have filters you want to reuse in your environment, Identity Governance helps you manage these filters. Except for Insight Queries, you can save these filters and edit or delete them as needed for searches, such as identities, permissions, roles, and policies.

For more information, see Chapter 5, “Using Advanced Filters for Searches,” on page 59.

12.5 Analyzing Data with Insight Queries

Identity Governance provides the ability to query data interactively by using Insight Queries. You can query the catalog across entity types, such as finding all users that have access to a certain permission. You can also query compliance activity and other information such as finding all users who have outstanding revocations.

To access Insight Queries, you must have one of the following authorizations:

- Global,Data, or Governance Insights Administrator
- Auditor

Insight queries are interactive, allowing you to change query options and update results without having to open a new window each time. You can download queries and import them and you can also download results of the queries. You can also create custom metrics using a query to populate the SQL statement and the metric columns fields. For more information about custom metrics, see “Creating Custom Metrics” on page 377. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

To create Insight Queries:

1. Log in as a Global, Data, or Governance Insights Administrator or Auditor.
2. Select **Catalog** > **Governance Insights**.
3. Select the **+** icon to create a query.
4. Specify the desired search criteria. The criteria includes a set of entity types, cross references, and additional filters that can be used to filter the result set based on specific entity type.
   - **4a** Select an entity type. For example, for queries related to fulfillment requests, select Change Requests. For queries related to identities, select Identities.
   - **4b** (Optional) Add a cross-reference filter. Cross-reference filters are relationships between the selected entity type being searched and other entities in the system. You can limit the query based on the specified filter using the **with** option or use **with or without** option to expand the search. For example, if you are searching for identities and want to only find all identities that are included as members of business roles, then add **with** Business Role Inclusion as a cross-reference filter. If you want to find users who might or might not have violated a Separation of Duty policy, then add **with or without** Violating SoD cross-

reference filter. For a detailed list of cross-reference filters, see the *Identity Governance Insight Query Technical Reference* (https://wwwtest.microfocus.com/documentation/identity-governance/4.3/tech-refs/Insight_Query_Technical_Reference.pdf).

4c (Optional) Select the filter icon to add attribute conditions and sub-expressions using the expression builder. For example, if you are searching for identities with a specific Title attribute, then add a condition specifying Title equal to the desired value, such as Reviewer.

NOTE: When searching for attribute values to include as search criteria, you can use the typeahead feature to select a value from the current catalog that matches your criteria, or type a partial string and press Enter. For information about supported wildcards, see Section 12.4.1, “Supported Wildcards and Handling Wildcards as Literal Characters,” on page 131.

---

5 Select the columns (attributes) to include in the results. The column order for the results matches the order you specify, and you can drag and drop the listed columns to change the order of display.

Default columns display automatically in the selected column list when changing the searched entity type or when adding a cross-reference filter. Columns associated with a cross-reference filter are also automatically removed from the selected column list when you remove the reference filter.

6 (Conditional) When querying large data, download the results to a CSV file.

Use the Download option instead of running the query to optimize performance and avoid the query from timing out and displaying an error even though the query ran successfully in the background. Download again when you change the query options.

7 (Optional) Select the Run icon to see query results on the Insight Query page. If you experience a connection timeout in the browser, this may be due to a large result set. Downloading the results to a CSV will avoid the timeout and allow you to view your data. You can also try and change the query options, then select the Run icon to update the results.

8 Select the Save icon to save the query.

If you include columns that contain multi-valued attributes, the query results contain multiple rows for those columns.

Identity Governance combines duplicate rows in the query results lists to avoid showing many rows with same value. For example, a query of identities on the Title attribute lists only one row for each title in your catalog, even though multiple identities might share the same title. In Oracle environments, the following object types and attributes do show multiple rows in the query results if you select any of them as a column:

- User: Geo Location
- Access Request Item: Change Item Comment
- Change Item Action: Item Comment

12.6 Downloading Catalog Entities

You can download the identities, accounts, groups, and permissions in the catalog as CSV files. All the columns displayed in the table will be downloaded. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

13 Database Maintenance

Identity Governance maintenance and archiving features allow Global, Data, Maintenance, and SaaS Ops Administrators to archive data, to clean up old and unused data, and to schedule maintenance. Use these features to maintain and monitor your data. For more information about Identity Governance authorizations, see Chapter 2, “Adding Identity Governance Users and Assigning Authorizations,” on page 19.

WARNING: You must have an effective data cleanup, archiving, and maintenance strategy. You must cleanup your operations database, create external archive destinations, schedule maintenance, and rename and rotate archives. Not following these database maintenance requirements and data retention recommendations outlined below will result in performance issues and you will not have historical data.

We recommend that you keep all your operations data for 30 days except for review instances and request data. We recommend that you keep your review and request instances for 90 days and archive every week. However, adjust specific timeframes and your archiving and maintenance strategy based on your system requirements, scope of governance activities, data dependencies, and data analytical and maintenance requirements.

For more detailed information about Identity Governance capabilities and procedures, see the following sections:

13.1 Understanding Database Maintenance

The operations database maintains a history of activities that occur in Identity Governance. For example, as part of the data collection process, the database stores the previous state of that collection to ensure that Identity Governance can return to that state if an error occurs. Over time, however, the size of the operations database increases with each new collection, publication, review, and other operations. This can have an adverse effect on the performance of some database queries, because they have to filter through more and more irrelevant historical data. Identity Governance includes the **Database Maintenance feature**, which allows Global, Data, or Maintenance administrator to archive older data in a separate archive database, then cleanup historical information from the operations database.

The Database Maintenance feature provides the following:

- Displays running summaries of database updates and items that can be purged

- Allows you to drill down to more specific data from summary items
- Shows categorized lists of archive and cleanup activities
- Allows you to cancel a running archive
- Allows you to select specific cleanup entities to purge
- Allows you to resume a canceled or otherwise disrupted scheduled archive
- Shows the latest complete archive details
- Allows you to start the database maintenance process, with optional database cleanup
- Allows you to run cleanup in the background concurrently with other operations such as reviews, data collection, and data publishing when archiving is disabled
- Allows you to schedule maintenance

When performing database cleanup, Identity Governance searches the operations database for purgeable items that are older than the number of retention days you specified. If you do not specify a number of retention days, Identity Governance cleans up anything that can be purged. It will not purge data that is still in a state where it might be needed for current operations. For more information about how Identity Governance decides which items can be purged, see Section 13.6, “Identifying Purgeable Data,” on page 147. If archiving is enabled, data is archived to the archive database before it is purged from the operations database. Database cleanup will not occur if an archive fails to complete. You can disable archiving to bypass this restriction and to run cleanup in the background while performing other user tasks.

IMPORTANT: Disabling the archive feature purges all your data from the Identity Governance archive database. Be sure you back up your data in your archive system before you disable the archive feature. For more information about disabling archiving, see Section 13.4, “Disabling and Enabling Archiving,” on page 144.

When you start database maintenance, Identity Governance selects, by default, the option for concurrent archiving, which allows archiving to occur while operations — such as collections, publications, scheduled processes, and starting reviews — are in progress. If you clear this selection, Identity Governance does not begin archiving until those operations are complete or are idling cleanly, and no new operations will start while archiving is in progress. Identity Governance operations automatically resume when archival tasks are complete or canceled. In addition, Identity Governance cannot update the operations database while an archive is in progress. Clear the selection only if you want to ensure that all updates to the operational database made by normal Identity Governance activities are archived to the archive database, and nothing is purged from the operations database until it has been properly archived.

If the **Recent Archival Activity** section lists an archive that was canceled or otherwise interrupted, you can click **Start Maintenance**, then select **Resume archive** on the Maintenance Options window to have the archive task resume from the point of interruption. Scheduled database maintenance allows you to configure concurrent archiving to automatically resume an archive that is canceled or otherwise interrupted.

NOTE: You may resume canceled or interrupted archive tasks only for concurrent archives.

An administrator has the ability to cancel archive and clean up tasks while they are running. Usually, both archive and cleanup tasks run automatically, one after the other, and when they are complete, normal Identity Governance operations automatically resume. However, an administrator may also

choose to pause after the archive phase, after the cleanup phase, or both. If you choose to pause after the archive phase, you must manually resume and continue to the cleanup phase or cancel the cleanup phase and return to normal operations. If you choose to pause after the cleanup phase, you must manually return to normal operations. These optional pauses give administrators opportunities to suspend Identity Governance maintenance at key points and do other maintenance tasks they may deem important before proceeding. For example, they want to look at the database, copy the database, troubleshoot issues, and so forth. The recommended and default mode of operation for maintenance is to allow Identity Governance to automatically move through the maintenance phases and then automatically return to normal operations.

13.2 Understanding Archive Destinations

Identity Governance allows you to archive data to an internal database or to an external database. Identity Governance automatically creates the internal database (`igarc`) at the time of installation, and that database is the default for archiving. We recommend that you use the default archive only in development environments. In your test (stage) and production enviroments, archive data to an external database, and rotate these archives as needed. Identity Governance supports the following databases as archive destinations:

- Vertica
- Oracle
- PostgreSQL
- MS SQL

NOTE: Identity Governance does not create reporting views for external databases. If you configure an external database as an archive destination, the view will contain only partial information.

- Section 13.2.1, “Before You Create an Archive Destination Using SSL Communication,” on page 139
- Section 13.2.2, “Creating an Archive Destination,” on page 141

13.2.1 Before You Create an Archive Destination Using SSL Communication

If you want to create an archive destination and configure the database to use SSL communication, you must first create and configure the proper global configuration properties for your data store type and for the SSL type -- server authentication or mutual authentication. Use the table below to determine which configuration properties you need to create and the values for each.

Table 13-1 *Global Configuration Properties and Value Types for Database and SSL Types*

Database Type/SSL Type	Configuration Property	Value Type
Vertica/Server	com.netiq.iac.vertica.ssl.truststore.path	Filename
Vertica/Server	com.netiq.iac.vertica.ssl.truststore.password	Password
Vertica/Mutual	com.netiq.iac.vertica.ssl.truststore.path	Filename

Database Type/SSL Type	Configuration Property	Value Type
Vertica/Mutual	com.netiq.iac.vertica.ssl.truststore.password	Password
Vertica/Mutual	com.netiq.iac.vertica.ssl.keystore.path	Filename
Vertica/Mutual	com.netiq.iac.vertica.ssl.keystore.password	Password
Oracle/Server	com.netiq.iac.oracle.ssl.truststore.path	Filename
Oracle/Server	com.netiq.iac.oracle.ssl.truststore.type	Type of truststore
Oracle/Server	com.netiq.iac.oracle.ssl.truststore.password	Password
Oracle/Mutual	com.netiq.iac.oracle.ssl.truststore.path	Filename
Oracle/Mutual	com.netiq.iac.oracle.ssl.truststore.type	Type of truststore
Oracle/Mutual	com.netiq.iac.oracle.ssl.truststore.password	Password
Oracle/Mutual	com.netiq.iac.oracle.ssl.keystore.path	Filename
Oracle/Mutual	com.netiq.iac.oracle.ssl.keystore.type	Type of truststore
Oracle/Mutual	com.netiq.iac.oracle.ssl.keystore.password	Password
PostgreSQL/Server	com.netiq.iac.postgres.ssl.root.cert	Contents of the certificate **NOTE:** Do not use a filename.
PostgreSQL/Mutual	com.netiq.iac.postgres.ssl.root.cert	Contents of the certificate **NOTE:** Do not use a filename.
PostgreSQL/Mutual	com.netiq.iac.postgres.ssl.client.cert	Contents of the certificate **NOTE:** Do not use a filename.
PostgreSQL/Mutual	com.netiq.iac.postgres.ssl.client.key	Contents of the key **NOTE:** Do not use a filename.
MS SQL/Server	com.netiq.iac.mssql.ssl.server.cert	Contents of the certificate **NOTE:** Do not use a filename.
MS SQL/Server	com.netiq.iac.mssql.ssl.password	Password

Use the information from this table to create and configure the required configuration properties for the archive destination you want to create.

NOTE: The configuration properties required for SSL communication could already exist in your environment. You can select **Configuration** > **Advanced**, then use the search feature to verify whether the configuration property you need is already configured as a global configuration setting.

To create and configure the proper global configuration properties for your archive destination and for the SSL type:

1. Log in as a Global or .
2. Select **Configuration** > **Advanced**.

3 Next to **Global Configuration Settings**, click the plus sign (+).

4 Type the name of the configuration property you want to create, then click **Add**.

5 Type the value for the configuration property you want to create, then click **Create**.

6 Perform Step 3 through Step 5 for each property you need to create.

13.2.2 Creating an Archive Destination

To configure an archive destination:

1 Select **Data Administration** > **Maintenance.**

2 Click **Archive Destinations**.

3 Click "+" to add an archive destination.

4 Click **Current Archive Destination** to specify the database as the archive location you want to use.

5 Provide the requested information.

6 Click **Test Connection** to verify your settings.

7 Click **Save**.

13.3 Performing Database Maintenance

When you start database maintenance, you can choose whether to perform concurrent database archiving.

If you do not select **Perform concurrent archive**, the Identity Governance server is put in an idle state before starting the archive, and it remains idle while the archive runs. The server does not start the database archive until any active Identity Governance background processes complete, and does not allow new background processes to start until archiving completes. Doing so ensures the database is in a logically consistent state, and that it remains in that state during archiving. No Identity Governance processes will run during archiving, and Identity Governance is not available for use. Therefore, if your archive process takes a long time, you may want to select **Perform concurrent archive**.

NOTE: Even a concurrent archive eventually must idle the Identity Governance server to finalize the archive.

If you select **Perform concurrent archive**, Identity Governance background processes may continue to run, and Identity Governance remains available. A concurrent archive comprises **iterations**, which are multiple archives. If a change occurs to the database during an archive, another iteration of the archive runs. Because each archive iteration archives only data that has changed since the last iteration, each iteration is an incremental archive that should have less data to archive than the previous iteration, and which reduces the amount of time it takes to archive. Ultimately, to achieve a logically consistent archive, the Identity Governance server must be idled for a final iteration. The final archive iteration is a non-concurrent archive, but because it was preceded by multiple incremental archives, the final archive iteration should not contain as much data to archive, which means Identity Governance is idled for only a very short period of time.

You must specify a time for the final iteration to occur. The final iteration will be produced on or after the specified time. The final archive iteration is, in effect, a non-concurrent archive. In addition to specifying a finalization time, you must specify a time interval to pause between archive iterations to control the number of archive iterations that occur between the time the concurrent archive starts and the time it is finalized.

NOTE: **Perform concurrent archive** is also an available option for scheduled maintenance that ensures Identity Governance processes are not idle during scheduled database maintenance periods.

If you perform a concurrent archive while an archival reader has accessed the archive, Identity Governance informs you that archiving is "Waiting on archival readers." Click the message to view details about the maintenance you started, including the number of readers in progress. You can click the number for details about the readers and determine whether you want to continue waiting, or if you want to stop the readers and proceed with the archive.

NOTE: Proceeding with the archive while read activities are in progress can result in incomplete or canceled reports, or missing data.

Large databases that require a long time to archive run the risk of being interrupted before completion due to connectivity issues or system failures. If you selected **Perform concurrent archive** as a maintenance option, you can also select **Resume archive** to ensure the last archival process can continue from the point of interruption, rather than beginning again, when an interruption occurs then resolves.

Database maintenance also allows you to choose whether you want to clean up the database after you archive. For more information about database cleanup, see Section 13.6, "Identifying Purgeable Data," on page 147.

To archive databases and perform maintenance:

1. Select **Data Administration** > **Maintenance.**
2. (Optional) Calculate and view:
   - Summary of what will be archived in the next archive
   - Summary of items that could be purged

   NOTE: If your database is large, these summaries can take a long time to calculate and can consume significant server resources to produce. Click the Refresh icon to calculate or recalculate summaries. Calculated summaries expire after an hour, and you must click the Refresh icon to calculate them again. You can cancel a running calculation at any time.

   ---
3. Click **Start Maintenance**.
4. To purge data without archiving, disable **Perform archive**. Identity Governance cleans up only items that were previously archived in the archive database. However, if you select the option Disable Archiving, all items can be purged. To preserve your data, archive before clean up. You should also make sure your archive data is backed up in your company's archive system before you disable archive.

   To purge data from the operations database after the archive process completes, enable **Perform archive**.

NOTE: Identity Governance disables all user operations during the archiving process.

5 To archive without stopping any processes currently in progress, select **Perform concurrent archive**, and then select values for the following items:

- **Finalize On Or After** to specify the date and time to finalize the archive.

  NOTE: At the end of each iteration, Identity Governance checks if the current time is at or past the specified finalization time. If so, Identity Governance immediately starts the final archival iteration. If not, Identity Governance starts the next concurrent archival iteration.

- **Pause Between Iterations** to specify the amount of time to pause after each archive iteration.
- **Resume archive** to ensure the last interrupted archival process continues from the point of interruption, rather than beginning again, when the interruption is resolved and the archive restarts.

6 Select whether to pause after the archive phase.

IMPORTANT: If you pause after a phase, the system does *not* automatically transition to the next phase or exit maintenance mode until a user either manually starts the next phase, or exits maintenance mode, even if the archive fails or is canceled.

7 Click **OK**.

13.3.1 Cleaning up Purgeable Data

Database maintenance allows you to choose to clean up the database after you archive. In the **Cleanup Options** tab, you can specify the instances you want to clean up, view the entities eligible for cleanup, and view the last time this data was calculated. Under the **Advanced cleanup options**, the data is grouped and sub-grouped by entity type. You can expand and collapse the entity types to specify the entities or entity types you want to clean up. You can select the number of retention days per entity type, and Identity Governance propagates that number to all its entities. However, you have the option to change the number for each entity. Identity Governance retains the data before it makes the data available for clean up. The number of items refers to the entity instances available for clean up.

NOTE: If you disable archiving and then enable it, cleanup could result in no results, because data was not archived, and no cleanup occurred. Be sure you enable archiving and refresh to update the number of items available for cleanup.

To clean up databases:

1 Select **Data Administration** > **Maintenance.**

2 Click **Start Maintenance**.

3 Select **Cleanup Options**.

4 (Optional) Deselect **Perform Cleanup** to archive data without cleanup.

NOTE: When **Perform Cleanup** is enabled, Identity Governance cleans up data after archiving. You can access the application and perform all governance operations while cleanup is running.

5 (Optional) Select whether to pause after the cleanup phase.

6 (Optional) Specify the number of **Retention Days** if you want Identity Governance to cleanup data based on the global retention day settings. This setting applies to all entity types and their instances. However, if you select a retention day for a specific entity or its instance, the selected value takes precedence.

We recommend that you keep all your operations data for 30 days except for review instances and request data. We recommend that you keep your review and request instances for 90 days and archive every week.

7 Click **show** to view the list of entity types eligible for cleanup.

Some entity types are selected by default, Identity Governance removes these entities during the cleanup phase of database maintenance. For more information, see Section 13.6, “Identifying Purgeable Data,” on page 147.

8 (Optional) Select **ENTITY TYPE** to select all items and deselect specific items, or deselect to clear all items and select specific items

---

NOTE: The selected items are considered in the number of items count, and the same number is reflected for the entity type at the folder level. You can select or clear the check box to recover the previous count or clear selection.

13.4 Disabling and Enabling Archiving

WARNING: Use this feature cautiously. Disabling archiving deletes all data from your archive database. Ensure you have previously backed up your data in your company’s archive system before disabling Identity Governance archiving.

Archiving processes might slow down your operation processes. To prevent this, a Global, Data, or Maintenance Administrator can disable archiving temporarily and then reactivate archiving by selecting **Disable Archiving** and **Enable Archiving**. Disabling archiving not only clears all data from the archive database but also deactivates triggers that capture updates to the operations database.

13.5 Scheduling Data Maintenance

Identity Governance enables SaaS Operations Administrators, Maintenance Administrators, Global Administrators, and Data Administrators to schedule archive and cleanup maintenance tasks to run at times when the archive or cleanup will not interfere with other governance tasks. You can cancel scheduled maintenance tasks while they are running.

- Section 13.5.1, “Scheduling Data Maintenance with Concurrent Archiving,” on page 144
- Section 13.5.2, “Create a Data Maintenance Schedule,” on page 145

13.5.1 Scheduling Data Maintenance with Concurrent Archiving

You can create scheduled maintenance tasks that perform concurrent archiving. However, specifying the finalization date and time requires configuration not required for concurrent archiving for manual data maintenance. The additional configuration is required, because a schedule could have

repeat intervals, so specifying an absolute finalization date and time is not possible. Identity Governance provides the following choices to specify the finalization date and time for maintenance schedules:

- **Run Once (not repeated)** If you set a scheduled archive to run only once, you must enter a date and time for finalization.
- **Run Daily** If you set the scheduled archive to run daily, enter the time of day to finalize. The finalization time of day must be greater than the time of day specified in the scheduled start date and time.
- **Run Weekly** If you run a weekly scheduled archive, you must enter a day of the week and a time of day to finalize. The day of the week must be on or after the day of the week you specified in the schedule start date and time. If the day of week is the same day of week as specified in the start date and time, then the time of day must be after the time of day specified in the schedule start date and time.
- **Run Monthly** If you run a monthly scheduled archive, you must also specify one of the following:
  - **Last Day Of Month** If you schedule an archive to run on the last day of the month, the only option to set is time of day, which must be greater than the time of day specified in the schedule start date and time.
  - **Week of Month and Day Of Week** If schedule an archive to run on a specified week and day of the week, your entry for the finalization date and time depends on which of the following options you specify:
    - **Last Week or Week 4** The only option you may specify for archive finalization is time of day, which must be greater than the time of day specified in the schedule start date and time.
    - **Weeks 1, 2 or 3** You may specify a week of the month, a day of the week, and a time of day for finalization. The week of the month should be the same, or later, week of the month than the week of the month specified for the schedule. However:
      - If you specify the same week of the month as the schedule, the day of the week must be the same, or later, day of the week than the day specified for the schedule.
      - If you specify a week of the month greater than the week specified in the schedule, the day of the week may be any day of the week.
      - If you specify a week of the month and the day of the week the same as the week and day specified for the schedule, time of day must be greater than the time of the day specified for the schedule.

13.5.2 Create a Data Maintenance Schedule

To create a new schedule:

1. Select **Maintenance Schedules**, and then click **+**.
2. Specify a name and description.
3. Select a future time as start time for maintenance task and set recurrence. The first run time will be the current hour, day, week, or month. Then the maintenance task repeats based on the specified schedule.

4 (Optional) Specify the maximum archive time. Maximum archive time is the length of time (in minutes) the archiving task/process runs before automatically stopping. It prevents user operation lock out for extended period and ensures that the archiving task has sufficient time to complete successfully. If unspecified, the archiving continues until it completes.

Identity Governance calculates the archiving task end time by adding the maximum archive time to the scheduled start time. The end time is an absolute time. Even if a scheduled maintenance task starts later than the specified start time (because a previous maintenance task is still running), the end time remains the same.

For example, if the schedule start time is 3:00 PM and maximum archive time is 180 minutes, the archiving task ends at 6:00 PM regardless of when the archiving actually started.

5 To archive without stopping any processes currently in progress, select **Perform concurrent archive**.

NOTE: Scheduling Data Maintenance with Concurrent Archiving describes the available configuration choices.

---

6 Select the maintenance type.

6a Select **Archive Only** to specify the schedule for automatic data archiving. Once the scheduled run starts, Identity Governance waits for all background processes to complete and then triggers archiving. All user operations are disabled during this process.

NOTE: If archiving is disabled, this schedule is skipped.

6b Select **Cleanup Only** to specify the cleanup schedule, and to specify the entity types to clean up and their retention days. For data to be cleaned up, it should satisfy the conditions described in Section 13.6, “Identifying Purgeable Data,” on page 147. You can perform governance operations while cleanup is running.

6c Select **Archive and Cleanup** to schedule archiving and cleanup and configure advanced archive and clean up options including retention dats.

We recommend that you keep all your operations data for 30 days except for review instances and request data. We recommend that you keep your review and request instances for 90 days and archive every week.

Once archiving is complete, cleanup starts automatically based on specified data types.

NOTE: If archiving is disabled, the archive phase is skipped and Identity Governance performs cleanup as if a **Cleanup Only** option was selected. When this occurs, the data must satisfy the conditions described in Section 13.6, “Identifying Purgeable Data,” on page 147.

---

7 (Conditional) If you selected **Archive Only** or **Archive and Cleanup**, as the maintenance type for a concurrent archive, you can select **Resume archive** to automatically resume the last archive that failed to complete.

8 Activate the schedule and save the schedule, or save the schedule and activate it later.

13.6 Identifying Purgeable Data

During the cleanup phase of database maintenance, Identity Governance removes some entity types from the operations database, and so, Identity Governance selects these data types by default. However, there are a few entity types which are not cleaned up by default and requires manual selection.

To view the list of entity types which are eligible for cleanup, click **show**. Select from the following entity types the purgeable data for cleanup:

- **Collection and publication**

  Account upload

  Can be purged when the account upload data production is complete and the container that contains the entities created during the upload is not a part of the current snapshot.

  Collect or publish production

  There are three types of data production that can be purged:

  - **Collection**

    Can be purged if:

    - Collection is not running
    - Version column is not previous or current
    - Publish change production does not reference the collection (publish changes production including child production associated with the collection must be purged first)
    - Entity container does not have entities that reference the collection or any of its child data collection

  - **Publish all**

    Can be purged if the publish all production is not running for an application and the entity container does not have entities that reference the production. However, snapshots containing the publication must be purged first.

  - **Publish changes**

    Can be purged if:

    - The publish changes production is not running for an application
    - The entity container does not have entities that reference the production
    - The publish changes production is not the latest that is run for the application. The latest production is retained.

  Collection

  Can be purged if:

  - It is not currently running, and is in a canceled, failed, completed, or terminated state
  - Its data is not part of any snapshot (snapshots containing data from a collection must be purged first)

  Data production

  Can clean up data production records that are not cleaned up by any other cleanup type.

Data source

Can be purged if it:

- Is not scheduled for collection
- Is not currently being collected or published
- Was deleted
- Is not part of a snapshot (snapshots containing data from data source must be purged first)

Additionally, when the data source is an application, it can be purged if the application:

- Is not a parent of another application
- Is not referenced by a business role
- Has no permissions referenced by a technical role
- Has no permissions referenced by a business role
- Has no permissions referenced by a separation of duty (SoD) policy

Permission upload

Can be purged when the permission upload data production is complete and the container that contains the entities created during the upload is not part of the current snapshot.

RTC (Real Time Collection) batch

Can be purged when the data production for the RTC batch (or RTC ingestion) is complete, failed with an error, or was canceled. Real time collection cannot be in progress.

Snapshot

Can be purged if it:

- Is not the current snapshot of the Identity Governance catalog
- Is not a precursor to another snapshot
- Is not referenced by a review instance
- No Separation of Duties violations exist for users or accounts in the snapshot
- No technical roles exist that reference permissions in the snapshot

Snapshot version

Can be purged if:

- The entity container is not associated with any snapshot, snapshots that reference the entity container must be purged first
- The entity container is not a result of one of the following data producer types:
  - Curator
  - Autocurator
  - Mortician
  - Historian
- The entity container is not the latest version for the data producer whose type is collector

Entity records from these data producer types is not associated with any snapshot, but should not be deleted.

User upload

Can be purged if the user upload data production is complete and the container that contains the entities created during the upload is not part of the current snapshot.

- **Data production**

Certification policy calculation

Can be purged if it:

- Is in its final state and has been completed, canceled, failed, or terminated
- Is not the last calculation or the last completed calculation production for the certification policy it is associated with

Data collection

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not the last data collection or the last completed data collection for the data collector it is associated with
- The data collected by the data collection (such as users, permissions, accounts) have all been purged first by snapshots and snapshot versions
- The data source collection data production it is associated with is in its final state and has been completed, canceled, failed, or terminated

Data policy calculation

Can be purged if it:

- Is in its final state and has been completed, canceled, failed, or terminated
- Is not the last calculation or the last completed calculation production for the data policy it is associated with

Data source collection

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not referenced by any data collection productions (data collection productions that reference the data source collection must be purged first)
- It is for an application data source or an application definition data source, its version is deletable and it is not referenced from a process change event production
- It is not the last data source collection or the last completed data source collection for the data source it is associated with

Data source test collection

Can be purged if it is in its final state and has been completed, canceled, failed, or terminated and there are no data test collection productions associated with it. Any associated data test collection productions must be purged first.

Data test collection

Can be purged if the test collection production and its associated data source is in its final state and has been completed, canceled, failed, or terminated.

Identity publication

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not the last identity publication or the last successful identity publication
- The data published by the identity publication (such as users and groups) has all been purged first by snapshots and snapshot versions.

Job end production

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not the last job end or the last completed job end production for the schedule it is associated with or it is not associated with a schedule
- It is not a prerequisite to any data productions or any data productions to it (other than the job start productions). All prerequisites productions (other than job start production) must be purged first. All productions it is a prerequisite to must be purged first

Job start production

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not referenced by any job end production (associated job end productions must be purged first)
- It is not a prerequisite to any data productions. All productions it is a prerequisite to must be purged first

Policy detection

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not the last policy detection or the last completed policy detection production for the policy it is associated with

Provisioning production

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not the last provisioning production or the last completed provisioning production for the application it is associated with
- There are no associated change request items that are not in their final state

Review task production

Can be purged if it is in its final state and has been completed, canceled, failed, or terminated and the associated review instance is not in a starting or start preview state.

Risk score production

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not the last risk score production or the last completed risk score production for the risk score configuration it is associated with

Verify provisioning production

Can be purged if:

- It is in its final state and has been completed, canceled, failed, or terminated
- It is not the last provisioning production or the last completed provisioning production for the application it is associated with or it is not associated with an application

- **History**

Account history record

Can be purged when the account record is marked as history and resides in the special history container.

Application history

Can be purged at any time.

Merge history record

Can be purged anytime. The merged histories are purged based on the Merge Event Time.

Permission history record

Can be purged when the permission record is marked as history and resides in the special history container.

User history record

Can be purged when the user record is marked as history and resides in the special history container.

- **Miscellaneous**

Analytical facts

Can be purged only when retention time is specified and facts are older than the specified retention time.

Auto fulfillment request

Can be purged when the associated change request item is in a final fulfillment state. Final fulfillment states include:

- Request refusal
- Error fulfilling the request
- Request verified
- Request *not* verified and verification ignored
- Verification timed out

Bulk data update definition

Can be purged if it was deleted.

Category

Can be purged if the category was deleted.

Custom form

Cleans up custom forms.

Performance log

Can be purged at any time.

Unregistered facts

Can be purged when fact tables are available in the schema, even after custom facts are unregistered from fact catalog.

NOTE: The purge conditions for each data type *might change* if a new scenario occurs that determines that the conditions have changed.

- **Policy**

Access request and approval policy

Access request

Can be purged only when the request is complete, which includes one of the following states:

- Request was denied approval
- Request was declined fulfillment
- Request was fulfilled and verified
- Request was fulfilled and verification failed

Access request approval policy

Can be purged when there are no access requests that reference the approval policy and the policy is deleted.

Access request policy

Can be purged when there are no access requests that reference the policy and the policy is deleted.

Auto resolution policy

Auto resolution

Can be purged if it is not currently running, and is in a canceled, failed, or completed state.

Auto resolution policy

Can be purged when there are no auto resolutions that reference the policy and the policy is deleted.

Business role policy

Business role

Can be purged if it:

- Has been deleted or it is an old version of a business role
- Is not referenced from any review definitions or review items
- Is not referenced from any change request items

Business role authorization

Can be purged when they are deleted. Business role authorizations are marked deleted when a business role detection removes them.

Business role detection

Can be purged if the business role detection is not currently running, because detection either completed successfully, failed, or was canceled.

Business role membership

Can be purged when they are deleted. Business role memberships are marked deleted when a business role detection removes them.

Inconsistency detection

Can be purged if the detection has been marked as deleted.

Certification policy

Certification policy

Can be purged if policy was deleted.

Certification policy violation

Can be purged if the violation was resolved.

Data policy and control

Data policy

Can be purged if it was deleted.

Data policy violation

Can be purged if the violation was resolved.

Remediation action or process

Can be purged if it is old, based on the timestamp. A remediation run will not be deleted if it is the only run for a policy remediation.

Risk score status

Can be purged if it:

- Is in the error, canceled, or completed state
- Is in completed state, and there is another completed risk score status of the same entity type with a later start time

Separation of duty policy

Separation of duties approval policy

Can be purged if the policy record was deleted.

Separation of duties case

Can be purged if:

- The case is closed
- No change request items were made to resolve the case or, if there are change request items associated with the case, they are all in a final verified or error state and not still pending fulfillment

Separation of duties policy

Can be purged if it:

- Was deleted
- Is not referenced in an SoD case (SoD cases should be purged first)
- No access requests with potential SoD violations for the policy exist (Such access requests must be purged first)

Separation of Duties detection

A separation of duties (SoD) detection is information associated with an SoD case that keeps track of the detection history for the SoD case. These detections are also purged if an SoD case itself is purged.

The SoD detection purge allows the detection history to be purged without having to purge the SoD case. SoD detection can be purged only if it is not the most recent detection for the SoD case.

Technical role

Can be purged if it:

- Was deleted from the Identity Governance catalog
- Is not referenced by a review instance
- Is not referenced by an SoD policy
- Is not referenced by a Review Definition
- Is not referenced by a business role

Technical role assignment

Can be purged if the technical role assignment was deleted (unassigned).

Review

Review definition

Can be purged if it:

- Was deleted
- Is not referenced by a review instance (review instances must be purged first)
- Is not referenced by a certification policy (certification policies must be purged first)
- Is not referenced by a remediation from a certification or data policy

Review instance

Can be purged if it:

- Is not running, and was canceled, experienced an error, or completed certification
- Is not referenced by a pending change request item action (is not in a final verified or error state)

NOTE: Materialized views, if any, are purged when review instances are purged.

Request approval policy

Can be purged if:

- The policy was deleted
- No requests associated with the policy exist (requests associated with the policy must be purged first)

Request policy

Can be purged if:

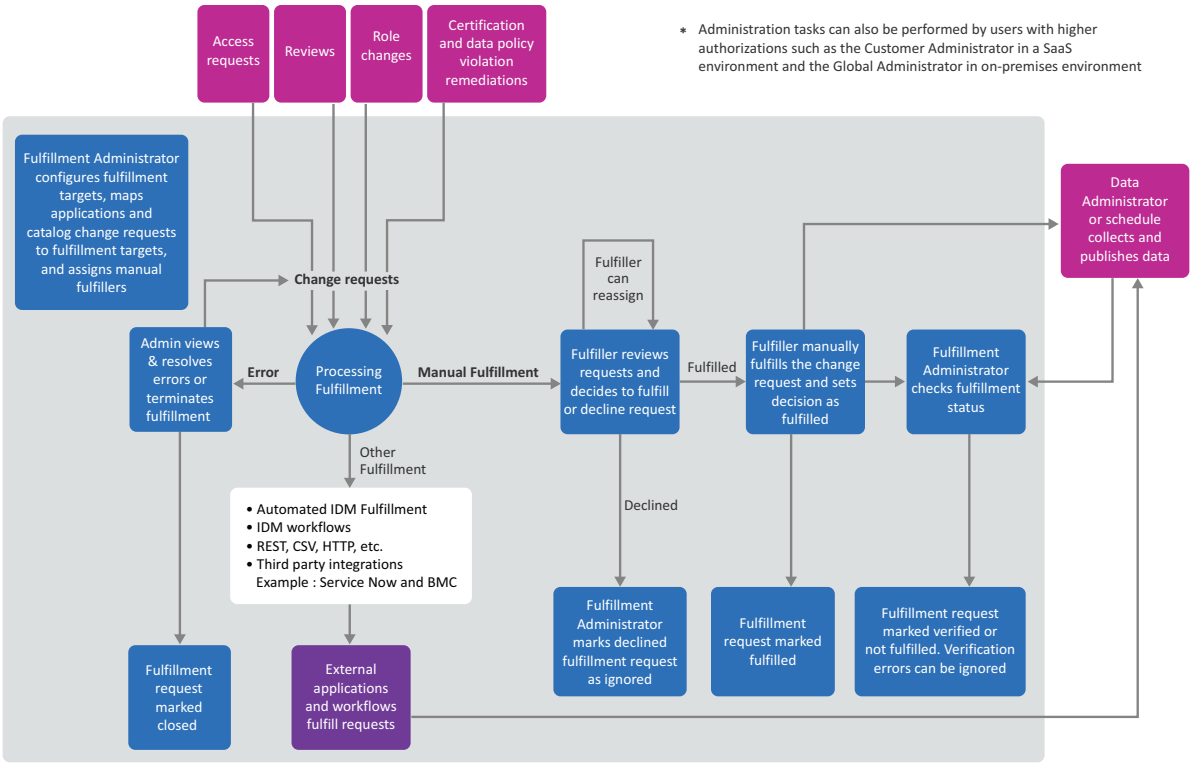
- The policy was deleted
- No requests associated with the policy exist (requests associated with the policy must be purged first)

14 Setting up Fulfillment Targets and Fulfilling Changesets

Various activities result in Identity Governance building a list of changes, or **changesets,** that are then submitted for **fulfillment**. Reviews, policy violations, role changes, and access requests can all result in changes that need to be fulfilled. The Identity Governance fulfillment system evaluates the individual permission change items, determines which applications use these permissions, and then sends the changesets to the appropriate fulfillment target for each application. If needed, administrators can modify the changesets before processing them for fulfillment. Identity Governance users with Bootstrap, Customer, Global, or Fulfillment Administrator authorization assignments can configure fulfillment options.

14.1 Understanding the Fulfillment Process

Figure 14-1 *Fulfillment Process*



Identity Governance refers to the implementation process of a changeset as fulfillment. Many users take part in the overall fulfillment process:

- Fulfillment administrators configure fulfillment targets, monitor fulfillment status, and take as needed actions to complete change requests.
- Requesters, Reviewers, Review Owners, Review Administrators, Business Role Administrators, or Data Policy Administrators take actions that generate change requests that are sent to the fulfillment process.
- Fulfillers manage change requests.

For more information about Identity Governance authorizations, see Chapter 2, “Adding Identity Governance Users and Assigning Authorizations,” on page 19.

14.2 Configuring Fulfillment

Identity Governance provides three default options for fulfillment targets for provisioning the changeset items from a review: Identity Manager automated, Identity Manager workflow, and Manual (a user or group). You can also integrate and automate Identity Governance fulfillment with your service desk system by adding and configuring a connector to your service desk system in Identity Governance **Fulfillment Configuration**.

Identity Governance supports the following connectors for fulfillment to help enable fulfillment via common methods and connected systems. Each template can be customized to connect to associated data sources.

NOTE: Customization of templates might require additional knowledge of connected systems, and all modifications are the responsibility of the customer. For further guidance, contact support or professional services. For information about confiuring the provided templates, see Chapter 17, “Understanding Variations in Collector and Fulfillment Target Configurations,” on page 183.

- Active Directory LDAP
- BMC Remedy Incident
- CSV
- eDirectory LDAP
- Generic HTTP
- Identity Manager Dxcmd Fulfillment for Active Directory
- IDM Entitlement
- JDBC Generic DB
- JDBC Oracle
- JDBC PostgreSQL
- JDBC SQL Server
- REST Generic
- REST Github
- Salesforce
- SCIM
- ServiceNow Generic
- ServiceNow Incident
- ServiceNow Request
- ServiceNow Task
- SOAP Service
- Workflow Service

For more information, see:

- Section 14.2.1, “About Fulfillment Types,” on page 158
- Section 14.2.2, “Configuring System Fulfillment Targets,” on page 161
- Section 14.2.3, “Understanding Service Desk and Other Fulfillment Targets,” on page 162

14.2.1 About Fulfillment Types

Identity Governance includes fulfillment types connectors for various service desk products to enable fulfillment integration with your incident management applications. When you connect to an application for fulfillment, you must configure the connector to map the data fields in the change item to the input fields of the application. In a typical service desk environment, all systems and applications that the service desk manages are input as configuration management items.

Identity Governance exposes the following data fields from each changeset item to the fulfillment target connectors:

changeItemId

A long value containing the internal change item number

changeSetId (optional)

A long value containing the internal changeset number

changeRequestType

A string value containing one of the following values:

NOTE: Supported change request types can vary based on your fulfillment target.

- `ADD_USER_TO_ACCOUNT`
- `REMOVE_PERMISSION_ASSIGNMENT`
- `REMOVE_ACCOUNT_ASSIGNMENT`
- `MODIFY_PERMISSION_ASSIGNMENT`
- `MODIFY_ACCOUNT_ASSIGNMENT`
- `REMOVE_ACCOUNT`
- `ADD_PERMISSION_TO_USER`
- `ADD_APPLICATION_TO_USER`
- `REMOVE_APPLICATION_FROM_USER`
- `ADD_TECH_ROLE_TO_USER`
- `REMOVE_ACCOUNT_PERMISSION`
- `MODIFY_ACCOUNT`
- `REMOVE_TECH_ROLE_ASSIGNMENT`
- `REMOVE_BUS_ROLE_ASSIGNMENT`
- `MODIFY_TECH_ROLE_ASSIGNMENT`

fulfillmentInstructions (optional)

Instructions the reviewer and request approver provided for the fulfiller

flowdata

Data item mappings and definitions that are passed through from request workflow to fulfillment workflow

userName

Display name of the user that is the target of the change item

account (optional)

Identifier of the account

accountLogicalId (optional)

Logical system identifier of the account. This only applies to Identity Manager SAP User Management driver accounts.

accountProvId (optional)

The collected identifier that indicates the unique ID of the account

appName

Name of the application to which the permission being provisioned belongs

fulfillerName (optional)

Name of the fallback fulfillment user

reason

Generated description of the action being requested by the change item

requesterName

Display name of the reviewer who requested the change

permName

Name of the permission being provisioned

permProvAttr

Name of the target permission attribute being modified

permProvLogicalId (optional)

Logical system identifier of the permission being provisioned. This only applies to the Identity Manager SAP User Management driver permissions.

permProvId (optional)

The collected unique provisioning identifier of the permission

reviewReasonId (optional)

The internal long value for the reason

reviewReason (optional)

The reason text

userProfile (optional)

Attribute to provide context to the fulfiller on the recipient of the fulfillment item

requesterProfile (optional)

Attribute to provide context to the fulfiller on the requester of the fulfillment item

accountProfile (optional)

Attribute to provide context to the fulfiller on the account if the fulfillment item is an account

permissionProfile (optional)

Attribute to provide context to the fulfiller on the permission if the fulfillment item is a permission

The following shows a sample change item payload:

```
{
    "accountProvId": "d2a293ff-71c5-492f-9415-e08830b635b2",
    "changeItemId": 8300,
    "changeRequestType": "REMOVE_PERMISSION_ASSIGNMENT",
    "userName": "Abby Spencer",
    "accountName": "aspencer",
    "account": "CN=Abby
Spencer,OU=Users,OU=MyServer,DC=mydc,DC=mycompany,DC=com",
    "appName": "Money Honey Financials",
    "reason": "REMOVE_PERMISSION_ASSIGNMENT remove permission Marketing
Portal requested by Aaron Corry while certifying Money Honey Financials",
    "requesterName": "Andrew Astin",
    "permName": "Marketing Portal",
    "permProvAttr": "member",
    "permProvId": "e07db779-5c30-44d2-bc0c-6dfa30cfa6af"
}
```

Fulfillment types use preconfigured templates that map the Identity Governance change item data and application-specific static values into various attributes in the SOAP XML payload. The WSDL from your service catalog request management application indicates any value constraints for input fields. The fulfillment target service can populate all valid fields in the service desk interface, so if you want to extend the set of fields that the Identity Governance template populates or modify the default mappings of the template, contact your NetIQ technical support representative for details.

The service parameters and other fulfillment target configuration fields vary, depending on the fulfillment type selected for a fulfillment target, and Identity Governance provides default values for many of the fields, but you can choose to customize field values.

For example, the “BMC Remedy Incident” fulfillment type uses the `HPD_IncidentInterface_Create SOAP service Helpdesk_Submit_Service` method for creating incidents in the Remedy application. For example, `http://your-service-host/arsys/WSDL/public/your_server/HPD_IncidentInterface_Create_WS`. In addition, **Fulfillment Item configuration mapping** displays the fields listed in the table below.

BMC Remedy Incident Field	Identity Governance Mapping
`Service_Type`	“User Service Request” (required)
`Reported_Source`	“Direct Input” (required)

BMC Remedy Incident Field	Identity Governance Mapping
Status	“New” (required)
Action	“CREATE” (required)
Urgency	“3-Medium” (required)
Impact	“3-Moderate/Limited” (required)
First_Name	(required)
Last_Name	(required)
Notes	Reason, appName, username, account (ecmascript transformation provided)
Summary	changeRequestType
HPD_CI_ReconID	

Mapping Identity Governance change item data to target application data fields is similar to configuring data source collectors. This includes support for static value mapping and per-field data transformation. Regardless of the fulfillment type you select, you must place quotes around the static values used for fulfillment type configuration.

Since the implementation of any particular service desk application varies widely for each customer, it may be useful to manually create sample incidents using the application user interfaces to validate the desired inputs for each fulfillment target.

14.2.2 Configuring System Fulfillment Targets

Identity Governance provides three default fulfillment targets: Identity Manager automated, Identity Manager workflow, and manual fulfillment targets. For these fulfillment targets, Identity Governance evaluates and fulfills the change items without the need for extensive configuration. When you are specifying one of the default methods of fulfillment, do the following:

Manual

Specify an individual or group of individuals to serve as the fulfiller. For more information about manual fulfillment, see Section 14.6.1, “Manually Fulfilling the Changeset,” on page 170.

To have Identity Governance email reminders to the fulfillers, ensure that you configure email notifications using the Identity Governance Configuration Utility. For information about customizing emails to fulfillers, see Section 4.4, “Customizing Email Notification Templates,” on page 46.

Identity Manager Workflow

Applies only when you integrate Identity Governance with Identity Manager.

Specify the name of a workflow that already exists in Identity Manager. The Identity Manager workflow must have inputs for the following fields:

- `String: changesetId`
- `String: appId`

To connect to the external provisioning system from Identity Governance, click **Configuration** > **Identity Manager System Connection** (or you can use the Identity Governance Configuration Utility in the console mode). For example:

URL

```
http://$test:8543/IDMProv
```

User ID

```
globaladmin
```

Password

```
adminpassword
```

For information about the Configuration Utility procedures, see "Using the Identity Governance Configuration Utility" in the *Identity Governance 4.3.1 Installation and Configuration Guide*. For more information about the workflow process, see Section 14.6.2, "Using Workflows to Fulfill the Changeset," on page 171.

Identity Manager Automated

Applies only when you integrate Identity Governance with Identity Manager.

Specify whether you want to use automated provisioning with manual fulfillment or a workflow as the fallback method, then specify the values associated with the fallback method. For more information, see Section 14.6.3, "Automatically Fulfilling the Changeset," on page 172.

14.2.3 Understanding Service Desk and Other Fulfillment Targets

In addition to the default fulfillement targets, Identity Governance provides service desk and other fulfillment target templates that enable you to use other fulfillment methods for various systems. When you create a service desk or other fulfillment target in Identity Governance, you provide the connection information and credentials for the target system, as well as a default configuration specifying the fields you want Identity Governance to populate in your incidents. After you assign a target fulfillment system to an application, you can then customize that default configuration to appropriately map the application configuration item, assignment group, severity, and other fields for that specific application.

To know how to configure service desk and other fulfillment targets, see Section 14.2.4, "Configuring Service Desk and Other Fulfillment Targets," on page 162. For variations reagrding specific systems, see Chapter 17, "Understanding Variations in Collector and Fulfillment Target Configurations," on page 183.

14.2.4 Configuring Service Desk and Other Fulfillment Targets

In addition to the system targets, Identity Governance provides default templates for various systems that authorized administrators can configure as their fulfiller. For example, you can integrate and automate Identity Governance fulfillment with your service desk system by configuring a connector to your service desk system in Identity Governance **Fulfillment Configuration**.

To configure service desk and other fulfillment targets:

1 Log in to Identity Governance as a Bootstrap, Global, or Fulfillment Administrator.

2 Select **Fulfillment** > **Configuration**.

3 To add a fulfillment target, select **+**. Ensure that you understand your connectors and special requirements if any before configuring your systems. For information about specific fulfillment targets, see Section 14.2.3, “Understanding Service Desk and Other Fulfillment Targets,” on page 162.

4 Complete the required fields.

4a Configure service parameters to connect Identity Governance to your fulfillment service. If applicable, enable Cloud Bridge connection when fulfilling Identity Governance as a Service requests using on-premises fulfillment services. Note that if you make changes to these parameters, Identity Governance will prompt you to re-enter the password.

NOTE: Micro Focus supports Cloud Bridge only in Identity Governance as a Service deployments.

4b Configure the fulfillment item and map attributes. Click the search icon to select edit data fields included for a parameter. For example, select **Fulfillment Instructions** for instructions from reviewers and approvers to be passed through to fulfillers. Select **Flow Data** for custom request and approval form information to be received by fulfillment systems. In addition, if required, click {...}, then edit the transform script or upload a script to map attributes. For examples, see Section 14.2.3, “Understanding Service Desk and Other Fulfillment Targets,” on page 162.

NOTE: When viewing the list of mapped attributes for a field, you could see some items not available to select and marked with a strike-through line across the text. You must enable these attributes in **Configuration** > **Context Fulfillment Attributes** in order to select them here.

---

5 (Conditional) If you want to modify a fulfillment target, click its name in the **Name** column, and then make necessary changes.

NOTE: Optionally, Global or Data administrators can download the fulfillment target templates, edit them, and upload them to Identity Governance prior to fulfillment administrators configuring the service parameters and mappings in the application itself. For more information, see Section 14.4, “Customizing Fulfillment Target Templates,” on page 169.

---

6 Make any additional updates for the selected fulfillment target, such as fulfillment response mapping and specifying change request types, then click the Save icon.

7 Select the **Application Setup** tab, and configure application fulfillment settings.

7a To modify changesets for a specific application prior to fulfillment, see Section 14.2.6, “Modifying Changesets Before Fulfillment,” on page 164.

7b To configure multiple targets for your applications, see Section 14.2.7, “Configuring Multiple Fulfillment Targets for Applications,” on page 165.

8 Select the **Catalog update setup** tab and select the fulfillment target for each type of catalog update request initiator you have in place.

14.2.5 Upgrading Fulfillment Targets

Authorized administrators can upgrade fulfillment targets. When you import an old template, Identity Governance enables you to preserve your configurations and scripts and upgrade the fulfiller template to the latest version. When upgrading, you can compare the parameters of the two versions and make changes as needed. If you decide to use Cloud Bridge for data transfer, you must first create a data center or import the data center JSON file, then configure a data source connection. You can restore the previous template if needed.

To upgrade the fulfillment template:

1. Under **Fulfillment**, select **Configuration**.
2. Click **Import a fulfillment target**. If you import a fulfillment target that was created with an older version of the template, click the imported fulfillment target and expand the view.
3. (Conditional) If you have upgraded Identity Governance, but have an older version of the fulfillment target, then select the existing target and expand the view.
4. Make necessary changes and save.
5. Click the fulfillment target from the Fulfillment Configuration page.
6. Click **Upgrade**.
   - **6a** Compare configurations and make changes as needed.
   - **6b** Click **Upgrade**.
7. (Optional) **Restore to Template Version** *number* if you want to revert to the older template.

Identity Governance continues to display the restore link until you dismiss the option.

14.2.6 Modifying Changesets Before Fulfillment

Changesets are automatically generated based on activities such as access requests, reviews, and role changes. Identity Governance enables administrators to modify the generated changeset using Javascript. For example, when a user who has no account requests permissions, you can modify the generated changeset to create an account for the user.

To modify changesets:

1. Log in to Identity Governance as a Bootstrap, Global, or Fulfillment Administrator.
2. Select **Fulfillment > Configuration** and select the **Application setup** tab.
3. Click **Edit** next to the application whose changesets you want to modify.
4. Click **+** to create a script to modify changesets.
5. Type the name and description.
6. Use the sample Javascript script to analyze the changeset and modify the script, or import a script from a file.
7. Click the Save icon and close the script window.
8. Publish the script.
9. Compare differences and edit the script if needed, then publish again.
10. Repeat the above steps to add more scripts.
11. Change the script execution order as needed.

14.2.7 Configuring Multiple Fulfillment Targets for Applications

Identity Governance enables administrators to configure one or more applications to use multiple fulfillment targets. For example, you might have one system that processes all requests to add access and a different system that processes all requests to remove access. Using application settings, you can add and modify access changesets to be processed by one system and remove access changesets to another.

To configure multiple fulfillment targets for one or more applications:

1. Log in to Identity Governance as a Bootstrap, Global, or Fulfillment Administrator.
2. Select **Fulfillment > Configuration** and select the **Application setup** tab.
3. To configure multiple fulfillment targets for a single application, click **Edit** next to the application for which you want to configure multiple fulfillment targets.

   or

   Select applications, then click **Change fulfillment targets**.

   NOTE: If you want to configure the same targets for all applications, select the check box in the column header.

   ---

4. On the Application Setup window, click **(+)** to add one or more fulfillment targets to the application.
5. Scroll to, and configure the new fulfillment target.
6. Under the fulfillment target for which you want to process change requests, select **Supported Change Requests**, and select the types of change requests you want the target to process. You can use the same fulfillment target to process all requests, or you can use a different target for certain requests.

   NOTE: To assist the Fulfillment Administrator in making sure that the configured fulfillment targets handle all change request types, Identity Governance shows which change request types are configured next to each fulfillment target. If a target does not support any of the change request types, those unsupported types appear in red text.

   ---

7. When you complete configuration, click **Save**.

14.2.8 Transforming Data from Fulfillment Targets

You can transform the incoming data from fulfillment targets to have Identity Governance display more meaningful information. For example, instead of displaying only the incident number from your fulfillment system, you could display additional text, such as “Incident number 123456 was created in ServiceNow” in Identity Governance.

The transforms are done through Nashorn-compatible Javascript in the **Fulfillment Response mapping** section of the fulfillment target configuration. Within the Javascript, you can access the incoming value by creating a variable name `inputValue`. After manipulating the incoming value, you can return the value to Identity Governance by assigning the value to a variable name `outputValue`.

The following example transforms the incoming value, which is a tracking number from the connected system to `Incident number 123456 created in ServiceNow` in the Identity Governance displays.

```
outputValue = 'Incident number ' + inputValue + ' created in ServiceNow'
```

To change fulfillment target response mapping:

1. Log in to Identity Governance as a Bootstrap, Global, or Fulfillment Administrator.
2. Under **Fulfillment > Configuration**, select an existing fulfillment target or create a new one.
3. Expand the Fulfillment Response mapping section and select the braces ({ }) next to the attribute you want to transform.

   NOTE: Two dots between the braces ({..}) denotes that a transform script exists for an attribute.

   ---
4. Enter or edit the existing transform script in one of the following ways:
   - Select **Edit** and edit the script in the resulting popup window
   - Use the drop down control to either create a new script or edit an existing script
   - Select **Or upload as script file** to upload a script file
5. Save the fulfillment target.

14.3 Monitoring Fulfillment Status

The fulfillment status list allows you to view the status of fulfillment requests by category, such as fulfillment items that:

- Ended in error or timeout conditions
- Are pending fulfillment
- Were verified
- Were ignored

The fulfillment status area also allows you to retry, or resubmit, fulfillment items that did not succeed.

To monitor fulfillment status:

1. Log in to Identity Governance as a Global or Fulfillment administrator.
2. Select **Fulfillment > Status**.
3. Select status categories you want to review.
4. (Optional) Select again any status categories you want to remove from the list.
5. (Optional) Select any fulfillment items that did not complete successfully, and then select **Retry** to resubmit them to the appropriate fulfiller.

14.3.1 Understanding Fulfillment Status

The following details on fulfillment status conditions can help with troubleshooting fulfillment in your environment. A change item has 11 possible status conditions, listed below in the associated status column. The general status column shows the broad status categories that Identity Governance displays to users. The table includes details on each status and what actions, if any, you can take to move an item to a different status. No user action is required for some status conditions, either because they are intermediate states or terminal states.

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
Error or timeout	Provisioning was marked as complete, but the status after a collect and publish cycle shows the item as not fulfilled.	Not fulfilled, verification error (`NOT_VERIFIED`)	Change item marked as fulfilled but updated catalog shows that status to be incorrect. This can be valid when fulfillment target is an asynchronous process, such as Service Now. When Service Now opens a ticket, Identity Governance marks the change request item complete. However, the help desk might not have completed the update to the associated application.	Examine the change item and take one of the following actions: ◆ If the fulfillment target is an asynchronous task, such as Service Now, ensure the help desk has fulfilled the item and then run another collect and publish cycle. ◆ If possible, fulfill the item and then run a collect and publish cycle. ◆ If not possible to fulfill the item, mark the item as **Ignore**.
	Fulfiller has marked item as Declined.	Declined by (`REFUSED`)	Manual fulfiller has marked and submitted item as Declined.	Mark the item as **Ignore**.

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
	Change item was marked as being in error.	Not fulfilled, verification error (`ERROR`)	This status will not be reached by normal operation of the system. It is a transitory state on the way to automatic retry in case there was an error detected during fulfillment. However, an API endpoint can set the status to `ERROR`, so an external system might have caused the item to have this status.	Intermediate status; no action needed.
	Change item has not been successfully verified at the end of verification expiration timeout.	Not fulfilled, verification timed out (`VERIFICATION_TIMEOUT`)	If Identity Governance is set up to monitor verification timeouts and the change item has not been verified within that time, it moves to this status. By default, this value is set to 365 days.	Mark the item as **Ignore**.
Fulfilled	Fulfillment is reported as complete.	Fulfilled, pending verification (`COMPLETED`)	Identity Governance has received communication that fulfillment has completed. This status might not mean the item is fulfilled. If the fulfillment target is an asynchronous process, such as Service Now, the status changes to completed when the asynchronous process opens a ticket, not when the tasks in the ticket have been fulfilled.	After the next collect and publish cycle, Identity Governance verifies the item target matches the change item. If so, the item status changes to Verified. If not, the item status changes to Error.
Pending fulfillment	Fulfillment is in progress.	Initializing (`INITIALIZED`, `IN_PROGRESS`)	Change request item has been created.	Intermediate status; no action needed.

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
	Fulfillment has been initiated.	Pending fulfillment by, Sending for fulfillment by external workflow (PENDING)	Identity Governance successfully communicates with provisioning workflow or adds change items to manual fulfiller queue.	Change item is acted on by either an automated fulfillment system or a manual fulfiller. If fulfiller marks item as fulfilled, the item status changes to Fulfilled (COMPLETED). If the fulfiller marks the item as refused, the item status changes to Error (REFUSED).
Verified	Catalog shows item has been fulfilled.	Verified (VERIFIED)	Identity Governance verifies changes in catalog.	Terminal status; no action needed.
Ignored	Fulfiller or review owner has ignored closed-loop verification.	Verification ignored (VERIFICATION_IGNORED)	Fulfiller or review owner has selected **Ignore** for a change item that was in error or timeout status.	Terminal status; no action needed.
Retry	The change item has had an error during fulfillment and is waiting for administrator action.	Retry	An error is detected during fulfillment.	Customer, Global, or Fulfillment Administrator selects **Retry** or **Terminate** for the item on the Fulfillment Requests page.

14.4 Customizing Fulfillment Target Templates

A fulfillment target template includes predefined service parameters and attribute mappings suitable for the fulfillment target application. To create a custom fulfillment target template, you can download and edit an existing template. Fulfillment target templates use JavaScript Object Notation (JSON) format for specifying the service parameters and mappings. You can use a JSON formatter or text editor to modify the content of the template file.

If a new or customized template replaces an existing template, you can disable the template that you no longer need.

1. Log in to Identity Governance as a Global or Data administrator.
2. Select **Configuration > Fulfillment Target Templates**.
3. Select a template, and then select **Download** or **Disable**.
4. Edit the content.

5 Under **Fulfillment Target Templates**, select **+**.

6 Specify a template name and add description, then browse to the location of the updated file.

7 Select **Save**.

14.5 Specifying Additional Fulfillment Context Attributes

The system sends basic information on how to perform fulfillment after a review or a request. Optionally you may specify additional attributes which also should be included when sending instructions to an external fulfillment target.

NOTE: Manual fulfillment target attributes are not affected by this setting.

---

1 Log in to Identity Governance as a Global or Fulfillment administrator.

2 Select **Configuration > Fulfillment Context Attributes**.

3 Specify **Requester**, **Recipient**, **Account**, **Permission**, and **Supervisor** attributes.

TIP: Use wildcard * to search for attributes.

---

4 Select **Save**.

14.6 Fulfilling Changesets

An application owner can configure the application source to require manual or automated fulfillment. When Identity Governance generates a changeset for fulfillment, Identity Governance determines which applications have change items. Depending on the specified fulfillment type for the application, Identity Governance performs one of the following actions:

- Section 14.6.1, “Manually Fulfilling the Changeset,” on page 170
- Section 14.6.2, “Using Workflows to Fulfill the Changeset,” on page 171
- Section 14.6.3, “Automatically Fulfilling the Changeset,” on page 172

Fulfillment administrators can configure the fulfillment target for an application, including configuring multiple fulfillment targets for an application based on change request types. For more information, see Section 14.2, “Configuring Fulfillment,” on page 157.

14.6.1 Manually Fulfilling the Changeset

During the fulfillment stage of the review instance, Identity Governance creates a task for each review item that must be changed. The assigned fulfillers complete the requested changes in a domain-specific manner, based on the actual permission. The process of fulfilling the changes might

occur over the span of many days and you might need to remove many permissions. To complete the process in a timely manner, Customer, Global, or Data Administrator can specify a group of users to serve as the Fulfiller. Users in the specified group can work concurrently to fulfill the changes.

Identity Governance provides change items, either through a completed review or SoD case review. Following are some examples of the change items:

- Remove user from account (user access review), fulfilled by either removing the user from the account or removing the account
- Modify user access with fulfillment instructions, fulfilled by following the reviewer's instructions
- Remove account (unmapped and mapped account review) fulfilled by removing the account
- Remove permission and inherited permissions (user access review), fulfilled by removing the permissions from the user
- Assign user (unmapped and mapped account review), fulfilled by assigning user to account
- Modify account with fulfillment instructions, fulfilled by following the reviewer's instructions

NOTE: Modify user access and modify account changesets might have a reason, and a user selection might also be required. For more information, see "Configuring Reasons for Review Actions" on page 347. For more information about specific change request types, and fulfillment status, see "Configuring Fulfillment" on page 157.

Identity Governance sends emails to the fulfillers to remind them that they have a manual fulfillment task. The email provides a link to the task. Administrators can customize the message in this reminder. For more information about customizing, see Section 4.4, "Customizing Email Notification Templates," on page 46.

For more information about performing fulfillment tasks, see Chapter 15, "Instructions for Fulfillers," on page 175.

14.6.2 Using Workflows to Fulfill the Changeset

If you integrate Identity Governance with Identity Manager, you can use a custom workflow to remove the permissions. You create the workflow in the identity applications. In Identity Manager, you specify global configuration values (GCVs) to store the connection parameters between the workflow and Identity Governance. The workflow also must have inputs specified in the following fields:

- `String: changesetId`
- `String: appId`

Identity Governance sends the `changesetId` and `appID` to the workflow to process the fulfillment tasks for the review's changeset. The workflow parses the information in the changeset and completes the tasks. When the workflow finishes, Identity Manager informs Identity Governance, which then changes the status of the changes to complete.

For more information, see "Configuring and Managing Provisioning Workflows" in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

To jump start your progress, use the included sample workflow as a starting point in creating your custom workflow to process the change request. Note there is also a companion download that defines the Global Config Values (GCV) that is used by the workflow to configure Identity Governance connection details.

To access the sample workflow:

1. Go to **Fulfillment** > **Configuration** > **Fulfillment Targets** > **Identity Manager workflow (system)**.
2. In the **Fulfillment Samples** section, download a sample workflow.
3. Import the sample workflow into Identity Manager Designer and deploy to Identity Manager Roles Based Provisioning Module (RBPM).
4. Update the sample workflow to specific details in your environment, including the **To do for Customer** section of the workflow.

14.6.3 Automatically Fulfilling the Changeset

You can assign automated provisioning to any application source that derives from Identity Manager. After you complete a review, Identity Governance sends the requested changes to the Identity Manager Identity Vault. The permission type determines whether Identity Manager can automatically provision the requested change. In the identity applications for identity Manager, you specify whether a permission is a **resource** or a **role**. Identity Manager can automatically deprovision all resources because they are explicitly set for the user. Similarly, if a role is explicitly set, it can be deprovisioned. For example, the user has an `nrfAssignedRole` attribute pointing to that role. However, Identity Manager cannot deprovision roles that a user receives indirectly. For example, the user is a member of a container or group to which the role has been assigned.

NOTE: Identity Manager automated provisioning relies on the Provisioning ID value for an identity to be a valid distinguished name in the Identity Manager system. When using multiple identity sources that are merged, be sure you set the Identity Manager identity source as the authoritative source for the Provisioning ID attribute in your identity merging rules.

If deprovisioning can be done automatically, Identity Manager propagates those updates to the connected systems. For those roles that cannot be deprovisioned automatically, the fulfillment process includes a **fallback method**. You can specify that Identity Governance can revert to manual fulfillment or to using an Identity Manager workflow.

14.7 Reviewing Fulfillment Requests

Various components of Identity Governance result in the generation of fulfillment requests. You can review and act on these requests in the Fulfillment Requests area.

1. Log in to Identity Governance as a Global or Fulfillment administrator.
2. Select **Fulfillment** > **Requests**.
3. Select the appropriate category to review and act on the requests.
4. (Optional) Select **Fulfillment Errors** to review errors from fulfillment requests.

14.8 Confirming the Fulfillment Activities

When the Fulfiller confirms the review fulfillment, Identity Governance updates the fulfillment item status under Fulfillment. Bootstrap, global, and fulfillment administrators can access the Fulfillment tab, as well as any individuals with the Fulfiller authorization in Identity Governance. After the administrator collects and publishes application sources again, Identity Governance updates the status of the fulfillment of all changesets except modify changesets.

The Review Auditor, if assigned, must accept or reject the review. Auditors can see the details and history of the review items. When rejecting a review run, the Auditor must add a comment about the rejection. Before the Auditor can verify fulfillment of the requested changes, you must collect and publish all identities and the application sources related to the review. If the review does not have any fulfillment activities, you do not need to perform this action.

For more information, see Section 14.3.1, “Understanding Fulfillment Status,” on page 167.

15 Instructions for Fulfillers

This section provides information for individuals assigned the Fulfiller authorization in Identity Governance. Periodically, individuals in your organization participate in a review to determine whether:

- Permissions granted to users and accounts should be kept or removed
- User identity attributes should be kept or modified
- Users should be kept or removed as members of business roles
- Supervisors assignments should be kept or changed
- Business role definition authorizations, memberships, and attribute values should be kept or modified

Individuals also request access and removal of access. They calculate policy violations and request changes to mitigate policy violations.

For each request, Identity Governance creates a task and routes it to a fulfillment target. When assigned to manually fulfill a request, a fulfiller reviews the request details and fulfills the requests, declines the request, or reassigns the task to another fulfiller.

- Section 15.1, “Understanding the Fulfillment Process,” on page 175
- Section 15.2, “Performing Manual Fulfillment,” on page 177

15.1 Understanding the Fulfillment Process

Identity Governance collects information from a variety of identity and application data sources in your environment. It allows your organization to periodically review and verify that users have only the level of access that they need to do their jobs. The review process, requests for access, business role definition changes, and remediation of policy violations result in a list of changes, or **changeset**, that are then implemented. Identity Governance refers to the implementation process of a changeset as **fulfillment**.

- Section 15.1.1, “Managing the Fulfillment Process,” on page 175
- Section 15.1.2, “Understanding the Fulfiller Authorization,” on page 176

15.1.1 Managing the Fulfillment Process

Fulfillment target configuration, application setup, and catalog update setup by the Customer, Global, or Fulfillment Administrator drives how requested changes are fulfilled. The changes can be fulfilled manually, by a help desk service, or sent to Identity Manager, which automatically makes the

changes or initiates external workflows. For manual fulfillment processes, the Customer, Global, or Fulfillment administrator specifies individuals or groups as fulfillers responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset.

Fulfillment Administrators also monitor the fulfillment process, and reassign manual fulfillment items if needed. Identity Governance provides the following status conditions for fulfillment items:

- Error or time out
- Fulfilled
- Pending fulfillment
- Verified
- Ignored
- Retry

When the fulfiller confirms the fulfillment activities, Identity Governance updates the status of the fulfillment item. After the administrator collects and publishes application sources, Identity Governance again updates the status of these fulfillment items. Customer, Global, and Fulfillment Administrators and Auditors can access the Fulfillment Status page to view the status of all fulfillment items. For more information about fulfillment targets and fulfillment status, see Chapter 14, “Setting up Fulfillment Targets and Fulfilling Changesets,” on page 155.

15.1.2 Understanding the Fulfiller Authorization

As part of the review, managers might change the permissions assigned to individuals in your organization. Access requests, business role definition changes, and user catalog changes can also generate change requests. Only Customer, Global, or Fulfillment Administrators can assign Fulfillers to complete fulfillment.

As a Fulfiller, you can:

- Sort items by column (the available columns depend on the tab you are accessing)
- Add a comment to a task individually
- Add comment to tasks in a batch by selecting all or multiple tasks, or by filtering tasks by specifying search criteria and selecting all or multiple tasks in the filtered list
- View the details of an item at the list level, including:
  - Where the change request originated
  - Potential SoD violations if any
  - Attribute value or supervisor changes
  - Reason for the request by clicking on the task link
- Reassign your tasks to a different user
- Make the changes to the user account in the affected application
- Declare your tasks complete in Identity Governance

15.2 Performing Manual Fulfillment

Identity Governance sends an email notification when you have tasks in a review run based on your review definition and when change requests from reviews, access requests, business role definition changes, and user catalog changes need to be fulfilled. This section provides the steps required for you to complete Fulfiller tasks after receiving an email to manually fulfill a request.

For more information about your authorization and the review process, see Section 25.1, "Understanding the Process Flow," on page 324.

1 In Identity Governance, select **Requests** to view the fulfillment requests.

2 (Conditional) If you have the Fulfillment Administrator authorization, access the **Fulfillment Errors** tab to view fulfillment errors. To resolve the errors:

   2a Click **Fix** to access the **Fulfillment Configuration** page.

   2b Click **Application Setup**, view the settings for the application producing errors, and adjust the settings.

   2c Go back to the **Fulfillment Requests** > **Fulfillment Errors** tab, and click **Retry** to route the item to the correct fulfiller.

   2d If it is not possible to fix the problem, click **Terminate** to remove the change request item from the **Fulfillment Errors** tab.

3 Select **Access Request**, **Business Role**, or **Catalog** tab to view change requests generated from different actions.

4 Click the fulfillment task link on **Access Request**, **Business Role**, or **Catalog** tab to expand the task description and determine the changes to be made, the reason for the change, and any potential SoD violations.

5 In the application affected by the requested change, modify the permission, user, account, or role according to the fulfillment task. This action might impact the SoD policies or uncover unmapped users.

6 Manually fulfill the change request by making the requested changes in the indicated system.

7 Return to Identity Governance and specify an outcome for individual, multiple, or all tasks.

   7a Select **Actions > Fulfilled and submit all** or **Actions > Declined and submit all** to specify an outcome for all items or

   7b Select individual task or multi-select tasks and use the **Actions** menu to specify one of the following outcomes:

   - **Fulfilled** to indicate that you completed the requested changes
   - **Declined** to indicate that you refused to complete the requested changes
   - **Reassign** to assign the fulfillment task to a different user

   NOTE: For fulfilled and declined outcomes, you can also enter comments explaining your action and submit decisions.

   7c (Conditional) To submit fulfillment decisions that were not previously submitted using the **Actions** menu, select **Submit**.

NOTE: Manual fulfillment changes to the fulfillment request do not affect the Review run. Once you specify **Fulfilled** or **Declined** as an outcome, Identity Governance updates the Request status in the Request timeline and when a Review run is complete also updates the fulfillment status of the review item on the Review page.

8 (Conditional) If you have Fulfillment Administrator authorization, you can select **Fulfillment > Status** to view the status of fulfillment requests in the Fulfillment area. For more information, see Section 14.3, “Monitoring Fulfillment Status,” on page 166.

16 List of Collector and Fulfillment Target Templates

Identity Governance provides the following templates.

IMPORTANT: Work with your integration account and network administrators to ensure that you have the minimum rights to the connected systems and that your system has the required security certificates. After initial configuration, you must always update credentials and other service parameters in each template as needed. For example, when connecting to applications that use access tokens for authentication, such as SCIM-compatible applications, you must change tokens when they expire, then reconfigure the template to use the current access token.

Data Sources and Fulfillment Systems	Identity Collector Templates	Account Collector Templates	Permission Collector Templates	Fulfillment Target Templates
Active Directory	◆ AD Identity ◆ AD Identity with Changes	◆ AD Account	◆ AD Permission ◆ AD Hybrid Permission	◆ Active Directory LDAP Fulfillment
Azure AD	◆ Aure AD MS Graph Identity	◆ Azure AD MS Graph Account	◆ Azure AD MS Graph Permission	◆ MS Azure AD Fulfillment
CSV	◆ CSV Identity	◆ CSV Account	◆ CSV Permission	◆ CSV Fufillment
eDirectory	◆ eDirectory Identity ◆ eDirectory Identity (W/O IDM) with Changes	◆ eDirectory Account	◆ eDirectory Hybrid Permission ◆ eDirectory Permission	◆ eDirectory LDAP Fufillment
Google Apps	◆ Google Apps User Identity	◆ Google Apps User Account	◆ Google Apps User Permission	

Data Sources and Fulfillment Systems	Identity Collector Templates	Account Collector Templates	Permission Collector Templates	Fulfillment Target Templates
Identity Manager	◆ Identity Manager Identity ◆ IDM with Changes	◆ IDM Entitlement Account	◆ Identity Manager AE Permission (only for Identity Manager AE systems) ◆ IDM Entitlement Permission	◆ Identity Manager Dxcmd Fulfillment for Active Directory ◆ Identity Manager Automated (system)(only for Identity Manager AE systems) ◆ IDM Entitlement Fulfillment
JDBC	◆ JDBC Identity	◆ JDBC DB2 Account ◆ JDBC Generic Account ◆ JDBC MySQL Account ◆ JDBC Non-specific Account ◆ JDBC Oracle Account ◆ JDBC PostgreSQL Account ◆ JDBC SQL Server Account ◆ JDBC Sybase Account	◆ JDBC DB2 Permission ◆ JDBC Generic Permission ◆ JDBC MySQL Permission ◆ JDBC Non-specific Permission ◆ JDBC Oracle Permission ◆ JDBC PostgreSQL Permission ◆ JDBC SQL Server Permission ◆ JDBC Sybase Permission	◆ JDBC Generic DB Fulfillmemt ◆ JDBC Oracle Fulfillment ◆ JDBC PostgreSQL Fulfillemt ◆ JDBC SQL Server Fulfillment
MS Teams			◆ MS Teams Permission	◆ MS Teams Fufillment
PAM		◆ PAM Account	◆ PAM Permission	
RACF	◆ RACF Identity	◆ RACF Account	◆ RACF Permission	

Data Sources and Fulfillment Systems	Identity Collector Templates	Account Collector Templates	Permission Collector Templates	Fulfillment Target Templates
REST GitHub		• REST GitHub Account	• REST GitHub Organization Permission • REST GitHub Repository Permission • REST GitHub Team Permission	• REST GitHub Fulfillment
Salesforce	• Salesforce Identity	• Salesforce Account	• Salesforce Permission • Salesforce Profile Permission • Salesforce Role Permission	• Salesforce Fufillment
SAP (Not supported in Identity Governance as a service environments)	• SAP HR Identity • SAP User Management Identity	• SAP User Management Account	• SAP User Management Permission	
SCIM	• SCIM Identity	• SCIM Account	• SCIM Permission	• SCIM Fufillment
ServiceNow	• ServiceNow Identity	• ServiceNow Account	• ServiceNow Permission	• ServiceNow Generic Fufillment • ServiceNow Incident Fufillment • ServiceNow Request Fufillment • ServiceNow Task Fufillment
SharePoint	• Sharepoint Identity	• Sharepoint Account		
Workday	• Workday Identity	• Workday Account	• Workday Permission	

Data Sources and Fulfillment Systems	Identity Collector Templates	Account Collector Templates	Permission Collector Templates	Fulfillment Target Templates
All systems				• Manual Fulfillment (system default) • Identity Manager workflow (system) • CSV Fulfillment • REST Generic Fulfillment • SCIM Fulfillment • Workflow Service Fulfillment
Any system reachable via http/ https (excluding systems that use SOAP and REST service)				• Generic Http Fulfillment
BMC Remedy systems				• BMC Remedy Incident Fulfillment (Deprecated)
SOAP systems				• SOAP Service Fulfillment

17 Understanding Variations in Collector and Fulfillment Target Configurations

This chapter focuses on additional configuration-related information specific to templates that might need additional guidance.

Identity Governance provides out-of-the-box templates that enable you to easily integrate with LDAP systems, service desk systems, protocols, and specific applications, to collect data and fulfill change requests. Identity Governance collectors enable you to collect identities, applications, accounts, and permissions to provide a view of all your enterprise data in the Identity Governance catalog. Identity Governance collects the attributes configured in the templates and those are mapped to Identity Governance attributes. You can edit the templates and add attributes to the template while configuring the templates. Identity Governance fulfillment target templates enable you to fulfill change requests generated from reviews, requests, and catalog curation.

Many of these templates are easy to use with tooltips and preconfigured default values. However, a few templates for complex systems might need additional guidance because of the variations in required minimum rights, authentication methods, identity categorizations, parent-child relationships, and other such unique features of the connected systems.

For template layout overview, change event processing, and configuration procedures common to multiple collectors and fulfillment targets, refer to the following sections and chapters:

- Section 6.8.1, “Understanding Collector Configuration,” on page 68
- Chapter 7, “Collecting Identities,” on page 77
- Chapter 8, “Collecting Applications and Application Data,” on page 87
- Section 13.2, “Configuring Fulfillment,” on page 131

For *additional guidance specific to collector and fulfillment target configuration*, see the following sections:

- Section 17.1, “Understanding and Configuring Active Directory and eDirectory Templates,” on page 184
- Section 17.2, “Understanding and Configuring Azure AD MS Graph Templates,” on page 185
- Section 17.3, “Understanding and Configuring CSV Templates,” on page 189
- Section 17.4, “Understanding and Configuring Google Apps Templates,” on page 190
- Section 17.5, “Understanding and Configuring Identity Manager Templates,” on page 191
- Section 17.6, “Understanding and Configuring JDBC Templates,” on page 194
- Section 17.7, “Understanding and Configuring PAM Templates,” on page 195
- Section 17.8, “Understanding and Configuring MS Teams Templates,” on page 196
- Section 17.9, “Understanding and Configuring REST GitHub Templates,” on page 199
- Section 17.10, “Understanding and Configuring Salesforce Templates,” on page 201
- Section 17.11, “Understanding and Configuring SAP Templates,” on page 202

- Section 17.12, “Understanding and Configuring SCIM Templates,” on page 203
- Section 17.13, “Understanding and Configuring ServiceNow Templates,” on page 205
- Section 17.14, “Understanding and Configuring SharePoint Templates,” on page 206
- Section 17.15, “Understanding and Configuring Workday Templates,” on page 207
- Section 17.16, “About REST Generic Fulfillment,” on page 208
- Section 17.17, “About Workflow Service Fulfillment,” on page 209

IMPORTANT: Work with your integration account and network administrators to ensure that you have the minimum rights to the connected systems and that your system has the required security certificates. After initial configuration, you must always update credentials and other service parameters in each template as needed. For example, when connecting to applications that use access tokens for authentication, such as SCIM-compatible applications, you must change tokens when they expire and reconfigure the template to use the current access token.

17.1 Understanding and Configuring Active Directory and eDirectory Templates

Identity Governance provides the following templates for Active Directory and eDirectory:

- AD Identity
- AD Identity with changes
- eDirectory Identity
- eDirectory Identity (w/o IDM) with changes
- eDirectory Hybrid permission
- AD Account
- AD Permission
- AD Hybrid permission
- Active Directory LDAP Fulfillment
- eDirectory LDAP Fulfillment

For additional information about configuring AD and eDirectory templates, see the following sections:

- Section 17.1.1, “About AD and eDirectory Collectors,” on page 184
- Section 17.1.2, “About Active Directory and eDirectory LDAP Fulfillment,” on page 185

17.1.1 About AD and eDirectory Collectors

To ensure synchronization of data from eDirectory to the Identity Governance catalog, the users or groups in eDirectory must have the required minimum rights in the eDirectory repository. The following rights are required for data synchronization:

- For full synchronization: Read permission on the users and their attributes that are collected

- For fast synchronization: Read permission on the users and their attributes that are collected
- For fulfillment: Read and write permission on the users and their attributes for whom the fulfillment request is raised

The Identity Governance collectors for eDirectory have two identity collector templates. The **eDirectory Identity** template is used when the connected system has both eDirectory and Identity Manager installed, whereas the **eDirectory Identity (w/o IDM) with changes** template is used when the connected system has eDirectory installed with the change-log module. The change-log module enables the connector to recognize the changes that require publication from the connected system to the Identity Governance catalog.

For more information about collecting identities with changes and the change event collection, and for more information about applying changes see Section 7.3, “Collecting from Identity Sources with Change Events,” on page 80 and Section 8.9, “Understanding Change Event Processing,” on page 94.

For Identity Governance to associate the accounts and permissions with the identities available in the catalog, while configuring the template, in the **Collect Account** view, use `mail` as the **Account-User Mapping** attribute and `email` as the **Map to attribute**. In the **Collect Permission** view, use `member` as the **Permission-Account or User Mapping** attribute and `Account ID from Source` as the **Map to attribute**.

Identity Governance also provides eDirectory and AD hybrid collectors for collecting permissions. For more information about hybrid collectors, see Section 8.4, “Understanding Hybrid Permission Collectors,” on page 91.

17.1.2 About Active Directory and eDirectory LDAP Fulfillment

If a user is present in Identity Governance but is not present in either Active Directory or eDirectory, you can configure the fulfillment target to create an account through the respective fulfillment targets.

NOTE: Before you configure a fulfillment target with either an Active Directory LDAP fulfillment type or an eDirectory LDAP fulfillment type, you must ensure that Active Directory collects the attributes required for fulfillment. To verify Active Directory or eDirectory LDAP collection, log in to Identity Governance and then click **Data Sources** > **Application Definition Sources**.

To configure the fulfillment target, in Step 4b on page 139, you must provide values for the **first name**, **last name**, **title**, and **workforceID** fields.

In addition, when you configure **Fulfillment item configuration and mapping**, click **{...}**, then edit the transform script for the **Account name generation payload** to connect to the correct Active Directory or eDirectory server for the user.

17.2 Understanding and Configuring Azure AD MS Graph Templates

Identity Governance provides the following templates for Azure AD MS Graph:

- Azure AD MS Graph Identity
- Azure AD MS Graph Account

- Azure AD MS Graph Permission
- MS Azure AD Fulfillment

For additional information about configuring Azure AD templates, see the following sections:

- Section 17.2.1, “About Azure AD Collectors,” on page 186
- Section 17.2.2, “About Azure AD MS Graph Fulfillment,” on page 188

17.2.1 About Azure AD Collectors

When your environment uses both Active Directory and Azure AD, user identities might be unique to one of the applications or might exist in both applications. If you use Active Directory and Azure AD with DirSync or AD Connect, you can create a single identity source for both applications by using the Azure AD User collector template.

In the collector template, specify an attribute that you want to use for merging duplicate identities and for matching identities to accounts and permissions. The attribute for the matching rule should contain a value that is unique to each identity. For example, in AD and Identity Manager, each user tends to have a unique `Distinguished Name`.

IMPORTANT: We have deprecated the 3.6.2 Azure AD User templates because Azure AD Graph is no longer supported by Microsoft. If you are still using the old Azure AD templates, you can reconfigure your template to map to the Microsoft Graph API by changing the **Azure AD Service Resource** default value to `https://graph.microsoft.com/v1.0`. For information about the differences between the previously supported API and Microsoft Graph API, see https://docs.microsoft.com/en-us/graph/migrate-azure-ad-graph-property-differences.

When using the Azure AD MS Graph collector, complete the following steps:

1. Enable the Azure Microsoft Graph API for your site and grant the following permissions to an account to access the API:

Permission	Types	Description
Application.Read.All	Application	Read all applications
Device.Read.All	Application	Read all devices
Directory.AccessAsUser.All	Delegated	Access the directory as the signed-in user
Directory.Read.All	Application and Delegated	Read directory data
Domain.Read.All	Delegated	Read domains
Group.Read.All	Application and Delegated	Read all groups
GroupMember.Read.All	Application and Delegated	Read group memberships
RoleManagement.Read.All	Delegated	Read role management data for all RBAC providers
RoleManagement.Read.CloudPC	Delegated	Read Cloud PC RBAC settings
RoleManagement.Read.Directory	Delegated	Read directory RBAC settings
User.Read	Delegated	Sign in and read the user profile
User.Read.All	Application and Delegated	Read all user profiles
User.ReadBasic.All	Delegated	Read all users' basic profiles

2 Verify that you can browse your Azure domain with the graph explorer using the account from Step 1. For more information, see https://developer.microsoft.com/en-us/graph/graph-explorer.

Identity Governance uses the Azure AD MS Graph collector to collect information from the SharePoint Team site. When you create a SharePoint Team site, a Microsoft 365 group is automatically created, and any user that you add or remove from the SharePoint Team site is added or removed from the Microsoft 365 group and vice versa. These details are saved in Azure as a group. During data collection, Identity Governance collects information as a group from the Azure portal, and whenever there is a collection, Identity Governance collects the SharePoint Team site information as part of the group collection.

NOTE: Only the SharePoint Team site is supported. Identity Governance does not support SharePoint Communication site.

17.2.2 About Azure AD MS Graph Fulfillment

Identity Governance uses the Azure AD MS Graph fulfiller to automatically assign or remove permissions from user accounts and add or remove members from Microsoft 365 and Security groups. Identity Governance does not support adding or removing members from the Distribution List and Mail-enabled Security type of groups because Mail-enabled and distribution groups cannot be managed by Microsoft Graph group APIs.

The template supports the following fulfillment change requests:

- `ADD_APPLICATION_TO_USER`
- `ADD_PERMISSION_TO_USER`
- `REMOVE_ACCOUNT_PERMISSION`
- `REMOVE_PERMISSION_ASSIGNMENT`
- `REMOVE_ACCOUNT`
- `REMOVE_APPLICATION_FROM_USER`
- `REMOVE_ACCOUNT_ASSIGNMENT`

The Azure MS Graph fulfiller has default mapping for some mandatory attributes. The Azure application requires these mandatory attributes to create an account. For the fulfillment to process successfully, you must add these mandatory attributes to the Fulfillment Context attribute. The following table provides the list of attributes.

Fulfillment Context Attributes	Attributes
Recipient	• User ID from Source • Last Name • First Name • Full Name • Email • Employee Status
Account	• Account ID from Source • Account Disabled
Permission	• Permission Type • Permission ID from Source

NOTE: We recommend that while adding users to the Azure application, you provide a unique `mailNickName` for each user. The purpose of this is to prevent the error that can occur when you try to add users with the same first and last name. The ECMA script includes the logic for creating the unique `mailNickName`, but you can customize it to meet your requirements.

In addition to this list of attributes, you can configure other attributes in the collector template such as department, title, job codes, or workforce ID to match the requirements of your application. However, you must add them to the Fulfillment Context attribute. In addition, while configuring the fulfiller, go to **Fulfillment item configuration and mapping**, click **{..}**, then edit the transform script for **User Profile.**

In the transform script, you must add the native application key as `outUserProfile` and add the corresponding fulfillment context attribute key in the `outUserProfile` value. For example, for the attribute Workforce ID, edit the transform script to:

```
if(inUserProfile.workforceId) outUserProfile["employeeId"] =
inUserProfile.workforceId
```

NOTE: If you want to specify Workforce ID as the attribute for matching identities to accounts and permissions, then while configuring the collector template you must map Workforce ID to the native ID value, for example, `employeeId`, and set it as the matching rule.

Identity Governance uses the Azure AD MS Graph fulfiller to provision and deprovision users as a group from the SharePoint Team site. The following change requests are supported when provisioning and deprovisioning users as a group from the SharePoint Team site:

- `ADD_PERMISSION_TO_USER`
- `REMOVE_ACCOUNT_PERMISSION`
- `REMOVE_ PERMISSION_ASSIGNMENT`

17.3 Understanding and Configuring CSV Templates

Identity Governance provides the following templates for CSV:

- CSV Identity
- CSV Account
- CSV Permission
- CSV Fulfillment

For additional information about configuring CSV templates, see the following sections:

- Section 17.3.1, “About CSV Collectors,” on page 189
- Section 17.3.2, “About CSV Fulfillment,” on page 190

17.3.1 About CSV Collectors

A CSV file provides a simple method for storing user account or permissions information that cannot be collected from other data sources. You can include group, account, permission, or user data in the file. For all CSV collections, data administrators need to generate the CSV and make it available to the Identity Governance service through a file share, http, or local file system. To collect from a CSV file, you must specify the full path to the file.

When configuring the CSV collector:

- Start the root path file on the Services Parameters section of the template page with `/conf` and end with `/`. For example, `/conf/`.
- If you placed the CSV file in subfolders, append the subfolder names to the root file path. For example, `/conf/csv/oracle/`.
- Enter the CSV file name in the Collect Views section of the template page. For example, `users.csv` or `http://`*`ipaddress`*`/users.csv`

If you use a CSV file as an identity source, you might also want to instruct Identity Governance to map the collected users to their collected group memberships. The **Group Members (Users and Groups)** setting allows you to specify an attribute in the CSV file that you want to use for mapping users and groups to groups. However, you can use this setting only when a given value for the specified attribute is not used to identify both a user and a group. For example, if you export data from Active Directory to the CSV file, you can use DN as the Group Members attribute. Otherwise, you can use **Collect Group to User Membership** or **Collect Parent Group to Child Group Relationships** to map users or groups to groups. These two settings match the specified attribute in the collected user or group data, respectively.

In preparing a CSV file, ensure that any values written into a column of the file do not contain any carriage returns and line feeds, since these characters define record boundaries in the CSV file.

NOTE: The CSV collector supports TSV files. In the **Column Delimiter** field, enter the word `tab` in uppercase, lowercase, or any combination thereof. To collect from a CSV file, you must specify the full path to the file. Collection is not supported when the CSV collector is accessed through HTTPS connection.

17.3.2 About CSV Fulfillment

This fulfillment target creates a CSV file in the specified directory that contains the attributes you configured in the fulfillment target.

17.4 Understanding and Configuring Google Apps Templates

Identity Governance provides the following templates for Google Apps:

- Google Apps User Identity
- Google Apps User Account
- Google Apps User Permission

Google Apps manages users, groups, and organizational units, including assigned roles and privileges. Collecting identities from Google Apps is similar to other data sources. However, to collect permissions, Identity Governance pulls information from Google Groups, which resembles discussion-based groups similar to those available in Usenet.

To gather information about actual user groups, Identity Governance collects from the Organizations (organizational units) in Google Apps. These organizational units can contain nested units. The top-level organization is always called ‘root.’ During collection, Identity Governance translates the organizational units into Identity Governance-style groups. In Identity Governance, the root group lists all the users in that organizational unit. If you select one of the nested groups under the root group, Identity Governance lists only the individuals assigned to that group.

17.5 Understanding and Configuring Identity Manager Templates

Identity Governance provides the following templates for Identity Manager:

- Identity Manager Identity
- Identity Manager Account
- Identity Manager AE Permission
- Identity Manager Automated Fulfillment
- Identity Manager Workflow
- IDM Entitlement Account
- IDM Entitlement Permission
- IDM Entitlement Fulfillment
- Identity Manager Dxcmd Fulfillment for Active Directory

For additional information about configuring Identity Manager templates, see the following sections:

- Section 17.5.1, “Understanding Authentication Methods for IDM AE Permission Collectors and IDM Automated Fulfillment Targets,” on page 191
- Section 17.5.2, “About Identity Manager AE Permission Collectors,” on page 192
- Section 17.5.3, “About Identity Manager Automated Fulfillment,” on page 192
- Section 17.5.4, “About Identity Manager Entitlement Collectors,” on page 193
- Section 17.5.5, “About IDM Entitlement Fulfillment,” on page 193

17.5.1 Understanding Authentication Methods for IDM AE Permission Collectors and IDM Automated Fulfillment Targets

The Identity Manager AE Permission collector requires both LDAP and user application credentials. All objects including roles collected using this collector are represented as permissions in the Identity Governance catalog. Note that the Identity Manager Automated Fulfillment fulfiller also uses the same credentials.

Use the following table to understand the order that you need to specify for this collector.

Authentication Type	Credential Set
LDAP	◆ User Name used to connect to Identity Vault Server (cn=admin,ou=sa,o=system) ◆ Password
User Application	◆ User Name used to connect to User Application (cn=uaadmin,ou=sa,o=data) ◆ Password

17.5.2 About Identity Manager AE Permission Collectors

The Identity Manager AE Permission collector is an Application Source collector that creates the base Identity Manager application in Identity Governance and automatically generates subordinate applications that represent IDM Drivers, such as the CloudAD Driver and SAP User Management Driver, that support Identity Manager entitlements.

IMPORTANT: No other application source permission collector provides *automatic generation* of subordinate applications or accounts. This collector uses both LDAP calls into eDirectory and SOAP calls to the user applications to collect data. Due to the complexity of the relationships managed by this collector, proceed with caution when changing the default values and mappings.

Before collecting Identity Manager AE permissions, ensure that you have installed Identity Manager applications. Additionally, when using AD Driver with Identity Manager AE, ensure that the Remote Loader is running.

When configuring service parameters, ensure that you include the port number that you use to connect to your Identity Manager system in the **User Application Base Provisioning Service URL** field. Enter comma-separated values in the **Additional permission attributes to collect** field when you want to collect multiple attributes from Roles, Resources, Groups, and Container-type permissions in addition to the default attributes. When adding these additional permission attributes, you must also include the attributes in the collector views.

When the Identity Manager AE Permission collector collects any User record from the Identity Manager application that has an association with a subordinate application (through the DirXML Association attribute on the User), it receives an Account assignment for that subordinate application. The Identity Manager AE Permission collector also automatically maps the User record to the Identity Manager User.

If, after testing the connection and collecting data, you do not see the expected data in the Identity Governance Catalog, verify that your **Account Collect LDAP Search Filter** is configured correctly in the template, then use LDAP search from the command line or LDAP browser to confirm that the missing data is still available in your data source. You can also directly call the SOAP endpoint to get the refreshed values of the Identity Manager AE system attributes that are used for mapping.

17.5.3 About Identity Manager Automated Fulfillment

The Identity Manager Automated Fulfillment template enables automatic fulfillment of change requests related to Identity Manager AE permissions. Specify whether you want to use automated provisioning with manual fulfillment or a workflow as the fallback method, then specify the values associated with the fallback method. For more information, see Section 13.6.3, “Automatically Fulfilling the Changeset,” on page 148.

NOTE: When an Identity Manager AE permission is requested in the Identity Governance Access Request, the `idmDn` attribute of the requesting user is utilized in the RBPM SOAP request as the `<ser:requester>`. If this value is *not* a valid user DN in the target Identity Manager system, the fulfillment request will fail.

17.5.4 About Identity Manager Entitlement Collectors

The Identity Manager Entitlement collectors are for users who want to use Identity Governance to provision or revoke accounts and permissions. The entitlement collectors collect accounts and permissions from Identity Manager using IDM drivers that support entitlements such as Azure, Workday, and SCIM drivers. Like the other Identity Governance collectors, the entitlement collectors map accounts and permissions to identities by association or other attributes. To successfully collect accounts and permissions:

- You must have collected identities from Identity Manager, and
- All supported drivers must be running

NOTE: For the list of supported drivers, see *Identity Governance Technical Requirements*.

You can use the account collectors to collect accounts and the permission collectors to collect permissions and their assignments. For example, the permission collector can collect the building access permission (list of buildings) and assignments (who can access the building).

In addition to IDM credentials, the LDAP distinguished name of the entitlement in the IDM driver is also a mandatory field for the entitlement collectors.

Typically, attribute mappings are preconfigured and have built-in fallback options. For example, by default, the collector maps the account or permission name to the IDM display name. If the collection process does not find the display name, the collector automatically maps the account or permission name to other available attributes such as the description. However, you do need to change the default **Account-User Mapping** value GUID to **Object GUID** and the default **Permission-Account or User Mapping** value association to **Account ID from source.**

17.5.5 About IDM Entitlement Fulfillment

The IDM Entitlement fulfillment target supports only the following fulfillment change requests:

- `ADD_APPLICATION_TO_USER`
- `ADD_PERMISSION_TO_USER`
- `REMOVE_ACCOUNT_PERMISSION`
- `REMOVE_PERMISSION_ASSIGNMENT`
- `REMOVE_ACCOUNT`

When a change request is sent to Identity Manager for fulfillment, the fulfiller modifies the User Attribute `DirXML-EntitlementRef`. The IDM engine then sends an event to the driver to ensure that the entitlement is fulfilled.

To successfully fulfill entitlement-related change requests:

- Identities must have been collected from Identity Manager
- Users must still be present in Identity Manager
- All the fulfillment context attributes required for Recipient (User), Account, and Permission profiles must be specified

17.6 Understanding and Configuring JDBC Templates

Identity Governance provides the following templates for JDBC:

- JDBC Identity
- JDBC Account
- JDBC Permission

  The identity, account, and permission templates are divided are organized by database:

  - DB2
  - Generic
  - MySQL
  - Non-specific
  - Oracle
  - PostgreSQL
  - SQLServer
  - Sybase
- JDBC Generic DB Fulfillment
- JDBC Oracle Fulfillment
- JDBC PostgreSQL Fulfillment
- JDBC SQL Server Fulfillment

For additional information about configuring JDBC templates, see the following sections:

- Section 17.6.1, “About JDBC Collectors,” on page 194
- Section 17.6.2, “About JDBC Fulfillment,” on page 194

17.6.1 About JDBC Collectors

To collect data from a JDBC source, Identity Governance needs the appropriate third-party connector libraries to be installed on the Identity Governance server. For more information on required third-party libraries, see “Identity Governance Server System Requirements” in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

17.6.2 About JDBC Fulfillment

Identity Governance uses the JDBC, Oracle, SQL Server, and PostgreSQL fulfillment templates to automatically fulfill change requests. Identity Governance uses the generic fulfillment template for all other databases, such as MySQL or SyBase. The appropriate third-party connector libraries must be installed on the Identity Governance server before you can use the JDBC generic fulfillment template. The generic template allows you to edit the transform script that builds the required payload to successfully process change requests.

The JDBC fulfillment template supports all change requests. The JDBC fulfillment is certified with the following database versions:

JDBC fulfillment type	Supported version
JDBC Oracle	Oracle 19c
JDBC PostgreSQL	PostgreSQL 14
JDBC SQL Server	MS SQL 2019
JDBC Generic DB	MySQL 8.0.x

17.7 Understanding and Configuring PAM Templates

Identity Governance provides the following templates for PAM:

- PAM Account
- PAM Permission

NOTE: The PAM application must have a minimum version of 4.4 and above for you to collect accounts and permissions using the PAM collector.

For additional information about configuring PAM templates, see the following sections:

- Section 17.7.1, “Required Minimum Rights for Integration with PAM,” on page 195
- Section 17.7.2, “About PAM Account Collector,” on page 195

17.7.1 Required Minimum Rights for Integration with PAM

To ensure data is mapped successfully from PAM to the Identity Governance catalog, the users in PAM must have the required minimum rights in the PAM application. The user can be a local user of PAM or an LDAP user to run the APIs for user roles, resource pools, and assignments. However, the user must be added as a group member or must be mapped to a group and have the `View Access Control Objects` permission in the PAM application.

17.7.2 About PAM Account Collector

NetIQ Privileged Account Manager (PAM) manages and monitors administrative access to servers, networks, and databases to any target application through its access control objects, such as user roles, resources, resource pool, and assignments.

User roles and resource pools are logical groupings, where user roles are allocated permissions to access resources. These resources, in turn, are organized within a resource pool. PAM utilizes the assignments to establish a connection between user roles and the associated resource pool.

The PAM account collector collects unique members and group members from all user roles, and the permission collector collects user roles and members included in the role, resource pool, and the user role-resource pool parent-child relationship. These accounts and permissions are mapped to identities by association or other attributes. Note that PAM uses LDAP as its identity source, so, the PAM collector maps only LDAP accounts to identities.

When configuring the PAM account Collector, configure service parameters as needed, then specify the Account-User Mapping parameter as “id” and map it to the identity attribute which holds the objID. Optionally, if you want the PAM accounts to be populated uniquely in the Identity Governance catalog, then in the Collect Account View for Mapped Attributes specify the PAM attributes for example, ID which is unique to PAM account. Then write an ECMA script for the Collect Account attributes for example:

```
[outputValue = "NetiqPAM" + inputValue]
```

When configuring the PAM Permission Collector, configure service parameters, then depending on the type of permission you want to collect, select the permission type separately for User Role and Resource Pool and specify if you want to collect disable permissions.

- To map the permissions to an account, specify Permission-Account or User Mapping parameter value as “ids” and map it to Account ID.
- To collect the parent-child relationship between User Role and Resource pool, specify the Parent Permission ID value as `parentPermission`.

17.8 Understanding and Configuring MS Teams Templates

Identity Governance provides the following templates for MS Teams:

- MS Teams Permission Collector
- MS Teams Fulfillment

For additional information about configuring MS Teams templates, see the following sections:

- Section 17.8.1, “About Microsoft Teams Collectors,” on page 196
- Section 17.8.2, “About Microsoft Teams Fulfillment,” on page 198

17.8.1 About Microsoft Teams Collectors

The Microsoft Teams application is a subordinate application and uses the Azure Active Directory database. It consists of teams and channels with members of their own. MS Teams further divides members into team and channel members, or team and channel owners, with higher privileges. Teams are public and private and channels are standard and private. Each team can have a number of channels with one default standard channel.

While collecting data from the Microsoft Teams application, you must use the Azure AD MS Graph collector for collecting accounts and identities and use the MS Teams collector to collect teams, channels, their members, and the associated permissions. However, for the collector to work, you must have the following API permissions in Azure Active Directory.

Resource	Permission	Type	Description
Team	`TeamSettings.Read.Group`	Application	Read team’s settings
	`TeamSettings.ReadWrite.Group`	Application	Read and write team's settings
	`User.Read.All`	Application	Read all user profiles

Resource	Permission	Type	Description
	User.ReadWrite.All	Application	Read and write all user profiles
	Team.ReadBasic.All	Application and Delegated	Read names and descriptions of all teams
	TeamSettings.Read.All	Application and Delegated	Read all teams settings
	TeamSettings.ReadWrite.All	Application and Delegated	Read and change all teams settings
	Group.Read.All	Application and Delegated	Read all groups
	Group.ReadWrite.All	Application and Delegated	Read and write all groups
	Directory.Read.All	Application and Delegated	Read all directory data
	Directory.ReadWrite.All	Application and Delegated	Read and write directory data
	Directory.AccessAsUser.All	Application	Access the directory as the signed-in user
	TeamMember.Read.Group	Application	Read team's members
	TeamMember.Read.All	Application and Delegated	Read all team members
	TeamMember.ReadWrite.All	Application and Delegated	Add, remove, and change roles for members of all teams
	TeamMember.ReadWriteNonOwnerRole.All	Application	Add and remove members with non-owner roles for all teams
Channel	ChannelSettings.Read.Group	Application	Read channel data of a team
	ChannelSettings.ReadWrite.Group	Application	Update channel data of a team
	Channel.ReadBasic.All	Application and Delegated	Read all channel names and descriptions
	ChannelSettings.Read.All	Application and Delegated	Read all channel data of a team
	ChannelSettings.ReadWrite.All	Application and Delegated	Read and write all channel data
	Group.Read.All	Application and Delegated	Read all groups
	Group.ReadWrite.All	Application and Delegated	Read and write all groups
	Directory.Read.All	Application and Delegated	Read directory data
	Directory.ReadWrite.All	Application and Delegated	Read and write directory data
	ChannelMember.Read.All	Application and Delegated	Read channel members

Resource	Permission	Type	Description
	ChannelMember.ReadWrite.All	Application and Delegated	Add, remove, and change roles for members of all channels

IMPORTANT: The Microsoft Teams collector does not collect data for itself. So, you *must* enable the Azure Active Directory data source to collect permissions from MS Teams.

You have the option to configure the MS Teams collector as a hierarchical structure and map the attribute **Unique Application ID** with the `applicationId`. Ensure that the `outputValue` in the ECMA script is mapped to the name of the collector. For example, `outputValue='MS_Teams'`. Also, configure the MS Teams Permission collector template mandatory attribute mappings, such as `ID`, and `objectType`. ID is the unique ID from a team or a channel, and objectType indicates whether the object is for teams or channels.

Occasionally, while collecting data using the MS Teams collector, the collection might fail with an error message. This occurs because of issues such as an application timeout when the response from the Microsoft Teams API takes a long time to return or a backend error when the Microsoft Teams API is not able to process the request. Check your configuration, change the timeout value, view logs and audit events, and try again.

17.8.2 About Microsoft Teams Fulfillment

If you have the appropriate permissions in Azure Active Directory, you can fulfill the following change requests:

- `ADD PERMISSION TO USER`
- `REMOVE ACCOUNT PERMISSION`
- `REMOVE PERMISSION ASSIGNMENT`

You can add or remove a member only from a private channel. However, before adding a member to a channel, ensure that the member is already a part of the team. When you add a user to a team, the Microsoft Teams fulfiller adds the user automatically to all standard channels under the team, as a member.

NOTE: To avoid unexpected behavior from the application, we recommend that you do not add a team and a channel member in the same request.

You can assign the user the role of an owner. To do so, you need to customize the request form and add ‘owner’ as **Data Source Values** and ‘roles’ as **Label**, then publish the form. This will allow you to select the role as ‘owner’ when you request permission for the user. For information about customizing forms using Form Builder, see Creating a Request or Approval Form. Additionally, while configuring **Fulfillment item configuration and mapping** in the template, you must add `"flowdata"` for the attribute **Permission Profile**. For example, add `["flowdata", "permissionProfile"]`.

NOTE: To assign a user as an owner you need to create custom forms for each team and channel separately.

For the fulfillment to process successfully, you must add the following attributes to the fulfillment context attribute:

Fulfillment Context Attributes	Attributes
Recipient	◆ User ID from Source ◆ Full Name ◆ Employee Status ◆ Last Name ◆ First Name ◆ Email
Account	◆ Account ID from Source ◆ Account Disabled
Permission	◆ Permission Type ◆ Permission ID from Source ◆ Permission Name

17.9 Understanding and Configuring REST GitHub Templates

Identity Governance provides the following templates for GitHub:

- REST GitHub Account
- REST GitHub Organization Permission
- REST GitHub Repository Permission
- REST GitHub Team Permission
- REST GitHub Fulfillment

For additional information about configuring REST GitHub and Generic templates, see the following sections:

- Section 17.9.1, “Required Minimum Rights for Integration with GitHub,” on page 199
- Section 17.9.2, “Understanding REST GitHub Authentication Methods,” on page 199
- Section 17.9.3, “About REST GitHub Collectors,” on page 200
- Section 17.9.4, “About REST GitHub Fulfillment,” on page 200

17.9.1 Required Minimum Rights for Integration with GitHub

To access all GitHub endpoints, you must use the credentials of a GitHub Enterprise Administrator, also known as the Site Administrator, for the authentication types.

17.9.2 Understanding REST GitHub Authentication Methods

The GitHub account and permission collector supports two authentication types: Basic Auth and Access Token. The collector collects all organizations.

Authentication Type	Credential Set
Basic Auth	◆ User Name ◆ Password
Access Token	◆ Access Token Header ◆ Access Token

IMPORTANT: For the access token, the user provides the token to connect to the target application, whereas, for the bearer token, the connector generates the token. When the access token expires, replace it with a new access token.

17.9.3 About REST GitHub Collectors

NOTE: Identity Governance currently supports GitHub Enterprise on-premises edition, version 3.8.3.

Like the other Identity Governance collectors, the REST GitHub collectors map accounts and permissions to identities by association or other attributes. To successfully map accounts and permissions to identities, identities must be collected using the identity source that is configured in the GIT server. The REST GitHub permission collector collects all organizations, teams, repositories, the permission to permission association, and also the holder association. The collector has a batch size limit of 100 records.

The REST GitHub collector template includes mandatory attribute mappings suitable for the target application. However, you can configure other attributes and then edit the transform script to build the required payload. For example, for GitHub accounts, if you want to map 'email' for the **Account-User Mapping** attribute, you need to map **Account-User Mapping** with `user` and write the script as follows to parse the email from the user JSON:

```
var user = JSON.parse(inputValue)

   outputValue = user['email'];
```

Apart from the mapped attributes, you can add other attributes for `organization` by parsing the values from the organization JSON. For `teams`, you can parse the values from the teams JSON and for `repository` from the repository JSON.

17.9.4 About REST GitHub Fulfillment

Identity Governance uses the REST GitHub fulfiller to add or remove members from an organization, or a team, or add or remove a collaborator from a repository. When a user is added to an organization or a team the default role assigned is of a "member", and for a repository, it is "read". However, members can log in to the GitHub application and change their roles as needed.

Users can get access to a repository directly as collaborators, or when they are members of an organization or a team. As members, they automatically inherit the permission to access the organization and team repositories. So, when you want to remove a collaborator from a repository, or a member from a team, ensure that the repository permission is not inherited from an

organization or a team. For the fulfillment verification to be successful, you must remove the member from the parent organization or team so the member loses the child permission, which means the repository permission.

NOTE: The term “collaborator” is specific to GitHub and it refers to a user who is given access to a repository directly. For more information, see the GitHub Docs (https://docs.github.com/en).

The REST GitHub fulfiller supports the following change requests:

- `ADD PERMISSION TO USER`
- `REMOVE PERMISSION ASSIGNMENT`
- `REMOVE PERMISSION FROM ACCOUNT`

For the fulfillment to process successfully, you must add these mandatory attributes to the Fulfillment Context attribute area. The following table provides the list of attributes.

Fulfillment Context Attributes	Attributes
Account	• Account ID from Source • Account Disabled • Account Aliases
Permission	• Permission ID from Source • Permission Type • Permission Name

17.10 Understanding and Configuring Salesforce Templates

Identity Governance provides the following templates for Salesforce:

- Salesforce Identity
- Salesforce Account
- Salesforce Permission
- Salesforce Profile Permission
- Salesforce Role Permission
- Salesforce Fulfillment

For additional information about configuring Salesforce templates, see the following sections:

- Section 17.10.1, “About Salesforce Collectors,” on page 202
- Section 17.10.2, “About Salesforce Fulfillment,” on page 202

17.10.1 About Salesforce Collectors

Using standard Identity Governance Salesforce collector templates, you can collect data from `User`, `UserRole`, and `Profile` objects. The `User` object is used for Salesforce Identity and Salesforce Account collectors as well as the permission-holder information in the permission collectors.

The generic Salesforce permission collector is configured by default to collect `UserRole` permissions. However, you can configure the collector to collect other permission types such as `UserLicense`, `PackageLicense`, `PermissionSetLicense`, `PermissionSet`, `PermissionSetGroup`, and `Profile`. For your convenience, Identity Governance also provides Salesforce Role Permission and Salesforce Profile Permission collector templates to collect only UserRole and Profile objects respectively.

17.10.2 About Salesforce Fulfillment

The Identity Governance Salesforce Fulfillment template provides a transformation policy that:

- Executes a query for a single existing user and creates a new Salesforce User if needed
- Assigns or revokes the following permission types: `UserRole`, `Profile`, `PackageLicense`, `PermissionSetLicense`, `PermissionSet`, and `PermissionSetGroup`

To assign some `PermissionSet` or `PermissionSetGroup` permissions, it might be necessary to assign an appropriate license first. We therefore recommend that you assign all licenses before you assign other permission types.

The default transformation policy also includes fulfillment attributes required for fulfillment operations. One required User attribute is **ProfileId**, which must contain the native ID value of a Profile permission. Since all Salesforce Users *must* have a Profile assignment at all times, it is your responsibility to provide a default ID that can be used for new Users or to reset a User whose profile has been removed by Identity Governance fulfillment actions. This attribute ID should replace the *`ID of default profile`* string in the transformation policy.

Depending on your operations, you might also need to specify additional Fulfillment Context attributes for `userProfile` and `permissionProfile`.

17.11 Understanding and Configuring SAP Templates

Identity Governance provides the following templates for SAP:

- SAP HR Identity
- SAP User Management Identity
- SAP User Management Account
- SAP User Management Permission

NOTE: Identity Governance does not currently support SAP collectors in the SaaS environment.

To collect data from an SAP source, Identity Governance needs the appropriate third-party connector libraries to be installed on the Identity Governance server. For more information, see "Identity Governance Server System Requirements" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

17.12 Understanding and Configuring SCIM Templates

The System for Cross-domain Identity Management (SCIM) is a protocol for identity exchange, especially across SaaS products. SCIM connectors enable Identity Governance to integrate with applications seamlessly and support multiple authentication methods.

Identity Governance provides the following templates for SCIM:

- SCIM Identity
- SCIM Account
- SCIM Permission
- SCIM Fulfillment

For additional information about configuring SCIM templates, see the following sections:

- Section 17.12.1, “Understanding SCIM Authentication Methods,” on page 203
- Section 17.12.2, “About SCIM Collectors,” on page 204
- Section 17.12.3, “About SCIM Fulfillment,” on page 205

17.12.1 Understanding SCIM Authentication Methods

SCIM connectors require a particularly complex configuration template that supports three different authentication types, each of which has different credential parameters that are required to properly configure the collectors and fulfillers. The choice of authentication type and grant type will depend on the use case and what the authentication token endpoint supports.

When using the bearer token authentication method, you can select **Password Flow** (when user involvement is required) or **Client Credential Flow** (for machine-to-machine communication) as the authentication grant type. When using the Password Flow, you will need to specify a username and password, then OAuth2 client ID and secret for API access to the SCIM-compatible application. When using the Client Credential Flow, you will need to specify whether the credentials should be included in the request header or request body and the client ID and secret. The process for

configuring the applications and generating the client ID and secret will vary depending on your data source. For additional information about getting the client ID and secret, contact the application owner.

The following table lists the available authentication types and related credentials.

Authentication Type	Credential Set
Basic Auth	◆ User Name ◆ Password
Access Token	◆ Access Token Header ◆ Access Token
Bearer Token	◆ User Name ◆ Password
Bearer Token	◆ Client ID ◆ Client Secret

IMPORTANT: For the access token, the user provides the token to connect to the SCIM-compatible application, whereas, for the bearer token, the connector generates the token. When the access token expires, replace it with a new access token.

17.12.2 About SCIM Collectors

The SCIM account and permission collectors use unique authentication methods. In addition to specifying the authentication method, you might need to change attribute mapping when configuring the template. SCIM supports singular, complex singular, complex multi-valued attributes, and extensions. However, if your application supports any other attributes or extensions different from those mentioned in the SCIM protocol, you can change the attribute mapping in the template by using delimiters. You can use ':' (colon) for attributes, for example, `emails:work:`*`value`*, and '+' (plus) for extensions, for example, `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User+`*`department`*.

To successfully map SCIM accounts and permissions to identities, you must use `email` as the mapping attribute during identity, accounts, and permissions collection. SCIM collects records in batches of up to 999 records, and the default batch collection session timeout value is set to 60 seconds.

By default, the generic SCIM permission collector collects groups as permission for the resource type. However, you can configure the collector to collect other permissions by setting the Resource Type and mapping the attributes of that resource type. For example, if you want to add printers as permission you can give the endpoint of that resource type and map the required attributes to perform the collection.

17.12.3 About SCIM Fulfillment

Identity Governance uses the System for Cross-domain Identity Management (SCIM) fulfillment template for managing identities, and fulfilling change requests for permissions and accounts, especially across SaaS products. Based on the SCIM protocol, the SCIM fulfiller has default attribute mapping that helps you fulfill requests. However, you can change these mappings to match the requirements of your application.

The SCIM fulfiller template allows you to edit the transform script to build the required payload for the change requests for generic fulfillment, user profiles, permissions, and accounts. The ECMA script includes comments that guide you through the payload generation process. After you generate the payload, Identity Governance sends the payload for fulfillment. The SCIM fulfiller generates the payload for the following change requests:

- `ADD_APPLICATION_TO_USER`
- `ADD_PERMISSION_TO_USER`
- `REMOVE_ACCOUNT_PERMISSION`
- `REMOVE_PERMISSION_ASSIGNMENT`
- `REMOVE_ACCOUNT`

17.13 Understanding and Configuring ServiceNow Templates

Identity Governance provides the following templates for ServiceNow:

- ServiceNow Identity
- ServiceNow Account
- ServiceNow Permission
- ServiceNow Generic Fulfillment
- ServiceNow Incident Fulfillment
- ServiceNow Request Fulfillment
- ServiceNow Task Fulfillment

For additional information about configuring ServiceNow templates, see the following sections:

- Section 17.13.1, “About ServiceNow Collectors,” on page 206
- Section 17.13.2, “About ServiceNow Fulfillment,” on page 206

17.13.1 About ServiceNow Collectors

Collection from the ServiceNow portal is similar to other identity and application data sources. When you are configuring the templates, we recommend that you map the User ID from Source, Account ID from Source, and Permission ID from Source attributes to a unique identifier, for example, `sys_ID` as the mapping attribute. After collecting data, Identity Governance maps accounts and permissions to identities by association or other attributes.

17.13.2 About ServiceNow Fulfillment

Identity Governance provides four distinct ServiceNow fulfillment target types: Generic, Incident, Request, and Task. Whereas the Identity Governance fulfillment targets are meant to provision or deprovision an application or permission to a user, the ServiceNow fulfillment types have a different purpose. Depending on your organization's requirements, select the template from the list that best suits your needs:

- Select the *generic* fulfillment type if you need customization that the other fulfillment types allow. In the out-of-the-box scenario, the generic fulfillment type generates an incident. It takes information from the Identity Governance change request item and then uses an ECMA script to create a SOAP XML payload which is then sent to ServiceNow.
- Select the *incident* fulfillment type to create a ServiceNow incident to process each change request item. Fulfillment verification happens at the incident level.
- Select the *request* fulfillment type is used to create a ServiceNow request to process each change request item. Fulfillment verification happens at the request level.
- Select the *task* fulfillment type to group fulfillment items together based on the user. It creates a hierarchy of ServiceNow request, request items, and tasks. Here one request contains one to n request items grouped by user. Inside each request item, there are tasks for the actual change request item. Fulfillment verification happens at the task level.

The fulfillment status from these fulfillment types remain in the pending verification state. After the request is approved, the status in Identity Governance changes to verified.

17.14 Understanding and Configuring SharePoint Templates

Identity Governance provides the following templates for Sharepoint:

- Sharepoint Identity
- Sharepoint Account

Microsoft SharePoint is a browser-based collaboration and document management tool that allows administrators to grant specified access rights to individual users and groups.

To gather information from SharePoint, the Service Account you use to configure the SharePoint collection must be a member of the WSS_ADMIN_WPG local group on the SharePoint server.

NOTE: Identity Governance does not support using the SharePoint collector for SharePoint Online.

17.15 Understanding and Configuring Workday Templates

Identity Governance provides the following templates for Workday:

- Workday Identity
- Workday Account
- Workday Permission
- Workday Fulfillment

Before configuring these templates, create an integration account and ensure that the minimum rights required to integrate with Workday systems are assigned to the integration groups and users in the Workday application.

For additional information about configuring Workday templates, see the following sections:

- Section 17.15.1, “Required Minimum Rights for Integration with Workday,” on page 207
- Section 17.15.2, “About Workday Collectors,” on page 207

17.15.1 Required Minimum Rights for Integration with Workday

The three minimum security domain rights that must be assigned to the integration group and users to get the data necessary for the default mappings in the Workday Identity Collector are:

- Person Data: ID Information
- Worker Data: Public Worker Reports
- Workday Accounts

The following rights are required to collect the necessary data for the default mappings in the Workday Application Collector:

- Account collector
  - Workday Accounts
  - Worker Data: Public Worker Reports
- Permission collector
  - Manage: Organization Roles
  - Org Designs: Assign Roles
  - User-Based Security Group Administration
  - Manager: Organization Integration

17.15.2 About Workday Collectors

Security groups control access to data in Workday. Security groups are a collection of users or of objects that are related to users. Identity Governance provides default templates for the Workday account and permission collections. Workday permission collectors support two types of permission collections: User Based Security Group and Role Based Permissions. Role-based permissions are

always associated with a specific organization. When using role-based permission collectors, you can also collect permission hierarchy. Collected role-based permission in the catalog includes role name, permission, and organization as the name of the permission, and displays permission relationships.

When configuring the Workday Account Collector, configure service parameters as needed, then specify the Account-User Mapping parameter as `WorkdayUserName` and map it to `Object GUID` to join accounts to identities.

When configuring the Workday Permission Collector, configure service parameters, then select the permission type.

- To collect user-based security group permissions, specify the Permission-Account or User Mapping parameter value as `WorkdayUserName` and map it to `Account Name` to join permissions to the account.
- To collect role-based permissions, specify the Permission-Account or User Mapping value as `WorkforceID` and map it to `Workforce ID` to map permissions to identities. Additionally, leave the organization type blank to collect all role-based permissions or specify an organization type to collect permissions associated with an organization.

  When specifying a specific organization, to collect the hierarchy of role-based permissions using the organization hierarchy, map the Parent Permission ID to `wd-superior_organization`. Mapping this will collect and establish the child/parent permission relationship for role-based permissions.

17.16 About REST Generic Fulfillment

The REST Generic fulfiller supports Oauth 2.0 and has three different authentication types: basic, generate bearer token, and enter access token. When using the bearer token authentication method, you must specify the username and password, then the OAuth2 client ID and secret for API access to the target application. The process for configuring the applications and generating the client ID and secret will vary depending on your target application. For additional information about getting the client ID and secret, contact the application owner.

Authentication Type	Credential Set
Basic Auth	◆ User Name ◆ Password
Access Token	◆ Access Token Header ◆ Access Token
Bearer Token	◆ User Name ◆ Password
Bearer Token	◆ Client ID ◆ Client Secret

Identity Governance uses the REST Generic fulfiller for fulfilling requests for any REST-based application using REST endpoints. This fulfiller also supports OAuth 2.0. The REST Generic fulfillment template allows you to customize the template. While configuring the **Fulfillment Item configuration and mapping,** click **{..}** for **Content**, then specify the `service_method` and the `http_body`.

17.17 About Workflow Service Fulfillment

Identity Governance uses the Workflow Service fulfillment target to get a workflow from the Workflow Service and run the workflow to fulfill changesets. You can either use an existing workflow or create a workflow in Identity Governance. Identity Governance then sends the `changeitemid` to the Workflow Service to process the fulfillment.

NOTE: To edit the workflow, click the **Edit** link next to the **Workflow** field to launch the Workflow Builder in the Workflow Administration Console. In the Workflow Builder, ensure that the default IGA fulfillment request form is selected for the fulfillment request to complete. Using any other form for your fulfillment request might result in unpredictable behavior.

The Workflow Service identifies the entity, parses the information, and completes the task. The Workflow Service, however, does not inform Identity Governance when the task finishes. To check the fulfillment steps or fulfillment status, select **Fulfillment** > **Status** or **Requests** > **Requests**.

18 Creating and Managing Technical Roles

Technical roles allow business owners to simplify the review process by grouping permissions, which provides a higher level of abstraction and reduces the number of items for business leaders to review. Technical roles allow the business to provide context for the set of items including a business-relevant title and description, risk, cost, and ownership.

18.1 Overview of Roles

Identity Governance enables you to manage both the technical and business roles in your organization. To enable easier management of these roles, Identity Governance assigns technical role administrators and business role administrators with separate but overlapping responsibilities.

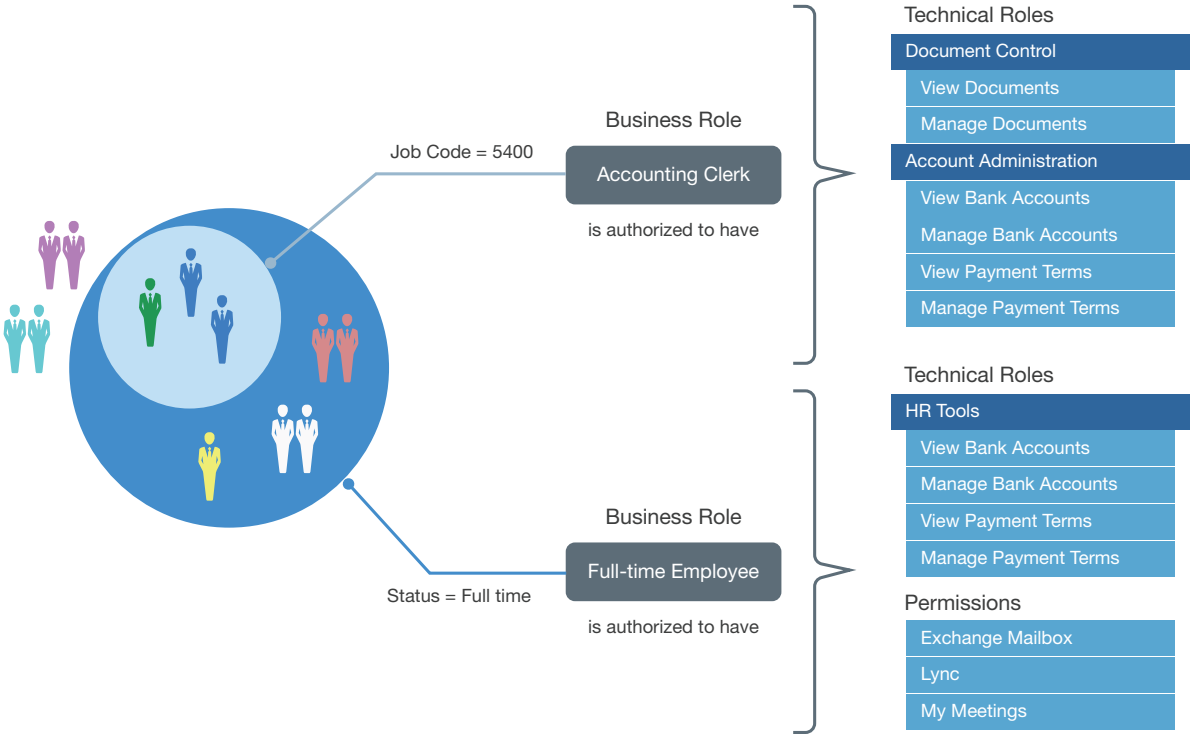
Business roles organize people by business function, and user-based attributes to determine what users should have access to, or if they can request that access without additional approval. Business roles authorize **resources** (permissions, technical roles, and applications) for users who are members of the business role. These authorizations also specify whether resources are to be auto-granted to users, auto-revoked from users, or should not be auto-granted and auto-revoked.

Technical roles organize lower-level permissions into sets of permissions that offer enough business value to be reviewed and assigned as a unit or requested as a unit. Technical roles are designed to limit the number of review items and surface permissions in ways that can be presented to typical non-administrator users.

Figure 18-1 illustrates how the different types of roles overlap. In this example, company policies authorize all full-time employees to have access to the HR Tools, Exchange Mailboxes, Lync, and My Meeting. Accounting clerks are authorized to have access to Document Control and Account Administration, a technical role that the technical role administrator created in Identity Governance. When you include a user as a member of a business role of Full-time Employee and Accounting

Clerk, Identity Governance authorizes the user to have any of the mandatory or optional technical roles or permissions listed for the given role. Identity Governance could potentially automatically provision mandatory permissions, while it could assign optional permissions at a later time without further approval, because they are pre-approved by the policy. This example illustrates how you can save time, effort, and error, and enable controlled access through business roles. To understand how your entitlement assignments conform to your business policies, you can view the Role Effectiveness widget on the Governance Overview dashboard. For more information, see "Viewing Entitlement Assignments Statistics to Leverage Roles" on page 386.

Figure 18-1 *Detailed Example of the Overlap between Business Roles and Technical Roles*



NOTE: This chapter primarily discusses technical role policy concepts and procedures. For information about business roles, see Chapter 19, "Creating and Managing Business Roles," on page 229.

18.2 Understanding Technical Roles

To manage the Identity Governance technical roles in the catalog, you must be a Customer, Global, or Technical Role Administrator. Administrators can also assign an owner for a technical role and delegate certain tasks to the technical owner. For detailed information about the various authorizations, see Section 2.1, "Understanding Authorizations in Identity Governance," on page 19.

After a Customer, Global, or Data Administrator publishes application data, you can create technical roles by grouping permissions that have common or frequent associations. After you create technical roles, Identity Governance detects users with permissions that match the technical roles you defined and lists the technical roles a user has in the user catalog. After you define technical roles, you can create user access review definitions for technical role reviews.

Users are members of a technical role either by detection, assignment or both. A user who has all of the permissions contained in a technical role has the technical role by detection. Having a technical role by assignment means that the user was explicitly assigned the technical role by a process in Identity Governance, such as an access request or a business role auto-grant.

Technical roles might be authorized in a business role for the members of the business role. If an authorized technical role was configured for auto-grant, Identity Governance will immediately assign the technical role to members of the business role. In addition, Identity Governance will issue requests for any permissions contained in the technical role for members of the business role. If the authorized technical role was configured for auto-revoke, and a user is removed from business role membership, Identity Governance will immediately remove the technical role assignment from the user, and will request that any permissions contained in the technical role be removed from the user. For information about business roles and automatic access provisioning and deprovisioning, see Chapter 19, “Creating and Managing Business Roles,” on page 229.

Technical roles cannot be deactivated if they form part of any governance policy such as business roles, SoD, access request, or access request approval policy. A deactivated technical role which references a business role, SoD, access request, or access request approval policy, must be activated before any of those policies are imported.

18.3 Understanding Technical Role States

Administrators can quickly search for a role by name or description in the **Catalog > Roles** page. Identity Governance performs a case-insensitive search of all of the technical roles in the catalog and returns any that contain the string in the technical role name, description, or cost. You can also use the advanced search feature to limit the number of roles. The search results also display the role states.

The life cycle of a technical role includes the following states, regardless of how the role was created:

Technical Role State	Description
CANDIDATE	Technical role was created by role mining and must be promoted before it can be activated. This state corresponds to the internal state called MINED.
ACTIVE	Valid, meaning all included permissions are available in the catalog, and the role is included in the detection process.
NOT ACTIVE	Valid, but the role is excluded from the detection process. This state corresponds to the internal state called INACTIVE.
INVALID	Invalid and excluded from the detection process due to a detected error. Detection errors are usually the result of a deleted permission that is included in the technical role.

18.4 Understanding Technical Role Mining

Technical role mining is the process of discovering and analyzing business data to logically group permissions to simplify the review process or allow grouping of related permissions under one technical role candidate. A **technical role candidate** is a set of permissions and users that can be promoted to a technical role. Identity Governance uses advanced analytics to mine business data and to identify role candidates. Customer, Global or Technical Roles Administrators can use role mining to create technical roles with common permissions after collecting related metrics.

Identity Governance uses the following two approaches to identify technical role candidates.

Automatic Suggestions

Enables administrators to direct the mining calculations by specifying the minimum number of permissions that a specified number of users should have in common, the coverage percentage, the maximum number of role suggestions, and other role mining options.

For more information about Automatic Suggestions criteria and computation, see Section 18.4.1, “Understanding Automatic Suggestions Mining Approach,” on page 215.

Visual Role Mining

Enables administrators to select role candidates from a visual representation of the distribution of users based on permissions. The map displays several clusters that can be potential technical role candidates. Administrators can click within the user access map and drag to select permissions within an area on the map, then view technical role candidates.

With both these approaches, you can edit and save role candidates. You must also promote candidates before you can activate them as roles. You can also generate technical role candidates when you use mining to create a business role. For more information about business roles, see Chapter 19, “Creating and Managing Business Roles,” on page 229.

Identity Governance performs role mining as a background process. If you navigate from the role mining page, role mining will continue. When you return to the role mining page, click **Load Previous Suggestions** to list the mining suggestions, then create the technical role candidates. The generated role mining suggestions are available for 96 hours. You can adjust the mining retention interval by selecting **Configuration** > **Analytics and Role Mining Settings**.

TIP: If you have a large catalog of users and technical roles, data mining performance might be very slow and eventually fail. Use the Configuration Utility console mode commands `set-property com.netiq.iac.analytics.roles.technical.MaxPermSize 10000` and `set-property com.netiq.iac.analytics.roles.technical.MaxUserSize 10000` to change the size to 10000 and improve data mining performance. For more information about the utility procedures, see “Using the Identity Governance Configuration Utility” in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

18.4.1 Understanding Automatic Suggestions Mining Approach

When Identity Governance collects technical role related **User to permission assignments** metric, it stores the permission-assignment map in the database to display automatic suggestions. The metric results are in a compressed format in the database where rows are permissions and columns are users holding permissions.

The database binary matrix includes all users who hold at least one of the permissions and all permissions which are held by at least one user. The number of included users and the number of permissions in this matrix are based on `com.netiq.iac.analytics.roles.technical.MaxUserSize` and `com.netiq.iac.analytics.roles.technical.MaxPermSize` configuration properties respectively. Identity Governance updates this data based on the metrics schedule.

The metrics results (permission-assignment map) include several clusters that can be potential technical role candidates. The map is like the visual representation displayed when you choose the Visual Role Mining approach. Identity Governance further analyzes these clusters, isolates (permission-user pairs), and sorts them by the rectangle area (number permissions multiplied by the number of users). During this process, the matrix is transposed repeatedly, and rows are moved based on similarity and similar rows are kept together until the top matching candidates are found.

When you select **Automatic Suggestions** and save the default criteria or specify criteria, Identity Governance applies the criteria as boundary conditions and removes the rows and columns that do not meet the specified criteria. It also removes any empty rows and columns that are created after applying criteria, then creates clusters of permission-user pairs and displays the top matching suggestions based on **Number of candidates to show** and weighted rank. The result is a set of rectangles (technical role suggestions) where the number of rectangles is equal to your specified number of candidates to show. For example, if you had requested 5 candidates, and 8 clusters are found, only the top 5 will be displayed.

Find next a simple example of the role mining settings and corresponding permission-assignment map and results.

- **Filter permissions by users**: `Display Name equals one of ['Armando Colaco', 'Franke Drake', 'Henry Morgan', 'Leon Lavalette', 'James Ross', 'Lisa Haagensen" or 'Camille Pissaro']`
- **Number of candidates to show**: `5`
- **Minimum number of permissions**: `3`
- **Minimum number of users**: `3`
- **Permission coverage**: `0%`

Based on these specified criteria,Identity Governance finds 4 candidates corresponding to the biggest clusters on the permission-assignment map.

Figure 18-2 *Permission-Assignment Map*

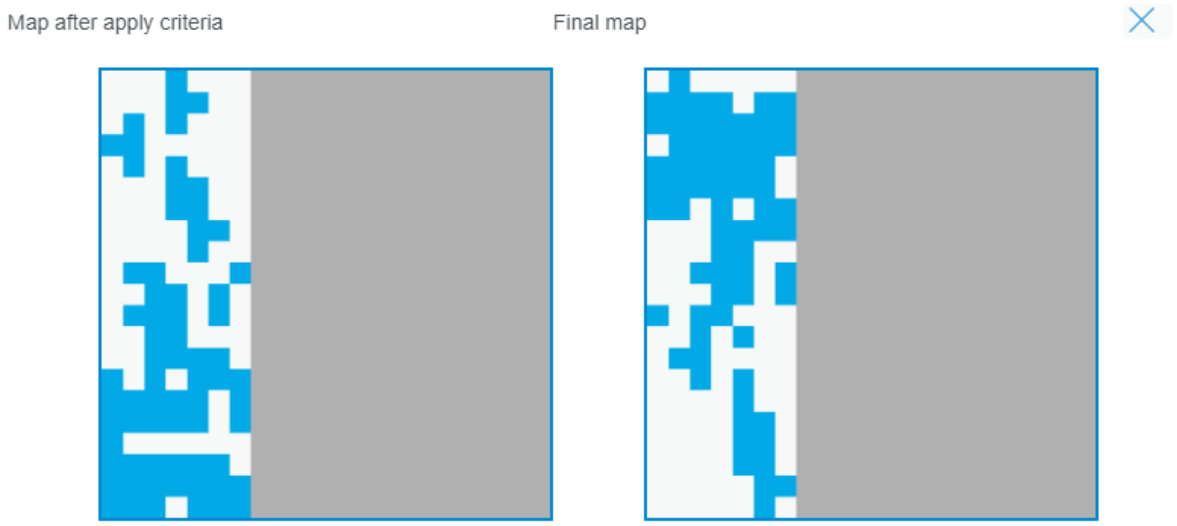


Figure 18-3 *Results*

Mining Suggestions

Role mining settings

Based on data analysis on 06/11/2024 3:15 PM, the following technical role suggestions are listed according to strength of recommendation. Select one or more items from the list to analyze for duplicate roles or to create candidates.

Actions

Search for value

Permissions	# Matching Users	Matching Roles	Weighted Rank
North Door, Cashflow Report View + 2	5	Not analyzed	1
Direct Report, North Door + 3	4	Not analyzed	2
Direct Report, North Door + 4	3	Not analyzed	3
All Doors, Alarm Reset + 1	4	Not analyzed	4

Identity Governance ranks the role mining suggestions by the number of permissions multiplied by the number of users. In the above example, *5 users* match the role mining criteria and hold 4 permissions in common (total twenty), Identity Governance lists them first as it has the *most number of users and the highest total of permissions multiplied by users*. The following candidates have *4 users* who hold 5 permissions in common (total twenty), 6 permissions held by 3 users (total 18), then 3 permissions held by 4 users (total twelve).

After collecting metrics and selecting **Automatic Suggestions**, you may start mining after only entering the description, and *without* entering any criteria. When criteria are not specified, Identity Governance generates the suggestions using the following default values:

- **Number of candidates to show**: 25
- **Minimum number of permissions**: 5

- **Minimum number of users**: 5
- **Permission coverage**: 15%

To generate more specific technical role suggestions, you can also:

- Change the maximum number of suggestions to display.

  NOTE: Identity Governance can display maximum thousand suggestions. Each suggestion includes a different set of users and permissions.

- Filter permissions by users and filter permissions settings using advanced filters to limit permissions used in a technical role using user and permission attributes respectively. Note that when you filter permissions by users, Identity Governance finds permissions that satisfy *all* your criteria. Therefore, all permissions held by your specified users might not be included in the suggested role candidates. You might want to increase the number of candidates to get more common permissions. This does not mean that all permissions held in common by your specified users will be found.
- Search and select specific users and permissions to exclude from the calculation of suggested technical roles.
- Specify minimum number of users that must hold the permissions to be included in the suggested role.
- Specify minimum number of permissions that the suggested role should include.
- Specify percentage of users that must hold a permission for the permission to be included in the calculation of roles. For example, if you specify permission coverage is ten percent for permissions held by hundred users, then at least ten users should hold the permission to be included in the suggestion.

18.4.2 Determining Which Technical Role Approach to Use

Use Table 18-1 to determine the type of role mining to select.

Table 18-1 *Determining Which Role Mining Approach to Use*

If	Then
You want to use user and permission relationships to automatically identify potential candidates and create more than one technical role	Select **Automatic Suggestions** **NOTE:** Automatic role mining identifies potential role candidates and allows you to choose a role candidate instead of creating one, thereby avoid duplicating a technical role.
You want to use the user access map to create a role candidate, add or remove permissions, estimate users, and analyze SoD violations	Select **Visual Role Mining**

18.5 Understanding Technical Role Detection and Assignments

When you activate a technical role, Identity Governance detects users in the catalog that contain the permissions as members of the role. Identity Governance assigns the technical role to the users when:

- Global Administrators, Technical Roles Administrators, or Technical Role Owners promote detected roles and assign users to roles
- Users become members of a business role that is authorized to auto-grant technical role authorization
- A fulfiller, or the automatic fulfillment process, fulfills technical role assignment requests

---

NOTE: For access requests, if an effective date is set when requesting access, the user is not assigned the role until the specified date.

Users might be detected in a role without being assigned the role, or they might be assigned the role without being detected in the role. Identity Governance Customer, Global, or Technical Roles Administrators can view which users are detected or assigned a role from the catalog role page by adding **# Users with all Permissions** and **# Assigned Users** as selected columns.

Administrators and owners can also view the details of a technical role assignment in the catalog on the Identity page Roles tab. The assignment details indicate how it was assigned, such as business role, access request, or promotion, as well as when it was assigned. If a role is assigned but not detected, administrators can also see the role permissions that are not held by the user.

Deactivating a role or changing its permissions does not change role assignments. When you deactivate a technical role, Identity Governance no longer detects users as members of the role in the catalog and excludes the technical role from future detection processes. Similarly, if you change the permissions in an active technical role definition, Identity Governance goes through the detection process and updates the catalog. However, users who are assigned the technical role remain assigned independent of detection.

18.6 Understanding Technical Role Revocations

Identity Governance removes assigned technical roles when:

- The automatic fulfillment process revokes a technical role assignment based on review or access request
- Users with fulfiller authorization fulfill review or access requests to revoke technical role assignment
- Users lose membership in a business role that authorizes the technical role and is configured to auto-revoke it

By default, when technical roles are removed because of any of the above conditions, Identity Governance triggers fulfillment requests to remove permissions contained in the technical role from users unless the permissions are assigned to the same user by other technical roles or Identity Governance is configured to not generate requests for permissions authorized by business roles.

Administrators can configure Identity Governance to honor business role authorizations so that fulfillment requests are not generated if the permission is authorized by business role membership by setting the `com.netiq.iac.request.honorBRoleAuthorizations` property to `true` using the Configuration Utility console mode procedures. Administrators can also control whether fulfillment requests are generated for both auto grant and non-auto grant authorizations only using the `com.netiq.iac.request.honorBRoleAutoGrantOnly` property.

18.7 Creating and Defining Technical Roles

To create technical roles you must have a Customer, Global, or Technical Roles Administrator authorization, and you must have collected metrics. You can create technical roles either manually or using role mining analytics. Additionally, the Business Role Administrator can generate technical roles when creating business role candidates.

When using role mining analytics, Identity Governance automatically groups permissions and presents them as technical role candidates. You must promote role candidates as roles before you can activate the technical role.

When you are creating technical roles manually, an understanding of what permissions you want to assign to the technical role is helpful. You cannot activate a technical role until you have added permissions to the technical role.

18.7.1 Creating Technical Roles Using Role Mining

Identity Governance uses advanced analytics to mine business data and identify role candidates. Technical role mining is the process of discovering and analyzing business data to logically group permissions to simplify the review process, or allow grouping of related permissions under one technical role candidate. Customer, Global or Technical Roles administrators can use role mining to create technical roles with common permissions. Identity Governance uses the following two approaches to identify technical role candidates.

Identity Governance allows you to use one of two role mining methods to create technical roles.

To create a technical role using role mining:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. Click the **Mining** tab.
4. Select a role mining approach. (See Table 18-1 to determine which role mining approach to use.)
5. (Conditional) If you choose **Automatic Suggestions**:

   5a Click **Generate New Suggestions**.

   NOTE: If you already generated new suggestions, you can click **Load Previous Suggestions**, then skip to Step 5f. Only saved suggestions still within the specified retention interval appear.

5b Provide a description that lists the attributes you want to use for role mining, or that specifies the purpose for the role.

5c (Optional) Specify role mining options relevant to the technical role you want to create.

5d Click **Start**.

5e Click **Load** next to the mining suggestion you want to use to load potential role candidates.

5f Select one or more potential candidates from the **Mining Suggestions**, then select **Actions** > **Create Candidates**.

5g In the Create Role Candidates dialog box, type a name for the technical role candidate, then click **Create Candidates**.

6 (Conditional) If you choose **Visual Role Mining**:

6a Use your mouse to select an area containing the permissions you want the technical role to contain.

6b Click **View Candidate**.

6c Type a name for the technical role you want to create.

6d Click **Estimate Users** to see how many users have the specified permissions

---

NOTE: You can click the highlighted number to view a list of users with the specified permissions.

6e Click **Analyze SoD Violations** to view potential separation of duties policies that would be violated if users held the permissions contained in this technical role.

NOTE: The Potential SoDs Violated window displays the names of the SoD policies potentially violated and the number of users affected. Click the SoD policy name or the highlighted number for details.

6f Click **Create Candidate**.

7 Click the **Roles** tab, then select the mined role candidates.

8 Select **Actions** > **Promote Candidates**, then click **Promote**.

9 (Optional) Click the promoted role to edit the role name, description, owner, risk, cost, or category.

10 (Optional) Estimate the impact by viewing the list of associated users and analyzing SoD violations if SoD policies were previously defined.

11 (Optional) Add or remove permissions based on the estimated impact and save the changes.

NOTE: When you add permissions to a role, the dialog displays all application permissions in Identity Governance. You can quickly sort or filter permissions by name, description, or application. You can also click the filter icon and use the expression builder to add additional criteria to the search and limit the displayed permissions further. You can save and reuse the filters that you have defined. For more information about filters, see Section 12.4.3, “Using Advanced Filters for Searches,” on page 134.

---

12 Click the gear icon to customize which columns display on the screen.

After you promote a role, you can use the **Actions** menu to add and remove categories, assign owners, promote or delete candidates, activate or deactivate roles, and download definitions. Note that roles which has reference to any business roles, SOD, access request, or approval policy cannot be deactivated. You must activate a technical role to allow Identity Governance to identify the users that hold permissions specified in the role.

18.7.2 Creating Technical Roles Manually

To define a technical role manually, you must define parameters, including permissions, owners, risk, cost, or category, for the role.

To create a technical role manually:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. Click the plus sign (+) to create a technical role.
4. Provide values for any of the following fields:
   - Name of the technical role (Required)
   - Description of the technical role
   - Owner(s)
   - Risk level configuration
   - Risk level
   - Cost
   - Categories
5. (Optional) Next to **Permissions**, click the plus sign (+), select the permissions to include in the role, then click **Add**.
6. Click **Estimate Users** to see how many users have the specified permissions

   ---

   NOTE: You can click the highlighted number to view a list of users with the specified permissions.

   ---

7. Click **Analyze SoD Violations** to see potential separation of duties policies that would be violated if users held the permissions contained in this technical role.

   NOTE: The Potential SoDs Violated window displays the names of the SoD policies potentially violated and the number of users affected. Click the SoD policy name or the highlighted number for details.

   ---

8. (Optional) Remove permissions to resolve potential SoD violations.
9. Click **Save**.
10. On the **Roles** tab, select the technical role you created.
11. Select **Actions** > **Promote Candidates**, then click **Promote**.
12. Click the gear icon to customize which columns display on the screen.

After you promote a role, you can use the **Actions** menu to add and remove categories, assign owners, promote or delete candidates, download definitions, and activate or deactivate roles. Note that roles which has reference to any business roles, SOD, access request, or approval policy cannot be deactivated. You must activate a technical role to allow Identity Governance to identify the users that hold permissions specified in the role.

18.8 Activating Technical Roles

After you have added permissions to a technical role definition, and promoted the role candidate, you can see an estimate of the number of users holding the permissions of the technical role, and you can activate the technical role. If you do not activate the technical role, Identity Governance does not identify the users that hold the permissions in the technical role.

NOTE: Mined technical roles are created in a candidate state and must be promoted before they can be activated and published. You can promote roles individually or select one or more roles and select **Actions > Promote candidates**.

To activate technical roles:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. Select one or more roles from the list, then select **Actions > Activate**.
4. Alternately, you can select a role name and click **Edit**.
5. In the role definition, select **Active**.

Activating and deactivating a technical role both start a detection process and result in automatic updates in the catalog.

18.9 Promoting Detected Roles to Assigned Roles

Identity Governance detects users that hold all the permissions of a role, but it might not have assigned the role to the user. Primarily, fulfillers would assign technical roles to users based on access requests or business role authorizations. However, promoting detected roles to assigned roles gives administrators the ability to onboard any initial assignments.

After you assign the users to the role, Identity Governance creates a report you can download that contains information about the technical role assignment. The report lists the following for each user:

- The name of the technical role assigned to the user
- The role unique identifier
- The user's unique ID
- The time the role was assigned
- Any notes or issues associated with the user assignment, such as:
  - The user attributes did not uniquely identify a single user
  - The user was already assigned to the role

- The role identified in a CSV file used for role assignment is not active
- The role identified in a CSV file used for role assignment cannot be found or is deleted

Administrators can use the following methods to assign technical roles to detected users:

18.9.1 Assigning a Technical Role to Specific Detected Users of a Role

When you create a technical role, Identity Governance automatically detects users that have all permissions specified in the role. You can choose to assign the technical role to only some detected users.

To assign a technical role to specific detected users of a role:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. Add **# Users with all Permissions** to the displayed columns.
4. Click the number of detected users for a role.
5. Select the users to assign.
6. Click **Assign role to users**.
7. Provide an **Assignment comment**.
8. Click **Assign**.

NOTE: You can also perform this technical role assignment when you edit a technical role. You can click the **Users with all Permissions** tab, then perform Step 5 through Step 8 in the procedure.

18.9.2 Assigning Technical Roles to Detected Users with All Permissions of a Role

When you create a technical role, Identity Governance automatically detects users that have all permissions specified in the role. Administrators can assign a technical role to users with all permissions to the role. Identity Governance also allows administrators to perform that function for multiple technical roles.

To assign technical roles to users with all permissions of a role:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. Select one or more roles from the list, then select **Actions > Assign role to users**.
4. Enter an **Assignment comment**.

5 From **Assignment strategy**, select **Users with All Permissions**.

6 (Optional) Click **Preview** to download a report that contains information about the technical role assignment.

NOTE: The **Assignment Time** column of the report will be empty, because the report is the result of a preview, not a role assignment.

---

7 Click **Assign**.

18.9.3 Assigning Technical Roles Using a Search Query

When you create a technical role, Identity Governance automatically detects users that have all permissions specified in the role. Administrators can create a search query to specify users to assign the technical role, including those who do not have all permissions for the role. For information about using the Expression Builder to create a search query, see Chapter 5, “Using Advanced Filters for Searches,” on page 59. Identity Governance also allows administrators to use a search query to assign multiple technical roles to users that match the search query.

To assign technical roles to users matching a search query:

1 Log in as a Global or Technical Roles Administrator.

2 Under **Catalog**, select **Roles**.

3 Select one or more roles from the list, then select **Actions > Assign role to users**.

4 Enter an **Assignment comment**.

5 From **Assignment strategy**, select **Users matching query**.

6 Click the filter icon and create a search query.

7 (Optional) Click **Preview** to download a report that contains information about the technical role assignment.

NOTE: The “Assignment Time” column of the report will be empty, because the report is the result of a preview, not a role assignment.

---

8 Click **Assign**.

18.9.4 Assigning Technical Roles Using a CSV File

When you create a technical role, Identity Governance automatically detects users that have all permissions specified in the role. Administrators can create a CSV file that lists specific users to assign the technical role, including those who do not have all permissions for the role. Identity Governance also provides administrators with two methods for using a CSV file to assign multiple technical roles to users listed in the file:

- By selecting one or more roles from the list
- By including the technical role names in the CSV file

Creating a CSV File

You can use the Identity Governance user interface to create a CSV file you must then modify for use to assign technical roles.

To create a CSV file:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Identities**.
3. Use the advanced filter to create a list of users you want to assign the technical roles. For information about using the Expression Builder to create a search query, see Chapter 5, “Using Advanced Filters for Searches,” on page 59.
4. Click **Download all as CSV**.

Modifying a Generated CSV File

The heading names that appear in the CSV file you generated are the display names for the attributes, but technical role onboarding requires heading names to be attribute keys. Before you can assign technical roles from the CSV file, you must open the CSV file and change each heading name from the display name to the appropriate attribute key. To see a list of attributes and their attribute keys, click **Data Administration** > **Identity Attributes**.

In addition, if you plan to assign technical roles to users by including the technical role name in the CSV file, you must create a column in the file for the technical role names.

To include technical role names to the CSV file:

1. Open the CSV file you generated.
2. Create a technical roles column with the heading name `technicalRole`.
3. Specify the technical role names you want to assign to a user into the associated technical role column cell.
4. (Conditional) If you are assigning multiple technical roles to a user, separate the technical role names by commas.

Assigning Selected Technical Roles to User Names Listed in a CSV File

One of two methods for assigning technical roles from a CSV file allows you to select roles in Identity Governance, then use a CSV file to assign those roles to users listed in the CSV file.

To assign technical roles to users from a CSV file by selecting roles from the list:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. Select one or more roles from the list, then select **Actions > Assign role to users**.
4. Enter an **Assignment comment**.
5. From **Assignment strategy**, select **Users from CSV**.
6. Click **Browse** to find the CSV file that contains the users you want to assign the technical roles.

7 (Optional) Click **Preview** to download a report that contains information about the technical role assignment.

NOTE: The “Assignment Time” column of the report will be empty, because the report is the result of a preview, not a role assignment.

8 Click **Assign**.

NOTE: If a user listed in the CSV file already has the role assigned to them, the role is not reassigned. However, the report Identity Governance generates after role assignment will indicate that the role was already assigned to the user, and the assignment time will indicate the time the role was first assigned to the user.

Assigning Technical Roles from a CSV that Includes Technical Role Names

One of two methods for assigning technical roles from a CSV file allows you to assign technical roles to users by including the technical role name in the CSV file. Before you use this method, be sure you modified the CSV file as described in “Modifying a Generated CSV File” on page 225.

To assign technical roles to users from a CSV file that includes the technical role name:

1 Log in as a Global or Technical Roles Administrator.

2 Under **Catalog**, select **Roles**.

3 Click **Actions** > **Assign roles to users**.

4 Enter an **Assignment comment**.

5 Click **Browse** to find the CSV file that contains the users you want to assign the technical roles.

6 (Optional) Click **Preview** to download a report that contains information about the technical role assignment.

NOTE: The “Assignment Time” column of the report will be empty, because the report is the result of a preview, not a role assignment.

7 Click **Assign**.

NOTE: If a user listed in the CSV file already has the role assigned to them, the role is not reassigned. However, the report Identity Governance generates after role assignment will indicate that the role was already assigned to the user, and the assignment time will indicate the time the role was first assigned to the user.

18.10 Editing and Deleting a Technical Role

When you edit a technical role, you can change permissions assigned to the technical role and either leave the technical role active or disable the technical role. However, Identity Governance automatically disables a technical role definition if a permission included in the technical role is

deleted from the application. The technical role remains in the disabled state until the permission is removed from the technical role definition or restored in the application and then collected and published to the catalog.

If a technical role references a business role, SoD, access request, or access request approval policy, then Identity Governance will not allow you to delete or deactivate the technical role unless the administrators of those policies remove the technical role from the policies, which reference the technical role.

When you delete a technical role, Identity Governance deletes the technical role in the catalog. However, if the technical role was authorized by a business role, this deletion triggers additional evaluation and consequent actions. When you add or remove permissions from a technical role that is authorized by a business role, the changes may cause business role authorizations to be gained or lost, which may trigger evaluation and consequent actions. For more information, see Section 19.8, “Automated Access Provisioning and Deprovisioning,” on page 247.

To edit or delete a technical role:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. (Optional) Click the gear icon to select additional columns such number of SoDs, number of business roles, and number of users with all permissions.
4. Select the role you want to edit or delete.

   Selecting the role displays a quick overview of the role definition including the name, description, owner, risk, state, and selected permissions.
5. Select **Edit** at the end of the details panel to edit the technical role.
6. (Conditional) Select **Delete** to delete the technical role.

   You must edit the technical role to delete the technical role.

NOTE: When you delete technical roles, Identity Governance removes the role assignments and detections from the users but does not change the permissions held by the users.

18.11 Monitoring Technical Roles and Downloading A List of Detected and Assigned Users

Identity Governance by default displays the name, description, and state of all your technical roles. You can customize the display to include additional details and download a list of assigned and detected users of a technical role.

To customize a display and download a list of technical role users:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog**, select **Roles**.
3. Click the gear icon.
4. Select **# Users with All permissions** and **# Assigned Users**.
5. (Optional) Select additional columns. For examples, select **# SoDs** and **# Business Roles** to view the associated SoD policy and business role.

6 Save your changes.

7 Click the number of users with all permissions, then click **Download all as CSV**.

8 Click the number of assigned users, then select **Actions > Download all as CSV**.

9 Select the download icon on the top title bar to access the saved files and download the files.

10 (Optional) Delete the downloaded files from the download area in Identity Governance.

If you do not manually delete files, Identity Governance automatically deletes them based on your default download retention day settings. For information about customizing download settings, see Section 4.9, “Customizing Download Settings,” on page 56.

18.12 Downloading and Importing Technical Roles

You can download technical roles, categories, and other referenced objects and import them later into an Identity Governance environment. The download will either generate a single JSON file or a zip file depending on the options you select during download, such as associated applications and assigned categories. In addition to downloading the role definitions, you can download the list of roles as a CSV file. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

19 Creating and Managing Business Roles

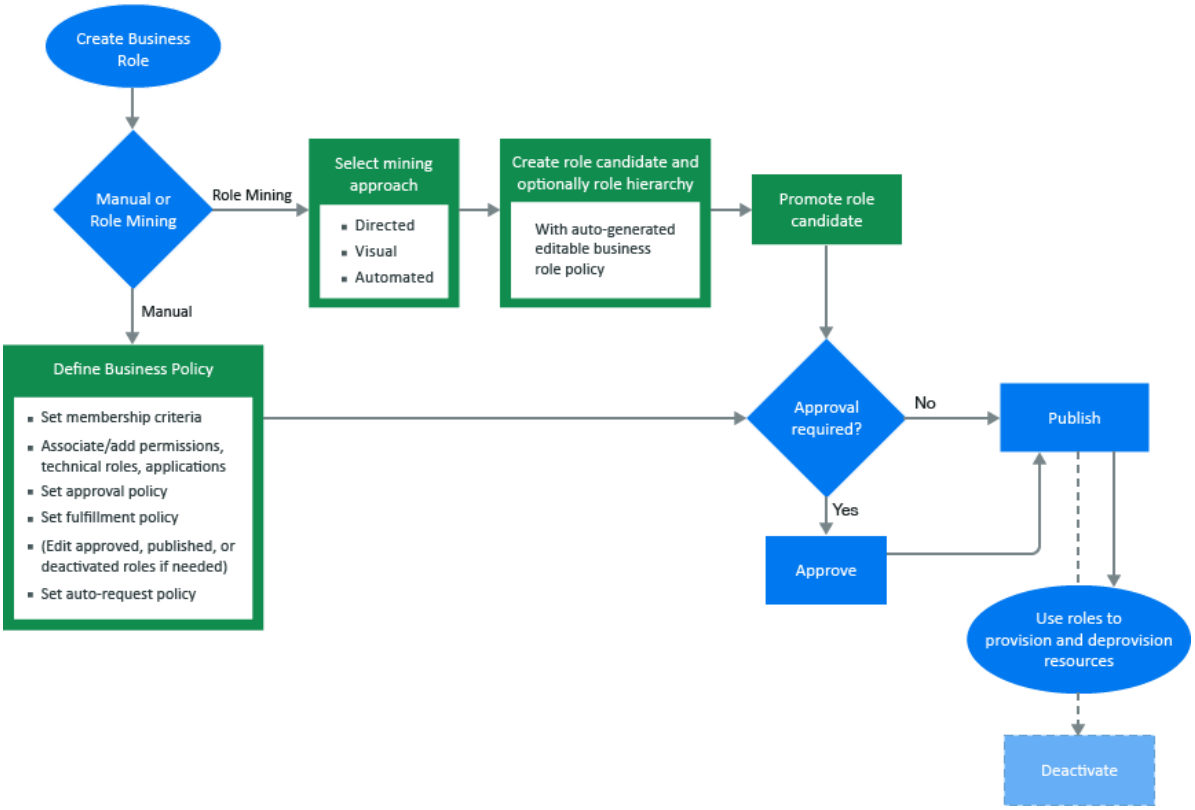
Business roles are roles whose users have common access requirements within your organization. The set of users is defined by the membership policy of each role.

19.1 Understanding Business Roles

Business roles specify a set of applications, roles, and permissions that each member of a business role is authorized to access. The set of authorized resources is defined by the authorization policy of the business role. A business role authorizes resources and generates requests, but does not assign resources.

Figure 19-1 shows the business role workflow in Identity Governance.

Figure 19-1 *Business Role Workflow*



- Section 19.1.1, “Understanding Business Role Access Authorizations,” on page 230
- Section 19.1.2, “Understanding Business Role Mining,” on page 230
- Section 19.1.3, “Understanding Role Hierarchy with Role Mining,” on page 233
- Section 19.1.4, “Understanding Business Role States,” on page 234

19.1.1 Understanding Business Role Access Authorizations

The Customer, Global, or Business Roles Administrator creates, modifies, and defines business roles, and manages business role policies. They can delegate administrative actions by specifying a Business Role Owner or a Business Role Manager for each business role. Business Role Owners can view and approve business roles but cannot edit business roles. Business Role Managers can edit business role membership and resource authorizations, submit business roles for approval, promote role candidates, publish roles, and deactivate roles. If the administrator does not specify role owners in the business role definition, Identity Governance automatically assigns the administrator who created the role as the role owner. For more information about access authorizations, see Section 2.1, “Understanding Authorizations in Identity Governance,” on page 19.

19.1.2 Understanding Business Role Mining

Business role mining is the process of discovering and analyzing business data to group multiple users and access rights under one business role candidate. Identity Governance uses advanced analytics to mine business data and to identify role candidates. Customer, Global, or Business Roles administrators can use role mining to reduce complexity in defining roles, and easily select role

candidates with authorized users, permissions, technical roles, and applications to create business roles and technical roles with common permissions. Identity Governance uses three approaches to business role mining to identify business role candidates.

Directed role mining

Enables administrators to direct the mining based on specified user attributes. If administrators are not sure which attribute to select, they can search for recommended attributes, then select an attribute from the recommended bar graph that displays the strength of attributes that have data. Additionally, directed role mining enables administrators to specify a minimum membership and coverage percentage to identify role candidates. For example, if an administrator selects **Department** as the attribute to group candidates by, the mining results display the list of items consisting of department name with the associated users, permissions, roles, and applications as role candidates.

Automated role mining

Enables administrators to enhance business role mining in larger environments by specifying a minimum number of attributes, a minimum number of occurrences, and the maximum number of results. Administrators can also specify a coverage percentage to identify role candidates. In this approach, Identity Governance uses the attributes specified in the role mining settings in **Configuration > Analytics and Role Mining Settings** to calculate role candidates.

NOTE: We recommend that you use this option if you have a large and complex catalog, such as a catalog with a greater number of variations in extended attributes, with multiple values of attributes, and a catalog size that slows role mining performance.

Visual role mining

Enables administrators to select role candidates from a visual representation of the user attributes. The width of an attribute circle displays the strength of the recommendation, and the width and darkness of the lines indicate the affinity of the attribute to other user attributes. Administrators can customize the mining results by modifying the default maximum number of results, the minimum potential members, and the number of automatic recommendations. In this approach, Identity Governance uses the attributes specified in the role mining settings in **Configuration > Analytics and Role Mining Settings** to calculate role candidates.

NOTE: Variations in the number of extended attributes, attributes with multiple values, or overall catalog size may affect the performance of visual role mining. You might see invalid results when mining larger or more complex data. You can disable this option by setting the `com.netiq.iac.analytics.role.mining.visual.hide` global configuration property to `true`. To optimize performance and to avoid invalid results, use the automated role mining option to mine for roles.

Identity Governance uses the permission, the technical role, and application coverage fields to determine which authorizations are automatically populated in the business role candidate for automated and directed role mining options. For example, if permission coverage is at 50%, then 50% of the members must hold the permission for Identity Governance to add it as an authorization in the candidate. If it is 100%, then all members must hold the permission for Identity Governance to add it as an authorization.

Table 19-1 helps you determine the type of role mining to use.

Table 19-1 *Determining Which Role Mining Approach to Use*

If	Then
You have a small catalog and want Identity Governance to mine for roles based on attributes specified in the role mining settings in **Configuration > Analytics and Role Mining Settings**, and automatically suggest role candidates.	Select **Visual Role Mining** or **Automated Role Mining**.
You have large and complex data to mine, want Identity Governance to mine the data based on the attributes specified in the role mining settings in **Configuration > Analytics and Role Mining Settings**, and want to include minimum occurrences of attributes as mining criteria without specifying any user attributes.	Select **Automated Role Mining**.
You want to direct the mining by specifying user attributes from the catalog. **NOTE:** When using this role mining option, you are not limited to using only the attributes included in the role mining settings in **Configuration > Analytics and Role Mining Settings**.	Select **Directed Role Mining**.

NOTE: Role recommendations are dependent on your data and role mining settings. To optimize search results, administrators can modify default role mining settings in **Configuration > Analytics and Role Mining Settings**. For more information see, "Configuring Analytics and Role Mining Settings" on page 373.

After previewing users and their associated permissions, technical roles, and applications, administrators can analyze specified potential role candidates to see if they duplicate existing roles by matching on membership or authorizations. Existing roles that match the membership or authorizations are displayed in the potential candidate list after performing the analysis. Administrators can then choose not to create those candidates. Additionally, Identity Governance could group common permissions under a technical role, and generate a technical role candidate for each application.

NOTE: Identity Governance creates the mined business or technical roles in a candidate state. Administrators can edit and save role candidates, but they must promote candidates before they can activate them as roles. Administrators can also select multiple role candidates and submit them for approval, publish them, or delete them using the options under **Actions**.

Identity Governance performs role mining as a background process. If you navigate from the role mining page, role mining will continue. When you return to the role mining page, click **Load Previous Suggestions** to list the mining suggestions, then create the business role candidates. The generated role mining suggestions are available for 96 hours. You can adjust the mining retention interval by selecting **Configuration** > **Analytics and Role Mining Settings**.

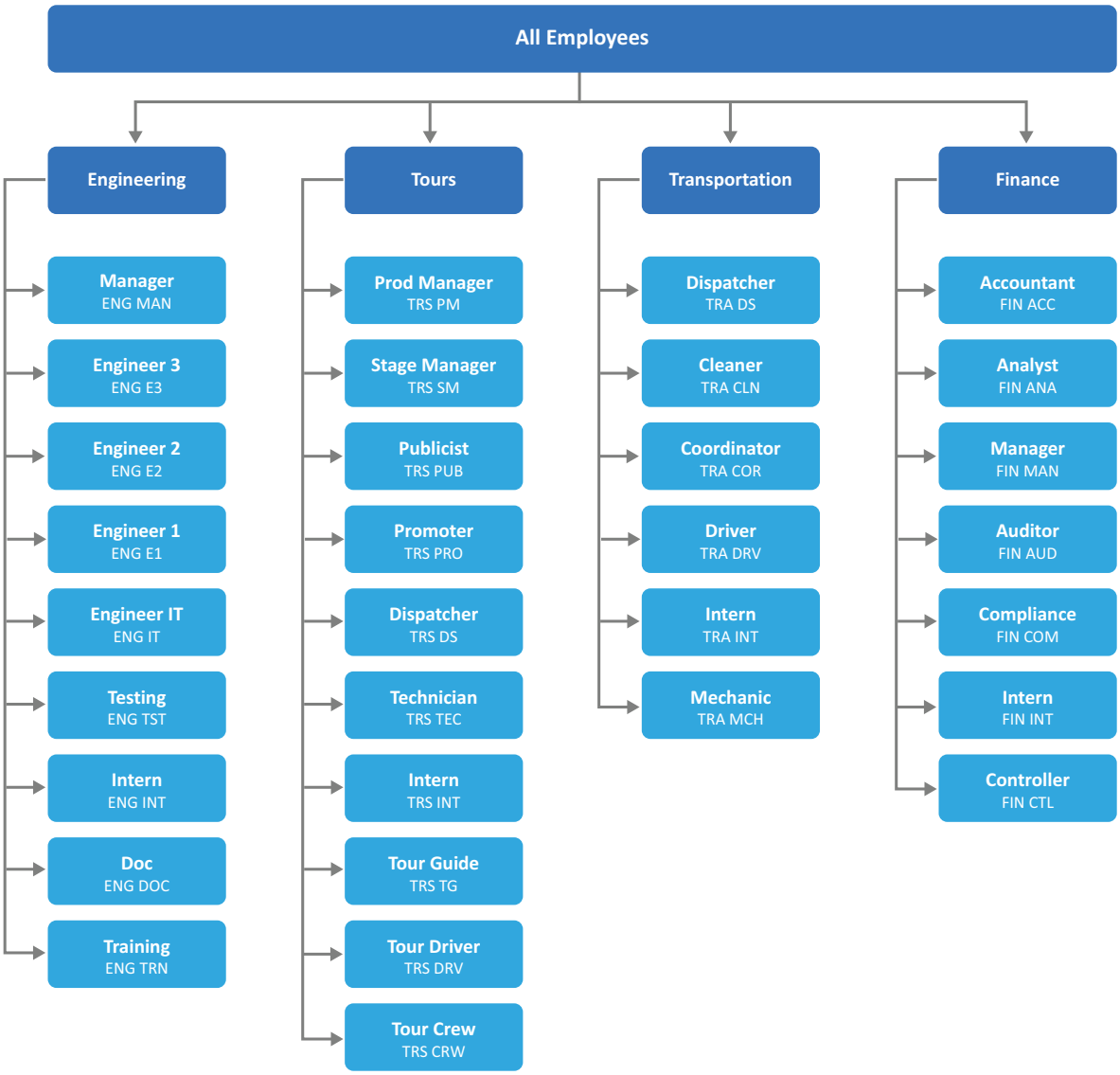
19.1.3 Understanding Role Hierarchy with Role Mining

Business role mining in Identity Governance creates business roles for each selected candidate, but cannot group the created roles. Role hierarchy allows you to create a hierarchy of roles, based on the mining attributes, that allow you to assign resources either at the candidate level, or by grouping the candidates at a higher level.

NOTE: Role hierarchy is not available for visual role mining.

When you select **Create business role hierarchy**, you can select the attributes used in the role mining as grouping attributes for the role hierarchy. For example, Figure 19-2 illustrates a company organization chart in which each department includes job codes that represent positions. The company wants to create departmental business roles for Engineering, Tours, Transportation and Finance, as well as roles for each job code. Furthermore, they want an “All Department” role that includes the Engineering department and all the other top-level departments. Selecting the department attribute as the role hierarchy grouping attribute would create business roles that mirror the organizational chart.

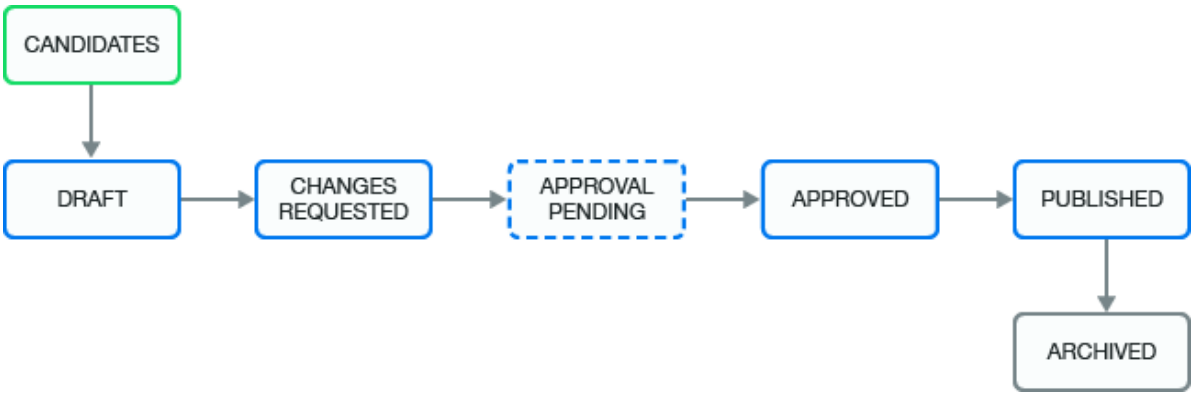
Figure 19-2 *Company Organization with Department and Job Codes*



19.1.4 Understanding Business Role States

After you create, or after Identity Governance mines a business role, the role goes through many states during its life cycle, as shown in Figure 19-3.

Figure 19-3 *Business Role States*



Business Role State	Description
CANDIDATES	The mining process created the business role, and the administrators must promote it before they or others can approve it (depending on the approval policy) and publish it. This state corresponds to the internal state called MINED.
DRAFT	The assigned approval policy requires approval and the administrator has not submitted the changes for approval.
CHANGES REQUESTED	The approver denies approval of a business role. This state corresponds to the internal state called REJECTED.
APPROVAL PENDING	Pending changes are ready for approval by the approver specified in the approval policy. This state corresponds to the internal state called PENDING_APPROVAL.
APPROVED	The approver approved the business role, but the business role has not yet been published.
PUBLISHED	The business role is approved and the administrator has published the role.
ARCHIVED	An administrator deletes the policy or creates a new version. Identity Governance archives the policy for history and reporting purposes. Identity Governance never displays archived business roles in the application.

19.2 Creating and Defining Business Roles

To create a business role, you must define a membership policy and an authorization policy for the business role based on your business needs. Identity Governance allows you to create business roles using role mining, or by creating the role manually.

19.2.1 Creating Business Roles Using Role Mining

Identity Governance can use advanced analytics to mine business data and to identify role candidates. Business role mining is the process of discovering and analyzing business data to group multiple users and access rights under one business role candidate. Identity Governance allows you to use one of three role mining methods to create business roles.

To create a business role using role mining:

1. Log in to Identity Governance as a Customer, Global, or Business Roles Administrator.
2. Select **Policy** > **Business Roles**.
3. Click the **Mining** tab.
4. Select a role mining approach (See Table 19-1 to determine which role mining approach to use).
5. Click **Generate New Suggestions**.

   NOTE: If you already generated new suggestions, you can click **Load Previous Suggestions**, click **Load** for the mining suggestion you want to use to load potential role candidates, then skip to Step 9. Only saved suggestions still within the specified retention interval appear as Previous Suggestions.

   WARNING: You might not see recommendations if the **Generate New Suggestions > Minimum potential members** value is set too high, or if the role mining settings in **Configuration > Analytics and Role Mining Settings** do not meet the required conditions. For more information, see “Configuring Analytics and Role Mining Settings” on page 373.
6. Provide the requested role mining options relevant to the business role you want to create.

   TIP: To differentiate among mining suggestions you generate, provide a description that lists the attributes you want to use for role mining, or that specifies the purpose for the role.
7. Click **Start**.
8. Click **Load** next to the mining suggestion you want to use to load potential role candidates.
9. Select one or more potential candidates.

   IMPORTANT: If you selected visual role mining, you must select one or more criteria from the visual representation before you can select potential candidates.

NOTE: You can click **Change Authorizations** to modify the authorizations used to create the mining suggestions. Changing the authorizations can modify the values for Users, Permissions, Roles, and Applications.

10 Click **Actions** > **Find Matching Roles** to determine if the specified potential candidates match members or authorizations of existing roles.

11 (Optional) Exclude potential candidates identified in the previous step that would create a duplicated role.

NOTE: If you choose to create a business role candidate with members and authorizations that match those in existing roles, you can analyze the candidate to calculate the match percentage. For more information, see Section 19.5, “Analyzing Business Roles,” on page 245.

12 Click **Actions** > **Create Candidates**.

13 Select **Create separate candidates for each criteria** or **Create a single business role candidate**. If you select the latter, specify a name for the business role.

14 (Optional) Select **Create associated technical roles for common permissions** to generate the technical roles with users who have the same permissions.

15 (Optional) Select **Group permissions added to technical roles by application** to create application-specific technical roles.

16 (Optional) Select **Create business role hierarchy**, then select the attributes by which to group values for each available level, to create role hierarchy when mining business roles.

NOTE: The number of available levels is one less than the number of attributes you selected in **Role Mining Options**. For example, if you selected three attributes, you would be able to group the roles for up to two levels.

17 On the **Roles** tab, select one or more newly generated inactive roles.

NOTE: Identity Governance creates role candidates in a pending state, and administrators must promote them before anyone can either approve the role candidates or publish them as a role. Click the role candidate to ensure that the membership criteria and authorizations are as you want them to be before publishing. You can edit the role candidate to estimate impact, analyze SoD violations, and make changes such as make the business role requestable or assign a risk value.

18 Select **Actions** > **Promote**.

19 Select the new role, then select **Actions** > **Publish**.

After you create the business role and assigned owners and administrators, the business role is ready for approval, depending on your approval policy. The approval policy allows you to have people review the business role and approve or request changes to the business role. For more information, see Section 19.3, “Adding a Business Role Approval Policy,” on page 243.

To detect users that meet the business role criteria in reviews or in the catalog, you must publish the business role. For more information, see Section 19.4, “Publishing or Deactivating Business Roles,” on page 244.

19.2.2 Defining Business Roles Manually

To create a business role manually, you must define a membership policy and an authorization policy for the business role based on your business needs.

To define a business role manually:

1. Log in to Identity Governance as a Customer, Global, or Business Roles Administrator.
2. Select **Policy** > **Business Roles**.
3. Click the **Roles** tab, then click the plus sign (+).
4. Specify the following information to create the business role:
   - Name of the business role
   - Business role description
   - Grace period

     NOTE: A grace period specifies the number of days that you want Identity Governance to consider the user as a member of the role when it detects that the member no longer meets the membership policy requirements.
   - Risk level
   - Potential SoD approval

     NOTE: Identity Governance disables potential SoD approval by default, you can enable it for specific business roles or set it globally. For specific business roles, Identity Governance checks for potential SoD violations that require approval on auto-grants arising from those business roles. If you select the global setting, Identity Governance will check for violations on requests from those business roles where **Potential Sod Approval** is not enabled or disabled. However, you can override the global configuration by explicitly setting this option to enabled for each business role. To enable the global setting, select **Use Global** for the option **Potential SoD Approval** or configure potential SoD violations by accessing the **Auto Requests** tab.
5. Select the **Membership** tab, if not already selected, and provide information for one or membership configuration items. For detailed information see Section 19.2.3, “Configuring Business Role Membership,” on page 239.
6. Select the **Authorizations** tab, then provide configuration information for one of more of the authorization configuration items.

   NOTE: Applications must have an account collector to allow you to specify automatic grant or revoke.

   For detailed information about authorizing permissions, technical roles, and applications, see Section 19.2.4, “Adding Authorizations to a Business Role,” on page 241.
7. Select the **Owners and Administration** tab to assign ownership for the following:
   - Role owner
   - Role manager
   - Fulfiller

- Categories
- Approval Policy

NOTE: If you do not make selections on this tab, Identity Governance makes default assignments for the owner and fulfiller and assigns a default approval policy to the business role.

8 (Optional) On the **Membership** tab, click **View Membership** to view the list of business role members.

NOTE: During migration or upgrades, you must always run publication to refresh the list of business role members. For more information about publishing data sources, see Chapter 9, "Publishing the Collected Data," on page 105.

9 Under **What-if Scenarios**, click:

- **Estimate Publish Impact** to estimate changes that would occur if the role were published, such as the users who would be added to or deleted from the business role, the resource authorizations that would be added or deleted, and the change requests that would be made.
- **Estimate Deactivate Impact** to estimate changes that would occur if the business role is deactivated or deleted, such as the resource authorizations that would be deleted, and the change requests that would be made.
- **Analyze SoD Violations** to analyze the SoD violations that would occur if users held the permissions and technical roles authorized by this business role.

10 (Conditional) Resolve SoD violations or edit the business role definition to resolve any issues. For more information about SoD violations, see "Approving or Resolving an SoD Violation" on page 280.

11 (Optional) Enable users to request business role membership through the Access Request interface.

TIP: After specifying a business role as requestable, make sure to publish the business role before assigning it to a Access Request policy. Unpublished business roles will not be available for request.

12 Click **Save** to save your modifications to the business role.

13 Select the saved role, then select **Actions** > **Publish**.

NOTE: When editing an existing business role, the **Owners and Administration** tab has a separate **Save** button, which allows you to change these items independent of other items that refer to the business role.

19.2.3 Configuring Business Role Membership

A membership policy determines which users are members of a business role. The membership policy can include membership expressions, membership policy from other business roles, user or group inclusion lists, and user or group exclusion lists. Regardless of how users become members of a role, they are authorized to have the resources specified in the business role for as long as they are members of the business role.

NOTE: Business role authorization of a resource (permission, technical role, or application) for a user is independent of assigning the resource to the user. For example, the business role might authorize a user to have a permission, but Identity Governance might not have assigned the permission. Similarly, Identity Governance might have assigned a permission, but the business role might not authorize the permission.

Included Membership

Optionally, specify business roles whose membership criteria, users, and groups you want to include in the new business role. When combining the included roles, Identity Governance includes only membership of published roles and eliminates duplicates. For example, you can include BR1 and BR2 in the membership of BR3. Then, role BR3 becomes the union of BR1 and BR2 along with any membership criteria specified for BR3.

NOTE: Excluded members of the including role takes precedence over the inclusion of included business role members. For example, when BR3 includes BR1, and BR1 has a member User A, and BR3 excludes User A then Identity Governance also excludes the user.

Also, note that Identity Governance does not allow circular inclusions. For example, you:

- Cannot include BR1 in BR1 (self inclusion)
- Cannot include BR2 in BR1 then include BR1 in BR2
- Cannot include BR2 in BR1 and BR3 in BR2 and then include BR1 in BR3

Membership expressions

Membership expressions are criteria that specify a set of users that are considered members of the business role. Identity Governance converts your specified criteria to create SQL SELECT statements to find the users that match the criteria. When you use the role mining feature, Identity Governance provides recommendations for role candidates based on your data and auto-generates the membership expressions when you create a role candidate. To optimize specific SELECT statements, follow query optimization principles such as creating indexes for attributes you are going to query. To optimize specific SELECT statements that might not be performing as expected, contact your database administrator. To set effective dates for authorizations, click the calendar icon at the top of the **Membership Expression** menu section.

TIP: When adding date attributes such as start date to membership expression, you can specify a date using the calendar date picker or use the date formula. For example, if you want to automatically make new employees a member of a business role two days before their start date, use the date formula.

Include and Exclude Users and Groups

Optionally, define specific users and groups that you want to include in the business role that might not match any membership expression. You can also specify users and groups to exclude from the business role who would otherwise match membership expressions. For example, you can have a membership expression that matches all managers in engineering, but you do not want John Smith or managers in the CTO group even if they match that criteria. You can also define a time period for when these inclusions or exclusions are valid.

NOTE: Excluding a user or group takes precedence over including them. For example, suppose you include the Sales group and exclude the Contractors group. Then, Identity Governance would exclude a user who belongs to both of those groups because exclusion takes precedence over inclusion.

You can click **View Membership** to view the list of business role members.

NOTE: During migration or upgrades, you must always run publication to refresh the list of business role members. For more information about publishing data sources, see Chapter 9, "Publishing the Collected Data," on page 105.

19.2.4 Adding Authorizations to a Business Role

A **business role authorization policy** defines the permissions, technical roles, and applications authorized by the business role. Users are not automatically assigned the permissions of a business role, nor are business role permissions removed if users no longer meet the criteria for a business role. The business role authorization policy defines only whether the user is authorized the access but does not assign the resource.

A business role can authorize technical roles, so the business role authorizes all business role users and groups for all of the permissions included in each technical role. For more information, see Chapter 18, "Creating and Managing Technical Roles," on page 211.

You add an authorization policy to the business role on the **Authorizations** tab when you create or edit the business role.

There are many different components to an authorization policy. The following information explains the different components.

Authorized Permissions

Identity Governance might preauthorize permissions when you mine for roles or you might need to define them. Select permissions from the entire catalog or from a list of permissions held by the business role members. Specify whether the permission is mandatory or optional. Specify whether Identity Governance should automatically grant or revoke permissions. If needed, select the calendar control to set an authorization period for when Identity Governance authorizes these permissions for users in the business role. The authorization policy can authorize a user in the business role for all of the permissions included in the authorization policy.

If an authorized permission comes from an Identity Manager application and is an Identity Manager role (parent) that contains other Identity Manager roles and Identity Manager resources (children), there will be an option to also authorize the contained permissions (the default is to *not* authorize contained permissions). You can view the hierarchy of contained permissions by clicking **show**.

NOTE: If you specify auto-grant or auto-revoke on this kind of permission, the selected option does *not* apply to any of the contained permissions. This is because if you grant or revoke a permission that is an Identity Manager role that contains other contained Identity Manager roles and Identity Manager resources, the Identity Manager system automatically grants or revokes any contained Identity Manager roles and resources.

Authorized Technical Roles

Identity Governance might preauthorize technical roles when you mine for roles or you might need to define them. The technical role acts as a grouping for the permissions. If all of the appropriate permissions are included in a technical role, you can add the technical role instead of the individual permissions. If needed, select technical roles from the entire catalog or from a list of technical roles held by the business role members. Determine whether the technical role is mandatory or optional. Specify whether Identity Governance should automatically grant or revoke the technical role authorization. If needed, select the calendar control to set an authorization period for when the permissions in the technical role are valid for the business role. The authorization policy can authorize a user in the business role for technical roles included in the authorization policy. If an authorized technical role comes from an Identity Manager application and is an Identity Manager role that contains other Identity Manager roles and Identity Manager resources, the authorization policy can authorize the member of the business role for both the explicitly specified and contained permissions (direct permissions) and permissions contained within the contained permissions (indirect permissions).

Permissions contained in a technical role might come from an Identity Manager application and might be an Identity Manager role that contains other Identity Manager roles and Identity Manager resources. For this reason, technical roles have two options for authorizing contained permissions. You can opt to only authorize the permissions that are explicitly specified in the technical role, or you can opt to authorize the permissions contained in the technical role and any permissions that are contained in those permissions. The second option applies only to permissions that are Identity Manager roles that contain other Identity Manager roles or Identity Manager resources. You can view the hierarchy of all contained permissions that Identity Governance authorizes by clicking **show**.

NOTE: If you select **Auto-grant** or **Auto-revoke** on a technical role, the selected option applies only to the permissions explicitly specified in the technical role. It does *not* apply to any of the permissions that those permissions might contain.

Authorized Applications

Identity Governance might preauthorize applications when you mine for roles or you might need to define them. If needed, define which applications the members of the business role are authorized to hold. This means Identity Governance can create accounts for the members of the business role in the listed applications. Select applications from the entire catalog or from a list of applications held by the business role members. Specify whether Identity Governance should or should not automatically grant or revoke the application authorization. If needed, select the calendar control to set an authorization period for when the members of the business role have access to the application. The authorization policy can authorize a user in the business role to have accounts in the applications included in the authorization policy.

NOTE: Applications must have an account collector to allow you to specify automatic grant or revoke.

Mandatory versus Optional

When an authorization policy specifies **Mandatory** on a permission, technical role, or application, it means that a user is expected to have it if the user is a member of the business role. However, there is no enforcement of having the mandatory item. **Optional** means the authorization policy allows a user to have a resource, but the authorization policy does not require it.

Automatic Grant or Revoke Settings

You can select whether to automatically grant or revoke each permission, technical role, and application. Applications must have an account collector to allow you to specify automatic grant or revoke. When the authorization policy applies the auto-grant or the auto-revoke policies in the business roles, Identity Governance might issue grant requests if the user does not have a resource, and revoke requests if the user has a resource. Under certain conditions, Identity Governance might issue grant requests even if a user has a resource, and revoke requests even if a user does not have a resource.

If you specify auto request on a technical role, the auto request applies only to the permissions explicitly specified in the technical role. It does *not* apply to any of the permissions that those permissions might contain. For example, for Identity Manager roles that contain children permissions, Identity Governance issues auto requests only for the top-level role and then Identity Manager rules apply for all children authorizations. For more information, see Section 19.8, “Automated Access Provisioning and Deprovisioning,” on page 247.

Authorization Period

The authorization policy can authorize a user in the business role for a set period of time defined in the authorization policy. Typically, you might need to set the authorization period only during transitions like mergers or changes related to compliance. Avoid setting an authorization period for business roles to change a specific role authorization, as you handle it more efficiently using periodic business role membership reviews.

19.3 Adding a Business Role Approval Policy

The approval policy for the business role governs all business role life cycle events. Identity Governance contains a default approval policy that it assigns to each business role that you create.

The approval policy for the business role specifies all approval requirements for each business role defined, including whether the business role requires approval when you create or modify that business role.

We recommend that your organization’s default policy require approval. A default policy that does not require approval enables Identity Governance to approve roles automatically. When your policy requires approval, you can submit each role for approval or select multiple draft roles and then select **Actions > Submit for Approval** to submit multiple roles for approval.

Identity Governance applies the default approval policy, which specifies that business roles do not require approval, to all business roles that you create. To change this you would have to change the default approval policy to require approval by owners or specify a list of approvers.

Identity Governance provides two additional policies for your convenience. One policy requires approval by the business owner (recommended) and the other policy does not require approval. A Customer, Global, or Business role Administrator can change or delete these sample policies.

You can create additional approval policies and apply them to existing business roles after you have created business roles. To change the default approval policy, select **Default approval policy** on the **Approval Policies** tab.

To create a new approval policy:

1 Log in to Identity Governance as a Customer, Global, or Business Roles Administrator.

2 Select **Policy** > **Business Roles**.

3 Click the **Approval Policies** tab.

4 Select **Add approval policy** (+).

5 Specify a name and description for the approval policy, then determine whether it is required or not.

6 Save the policy.

You can change the approval policy for a group of business roles at the same time by using the bulk action on the business role list. You can also download business role approval policies as JSON files using the bulk action menu. After editing, you can import the policies on the page that lists all approval policies.

19.4 Publishing or Deactivating Business Roles

Two possible versions of a business role can exist:

- **Published:** Before you can publish a business role, it must go through the approval process and be approved, if it requires approval. A published business role is available for the governance process and in the general catalog.
- **Deactivated:** You can edit published, approved, and deactivated roles. When you edit a published business role, Identity Governance creates a draft of the business role that appears on the **Draft** tab that you can send for approval if required, publish, or discard. However, deactivated roles are not available for the governance process or in the general catalog.

The edit and approve cycle is a single cycle that is independent of the publication cycle. When you edit the published business role, Identity Governance creates a draft version of the business role.

The approval cycle is not independent of the draft. If no approval is required, Identity Governance automatically approves the draft but does not publish the draft. If an administrator publishes the draft, it replaces the currently published version.

When the business role administrator deactivates a published role, Identity Governance takes one of the following actions:

- If there is an approved draft, Identity Governance archives the active version and the approved draft replaces it.
- If there is not an approved draft when the published role is deactivated, Identity Governance prompts the administrator to keep the published version or the unapproved draft version of the business role.
- If there is no draft, Identity Governance moves the published business role to the approved state.

To publish or deactivate a business role:

1 Log in to Identity Governance as a Customer, Global, Business Role Administrator.

2 Select **Policy** > **Business Roles**.

3 Select the business role to change, then select **Edit**.

4 If you have one version of the business role, select **Publish** or **Deactivate** the business role.

NOTE: Deactivating a business role disables the role from being a part of the review process and removes resource authorizations from its members for its resources. However, deactivation does not issue auto-revoke requests for resources that specify auto-revoke, and does not change or retract any current or pending auto-grant or auto-revoke request.

or

If you have multiple versions of the business role, select the **Draft** or **Published** tab, then select **Publish** or **Deactivate**.

NOTE: You must have two versions of the business role to have the **Draft** and **Publish** tabs appear.

If you have many business roles that need to be published, Identity Governance provides a way to publish all of the roles at the same time. On the Business Roles page, select the business roles to publish, then select **Actions** > **Publish**.

19.5 Analyzing Business Roles

Identity Governance allows you to improve role quality and effectiveness by providing you with various analytical tools. To maintain an effective role model, it is important that organizations are able to understand the quality of the roles that have been implemented. For example, you might create a business role that has all or almost all of the members as another business role. This might indicate that these roles are redundant and are not actually needed. Using role analysis, you can analyze selected business roles, all business roles, or membership expression of existing roles to find:

- Similarity in memberships and authorizations
- Effectiveness of the selected business roles based on the percentage of users that hold the role authorizations
- Members and authorizations in common
- Members without mandatory authorizations
- Members without auto-grant authorizations

To analyze business roles:

1. Log in to Identity Governance as a Customer, Global, or Business Roles Administrator.
2. Select **Policy** > **Business Roles**.
3. Click **Analysis** tab.
4. Select an **Analyze** option and configure related parameters. For example, when selecting the similarity analysis, you can modify the default similarity threshold. If you specify 60%, the results display business roles that have 60% similarity with any authorization or membership.

NOTE: You can perform **Business role similarity** and **Common authorizations** analysis on published or unpublished business roles, while you can perform **Authorization effectiveness**, **Mandatory authorizations**, and **Auto-grant authorization** analysis only on published business roles. If there are unpublished business roles in the list selected for **Authorization effectiveness**, **Mandatory authorization**, and **Auto-grant authorization** analysis, Identity Governance highlights them and skips them during analysis.

5 Select **Start Analysis**.

6 Click the links in the analysis results for additional information such as comparison tables of memberships and authorizations in **Business role similarity** analysis, and lists of members in **Mandatory authorization**.

7 (Optional) Select **Download as CSV** to download the results as a CSV file for further analysis.

19.6 Editing Business Roles

Identity Governance allows you to edit business roles. If you edit and save an approved business role, the state changes to DRAFT, and the role must be re-approved. To edit a published business role, a new draft copy is made for editing, and the published role continues to be used in governance processes until the new draft is approved and published. You can also use the bulk action menu to download business roles as JSON files. After editing, you can import the roles on the page that lists all business roles.

To edit a business role:

1 Log in to Identity Governance as a Business Role or Global Administrator.

2 Select **Policy** > **Business Roles**.

3 Select the business role you want to edit, then click **Edit**.

4 (Optional) If the business role is published, on the top of the page, click **Edit**.

NOTE: We recommend that you think through business role definitions and add all members and authorizations, estimate impact, and analyze SoD and potential SoD violations before publishing. If you need to make changes after publishing, keep in mind that business role detections compare your last published state with the current state and automatically generate grants and revocations if auto-grants and auto-revoke settings are enabled. Also, note that the membership policy of a business role can include members from other published business roles, however, circular inclusions are not allowed.

Identity Governance creates a draft of the business role for you to edit on the **Draft** tab.

5 (Optional) Enable users to request business role membership through the Access Request interface.

TIP: After specifying a business role as requestable, make sure to publish the business role before assigning it to a Access Request policy. Unpublished business roles will not be available for request.

---

6 (Optional) Make other appropriate changes to the business role such as setting a risk value or specifying a grace period value for a member who no longer meets the membership policy criteria.

7 Select **Save** to save the draft.

8 (Conditional) Click **Compare with published** to compare the draft version with the published version of the business role to ensure that the changes are correct.

9 (Conditional) If the business role approval policy requires approval, when the draft is ready for approval, click **Submit for approval**. If the business role approval policy does not require approval, the draft is automatically approved whenever you save your edits.

10 After you approve a draft, select **Publish** to publish it.

When you delete a published business role, Identity Governance archives the business role for reporting and auditing purposes.

19.7 Approving Business Roles

Identity Governance provides an approval process for users, groups, or business role owners to approve the business roles they have been assigned to approve. The business role owners can approve the business role if the role's approval policy specifies **Business role owners**. However, you can also specify a list of users or members of a group to be approvers of the business role.

To approve a business role that is pending:

1 Log in to Identity Governance as a user assigned to approve the business role.

2 Select **Policy** > **Business Roles**.

3 Select the **Pending Your Approval** tab.

4 Select any of the pending approvals, then read and review the content of the business role.

5 Specify a comment in the **Comment** field as to whether you approve the business role or if you want changes to the business role.

6 Select **Approve** to approve the role.

or

Select **Request changes** if you want the business role to be modified.

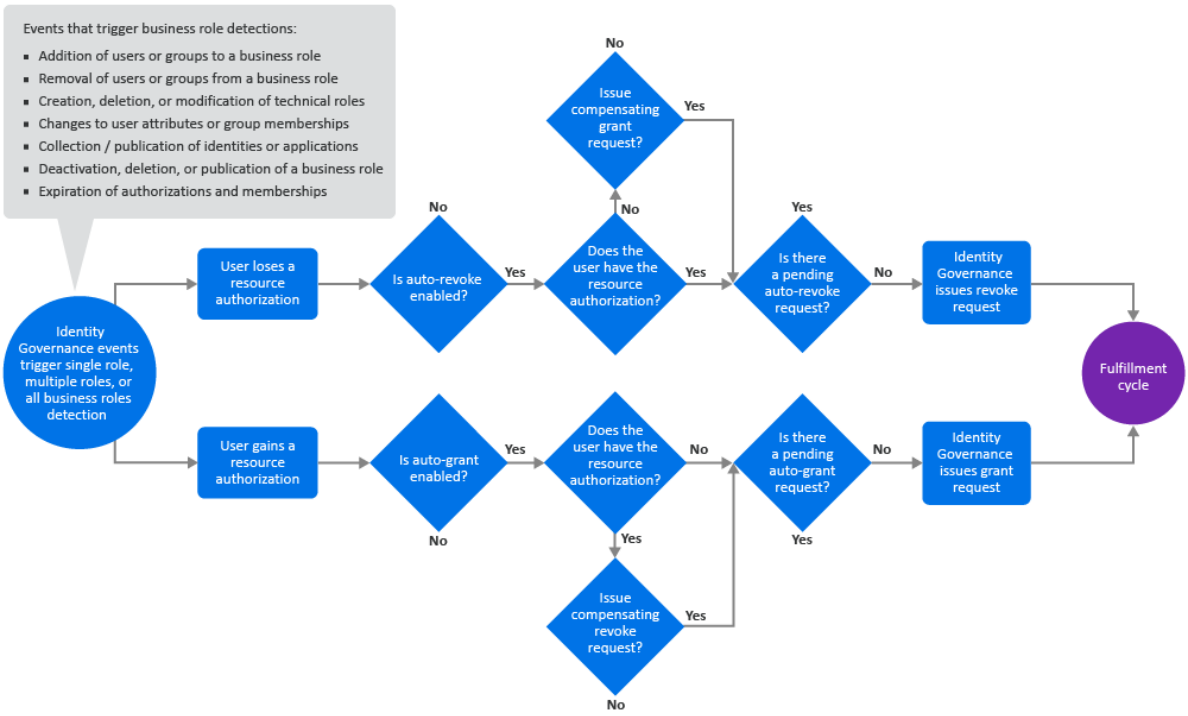
When you select the **Request changes** option, the creator of the business role receives notification of the change request. After you or an administrator modify the business role, the approval workflow process starts again.

19.8 Automated Access Provisioning and Deprovisioning

You can set up business roles to automatically request provisioning and deprovisioning of authorized resources for users in the business role by selecting the auto-grant or the auto-revoke setting for each resource. Identity Governance performs business role detections and evaluates business role membership changes to determine whether to issue the auto requests. During business role detection, Identity Governance only evaluates whether auto requests should be issued. After all business role detections including checking for pending requests, Identity Governance determines if the auto requests including compensating requests should be issued. If potential SoD violation checking is enabled for detection, before sending the auto request for fulfillment, Identity Governance checks for potential SoD violations and if granting the request results in one or more SoD violations, as defined in the SoD approval policy, the request is sent to an SoD administrator or SoD owner for approval. If the potential SoD violation is approved, the permission or application resource request is then sent to the fulfillment system where the fulfillment system handles them according to the rules specified in your system fulfillment configuration. Note that a request with several potential SoD violations is not sent for fulfillment until all the violations are approved.

NOTE: During detection, Identity Governance monitors when a user gains or loses an authorization, or when an authorization changes its auto-grant or auto-revoke policy. When Identity Governance observes these kinds of changes, it triggers an evaluation of whether it needs to issue the auto requests. However, detection does not monitor changes in user resource assignments. Authorization for a resource is not the same thing as being assigned a resource. Since the detection process does not monitor the assignment changes, assignment changes do not trigger an evaluation of whether to issue the auto requests.

Figure 19-4 *Business Role (Permissions and Applications) Automated Access Provisioning and Deprovisioning Process*



When you specify auto-grant and/or auto-revoke for technical roles, Identity Governance performs two different actions.

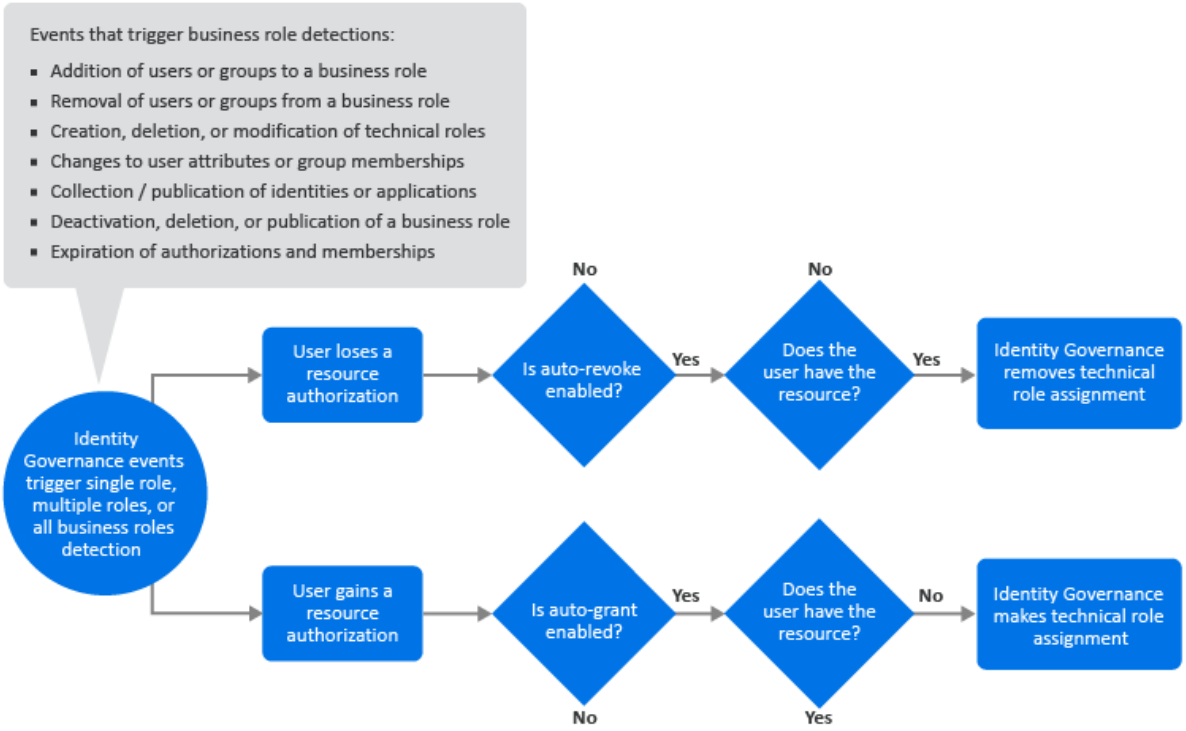
- Identity Governance auto-grants and/or auto-revokes the permissions that make up the technical role, and follows the usual process for granting and revoking permissions

  By default, when technical roles are revoked, fulfillment requests are generated to remove permissions regardless of the business role authorization settings. Administrators can configure Identity Governance to honor business role authorizations so that fulfillment requests are not generated if the permission is authorized by business role membership by setting the `com.netiq.iac.request.honorBRoleAuthorizations` property to `true` using the Configuration Utility console mode procedures. Administrators can also control whether fulfillment requests are generated for both auto grant and non-auto grant authorizations only using the `com.netiq.iac.request.honorBRoleAutoGrantOnly` property.

- Identity Governance auto-grants (makes) and/or auto-revokes (removes) a technical role assignment as needed. If Identity Governance determines that a technical role assignment should be made or removed, it makes or removes the assignment during business role

detection itself and does not generate a fulfillment request. This is because technical role assignments are not provisioned from external data sources, but are provisioned and maintained by Identity Governance. However, if granting a technical role results in one or more potential SoD violations, Identity Governance sends the request through potential SoD violation approval first, as specified in the SoD approval policy.

Figure 19-5 *Business Role (Technical Roles) Automated Access Provisioning and Deprovisioning Process when Business*



The events that trigger Identity Governance to perform business role detections do not necessarily result in Identity Governance issuing auto-grant or auto-revoke requests. The rules that trigger a detection are different from the rules that govern whether Identity Governance will issue the auto requests. For example, deactivating a technical role that is an authorized resource of a business role triggers a business role detection, but does not result in an auto-revoke request or changes to any current auto-grant or auto-revoke request. Publication of application sources trigger detection but do not necessarily result in Identity Governance issuing the auto requests.

- Section 19.8.1, “Understanding Business Role Detections,” on page 250
- Section 19.8.2, “Automatic Provisioning Requests,” on page 252
- Section 19.8.3, “Automatic Deprovisioning Requests,” on page 253
- Section 19.8.4, “Managing Compensating Requests,” on page 254
- Section 19.8.5, “Understanding Inconsistency Detection and Resolution,” on page 255
- Section 19.8.6, “Creating Inconsistency Resolution Policies,” on page 258
- Section 19.8.7, “Manually Detecting and Resolving Inconsistencies,” on page 259
- Section 19.8.8, “Monitoring Business Role Detections,” on page 260

19.8.1 Understanding Business Role Detections

Business role detection is a process where Identity Governance updates business role memberships and business role authorizations. After business role memberships and authorizations are updated, Identity Governance might also issue the auto-grant and auto-revoke requests.

There are currently three types of business role detection:

All business roles

Identity Governance processes all published business roles in this type of detection. The following events trigger this type of detection:

- Publication of identities and applications
- Creation, deletion, or modification of technical roles
- Collection of identities after change events (also referred to as real time collection)

Business roles with expiring memberships or authorizations

Identity Governance processes business roles that have memberships or authorizations with an expiration date. Identity Governance automatically runs this type of detection every 24 hours.

Single business role

Identity Governance processes exactly one business role in this type of detection. The following events trigger this type of detection:

- Publication of a business role
- Deactivation or deletion of a published business role
- Curation (manual or bulk update) of users

  During this type of event, Identity Governance determines which business roles have membership expressions involving the attributes that were curated and schedules a business role detection for each of those business roles so that their membership is recalculated.

A business role detection, regardless of its type, has two phases. In phase one, it calculates business role memberships and authorizations. It also keeps track of all of the following types of authorization changes and uses this information in phase two:

- A user gains a new authorization for a resource that is auto-granted.

  This might occur because a user became a member of a new business role, or a new authorization was added to a business role that the user is already a member of.

  NOTE: If a business role authorizes a technical role and a new permission is added to the technical role, it ultimately results in a new authorization for that permission for all of the business role members.

- An authorization that is auto-granted and was *not* previously in its validity period enters its validity period.
- An authorization that is in its validity period changes from not auto-granted to auto-granted.
- A user loses an authorization for a resource that is auto-revoked.

This might occur because a user lost membership in a business role, an authorization was removed from a business role that the user is a member of, the business role is deleted, or the business role is deactivated.

NOTE: When evaluating whether to issue an auto-revoke request, Identity Governance ignores the loss of authorizations that occurs because an administrator deactivated the business role.

If a business role authorizes a technical role and a permission is deleted from the technical role, it ultimately results in the members of the business role losing their authorization for that permission. If the technical role itself is deleted, it ultimately results in the members of the business role losing authorization for all of the permissions that were contained in that technical role. However, if a technical role is simply deactivated rather than being deleted, business role authorizations stemming from that technical role are not lost.

Note that if a technical role is referenced by a business role, then Identity Governance will not allow you to delete or deactivate the technical role, unless the technical role is removed by the business role administrator from the list of all policies that references this technical role and prevents deactivation.

- An authorization that is auto-revoked and was *not* previously in its validity period exits its validity period.
- An authorization that is not in its validity period changes from not auto-revoked to auto-revoked.

During phase one, after Identity Governance calculates a business role's membership and authorizations, it determines what other business roles include the members of the business role and schedules single-role detections for each of those business roles. This occurs whether Identity Governance detects BR1 during an *all* business role detection or during a single-role detection for just BR1 because changes to the membership of a business role affect the membership of any business roles that include it. For example, if BR1 is included by BR2 and BR3, after calculating membership and authorizations for BR1, Identity Governance schedules single-role detections for BR2 and BR3.

In phase two of detection, using the information collected in phase one, Identity Governance determines what, if any, auto requests it should issue. For specific conditions that could result in auto-grant requests being issued, see Section 19.8.2, “Automatic Provisioning Requests,” on page 252. For specific conditions that could result in Identity Governance issuing auto-revoke requests, see Section 19.8.3, “Automatic Deprovisioning Requests,” on page 253.

Some of the conditions that could result in Identity Governance issuing an auto-grant or an auto-revoke request involve compensating for in-progress requests that would change whether a user has a particular resource. An administrator can configure Identity Governance to compensate for in-progress requests. For more information about compensating requests, see Section 19.8.4, “Managing Compensating Requests,” on page 254.

Although Identity Governance might issue auto-grant requests and auto-revoke requests in phase two of a business role detection, the requests might not ever be fulfilled for a variety of reasons. This results in situations where there might be users whose assigned resources are inconsistent with the auto-grant or the auto-revoke policies, or users that have pending grant or revocation requests for resources that, if fulfilled, would cause them to be inconsistent with the auto-grant or the auto-revoke policies. For more information about inconsistencies and inconsistency detection and resolution policies, see Section 19.8.5, “Understanding Inconsistency Detection and Resolution,” on page 255.

Depending on a variety of factors, business role detections can potentially take some time to complete. Identity Governance allows administrators to monitor the progress of business role detections and to see detailed information about in-progress and completed business role detections. For more information, see Section 19.8.8, “Monitoring Business Role Detections,” on page 260.

After business roles are detected, Identity Governance identifies auto-grants that require approval for potential SoD violations resulting from business roles. An administrator can view the status and timeline of those auto-grants if they navigate to **Business Roles** > **Auto Requests** > **Auto Requests**. They can check each request to know the list of business roles that made that request or select a request item status to view the timeline of underlying events associated with that request, including request details and the number of SoD violations the request is contributing to.

19.8.2 Automatic Provisioning Requests

During phase one of business role detection, Identity Governance gathers various types of authorization change events which trigger an evaluation of whether to issue an auto-grant request. The change events include user gaining a new authorization for a resource that specifies auto-grant, an auto-granted authorization entering its validity period, or an authorization in its validity period changing from *not* auto-granted to auto-granted. In phase two of business role detection, Identity Governance evaluates what, if any, auto-grant requests to issue.

Identity Governance issues an auto-grant request only if *all* of the following conditions are satisfied:

- The user + resource ends up being authorized after phase one business role detection.
- The user either is currently not assigned the resource (for applications assigned means the user has an account in the application) or there is a pending request to revoke the resource from the user and the request is one of the types that an administrator has specified as being compensatable.

  NOTE: Identity Governance considers a request as pending until it is in a **final state**. Final states include the following states: rejected by fulfiller, fulfillment error, fulfillment timed out, completed and verified, completed and not verified and verification ignored, or completed and verification timed out.

- There is no previously issued auto-grant request from a business role detection for the user + resource that is still in-progress. Auto-grant requests in a final state (see above) are obviously no longer in progress. In addition, a request that has completed (marked as fulfilled) is not considered to be in-progress, even though it might not yet be in verified, not verified and verification ignored, or verification timed out state.

  NOTE: When auto-grant option is enabled for a technical role resource, Identity Governance generates fulfillment requests for the permissions that make up the technical role, but does *not* generate fulfillment requests for the technical role assignment itself. Instead, Identity Governance makes a technical role assignment immediately if it determines that the user does not currently have the technical role assignment. Because there is no fulfillment request for making technical role assignments, the previous comments about Identity Governance checking for completed and in-progress pending fulfillment requests do not apply in the case of making technical role assignments.

19.8.3 Automatic Deprovisioning Requests

During phase one of business role detection, Identity Governance gathers various types of authorization change events which trigger an evaluation of whether to issue an auto-revoke request. The change events include a user losing an authorization for a resource that specifies auto-revoke, an auto-revoked authorization exiting its validity period, or an authorization in its validity period changing from *not* auto-revoked to auto-revoked. In phase two of business role detection, Identity Governance evaluates what, if any, auto-revoke requests to issue.

Identity Governance issues an auto-revoke request only if *all* of the following conditions are satisfied:

- The resource is not authorized for the user by any business role.
- The user either is currently assigned the resource (for applications, assigned means the user has an account in the application), or there is a pending request to grant the resource to the user and the request is one of the types that an administrator has specified as being compensatable.

  NOTE: Identity Governance considers a request to be pending until it is in a **final state**, which includes the following states: rejected by fulfiller, fulfillment error, fulfillment timed out, completed and verified, completed and not verified and verification ignored, or completed and verification timed out.

- There is no previously issued auto-revoke request from a business role detection for the user and resource that is still in progress. Auto-revoke requests in a final state (see above) are obviously no longer in progress. In addition, Identity Governance does not consider a request that has been completed (marked as fulfilled) to be in-progress, even though it might not yet be in verified, not verified and verification ignored, or verification timed out state.

  NOTE: When the auto-revoke option is enabled for a technical role resource, Identity Governance generates fulfillment requests for the permissions that make up the technical role, but does *not* generate fulfillment requests for the technical role assignment itself. Instead, Identity Governance removes a technical role assignment immediately if it determines that the user currently has the technical role assignment. Because there is no fulfillment request for removing technical role assignments, the previous comments about Identity Governance checking for completed and in-progress pending fulfillment requests do not apply in the case of removing technical role assignments.

The above conditions apply only to published business roles. Identity Governance ignores deactivated business roles when determining if all conditions are met. The following scenario provides an example of automatic deprovisioning.

Scenario 1: An authorized permission is removed from a business role

1. BR1 authorizes permission X and specifies auto-grant and auto-revoke on it.
2. User A is a member of BR1 and currently has permission X.
3. A business role administrator removes the permission X authorization from BR1 and re-publishes BR1. This action triggers business role detection on BR1.
4. Identity Governance detects that Permission X is no longer authorized for BR1, which means that all members who had authorizations for permission X from BR1 lose that authorization. User A is one of those members who lose the authorization.

5. The loss of user A's authorization for permission X causes Identity Governance to evaluate whether it should issue an auto-revoke request to remove permission X from user A.
6. Identity Governance issues an auto-revoke request to remove permission X from user A because all conditions for automatic deprovisioning are met:
    a. User A no longer has any authorization for permission X from *any* other business role,
    b. User A currently has permission X, and
    c. There is no in-progress auto-revoke request to remove permission X from user A.

19.8.4 Managing Compensating Requests

Identity Governance examines both the current state of the Identity Governance catalog and pending requests that might alter that state to determine if a user has a resource when it evaluates whether to issue an auto-grant or an auto-revoke request. Identity Governance compensates for pending fulfillment requests that would change whether the user has a resource. Identity Governance could grant a request to compensate for a pending revoke request, and it could issue a revoke request to compensate for a pending grant request.

NOTE: Identity Governance rules for generating compensating requests are applicable to the permissions that make up the technical role but are *not* applicable to technical role assignments.

The technical roles are managed and provisioned by Identity Governance itself. Auto-grant and auto-revoke of technical role assignments do *not* involve generation of fulfillment requests because there is no external data source for technical role assignments. Identity Governance makes or removes a technical role assignment immediately and does not trigger fulfillment requests or compensating requests.

Administrators can configure the types of requests for which Identity Governance might issue a compensating request. The type of request indicates the Identity Governance process from which the request originated. It might be an access request, a review, or a resolution of separation of duties violations.

NOTE: Identity Governance always compensates for pending requests that originated from the business role detection process.

To specify types of request that should generate compensating requests:

1 Log in to Identity Governance as a Customer, Global, or Business Roles Administrator.

2 Select **Policy** > **Business Roles** > **Auto Requests** > **Configure Compensating Requests**.

3 Select the additional type of requests for which the system should automatically compensate.

The following scenarios provide a few examples of when Identity Governance would issue compensating requests.

Scenario 1: User gains an auto request enabled permission that was lost but which Identity Governance considers as still authorized

1. Business role BR1 and business role BR2 both authorize permission X and both specify auto-grant and auto-revoke.
2. User A is a member of BR1 and currently has permission X.

3. An administrator or the system modifies user A's attributes so that the user is no longer a member of BR1. Identity Governance's real-time identity collection detects this change and user A loses authorization for permission X.
4. Identity Governance issues a revoke request to remove permission X from user A.
5. The application containing permission X removes permission X from user A.
6. An administrator or the system modifies user A's attributes again so the user becomes a member of BR2 and as such is authorized for permission X. The application containing permission X has removed permission X from user A, but the Identity Governance catalog still shows that user A has permission X because no one executed collection and publication of that application since Identity Governance issued the revoke request. Therefore, Identity Governance would not normally issue an auto-grant request for permission X.

   However, because the revoke request for permission X still shows that it is pending verification, and you configured Identity Governance to issue compensating grant requests for this type of revoke request, Identity Governance issues a compensating grant request for user A to be given permission X.

Scenario 2: User loses an auto request enabled permission that was granted but which Identity Governance considers as not authorized

1. Business role BR1 authorizes permission X and specifies auto-grant and auto-revoke.
2. User A has no permissions but an administrator or the system changes the user's attributes making the user a member of BR1. Real-time identity collection in Identity Governance detects this change and user A becomes a member of BR1 and gains an authorization for permission X.
3. Identity Governance issues a grant request for user A to have permission X.
4. The application that contains permission X assigns permission X to user A.
5. User A's attributes are changed again so that the user is no longer a member of BR1. User A's authorization for permission X is lost. The application containing permission X has assigned permission X to user A, but the Identity Governance catalog still shows that user A does not have permission X because no one executed collection and publication of that application since Identity Governance issued the grant request. Therefore, Identity Governance would not normally issue an auto-revoke request for permission X.

   However, because the grant request for permission X still shows that it is pending verification and you configured Identity Governance to issue compensating revoke requests for this type of grant request, Identity Governance issues a compensating revoke request to remove permission X from User A.

19.8.5 Understanding Inconsistency Detection and Resolution

Although Identity Governance might issue auto-grant requests and auto-revoke requests in phase two of a business role detection, the requests might not ever be fulfilled for a variety of reasons. The fulfillment system might handle the requests in a different order than they were issued, the fulfillment system could reject the request, or there could be an error fulfilling the request. In addition, external systems might change resource assignments without Identity Governance issuing

a request to do so. Identity Governance does not examine resource assignment changes when determining whether to issue an auto-grant or auto-revoke request because there would be additional overhead to do so, thus slowing down the business role detection process.

These kinds of scenarios can result in situations where there might be users whose assigned resources are inconsistent with the auto-grant or the auto-revoke policies, or users who have pending grant or revocation requests for resources that, if fulfilled, would cause them to be inconsistent with the auto-grant or the auto-revoke policies.

Inconsistency checking for permissions and applications includes checking for pending requests that might cause the permission or application to be held or not held in the future. A request is considered to still be pending even if its status has been changed to completed by a fulfiller (manual or automated provisioning process) and it is waiting for verification because the request might or might not result in the permission or application being held or not held in the future. Verification happens after a publication occurs. Once verification happens, the request will no longer be considered to be pending. Its status will change to either not verified or verified. Although not a final state, not verified is considered by inconsistency checking to no longer be a pending request and such a request is not considered when determining whether the permission or application might be held or not held in the future.

Administrators can detect and resolve inconsistencies manually or via policies. Administrators can:

- Manually click on refresh icon in the Action column to start auto-grant and auto-revoke inconsistency detections and optionally resolve them from the Manage Inconsistencies tab on the Business Role page.
- Create inconsistency resolution policies that automatically detect and resolve inconsistencies. Administrators can configure these policies to run on a schedule and also run them manually if needed from the Auto Resolution page.

Both methods, enable administrators to additionally:

- Detect *potential* auto-grant and auto-revoke inconsistencies

  If a user has a resource that is auto-granted by a business role and there is a pending request to revoke the resource, Identity Governance flags the pending revoke request as a potential inconsistency. Likewise, if a user does not have a resource that is auto-revoked by a business role and there is a pending request to grant the resource, Identity Governance flags the pending grant request as a potential inconsistency. Checking for potential inconsistencies is enabled by default, but it might need more resources and might be expensive, so administrator might choose to disable potential inconsistency detections.
- Use default (single complex query) or alternate (multiple simpler queries) algorithms for inconsistency detections

  Both algorithms result in the same number of detected inconsistencies, however, the elapsed time will differ based on the chosen algorithm. Administrators could monitor the performance using the two algorithms and choose the one that better meets their needs.

Though both methods support similar data monitoring and governance tasks, inconsistency resolution policies provide administrators greater flexibility in controlling what is automatically detected and resolved. When creating policies for inconsistency detection and resolution, administrators can select one or more inconsistency type to detect and resolve. Additionally, they can also configure specific rules to filter what is detected and resolved. For example, administrators could configure the policy to include or exclude potential inconsistency detection and not resolve inconsistencies if SoDs were not checked.

Identity Governance detects, resolves, and displays information about six types of inconsistencies: Auto-grant Permissions, Auto-grant Technical Roles, Auto-grant Applications, Auto-revoke Permissions, Auto-revoke Technical Roles, and Auto-revoke Applications. Information includes status, start time, end time, count of inconsistencies detected, who started the detection, who canceled the detection (if canceled), and so forth. If inconsistencies were not detected, the count column will have a value of zero. Administrators can import and export policies and download the inconsistency detection results to a CSV file.

Auto-grant request inconsistencies occur under the following conditions:

- One or more business roles authorize a resource (permission, technical role, or application) and specify that the resource is to be auto-granted to users.
- A user who is a member of one or more business roles either does not currently hold the authorized resource or may not hold the resource in the future due to a pending revoke request. In this context, Identity Governance considers only pending revoke requests that have been configured as compensatable requests.
- There is no in progress auto-grant request that would grant the resource to the user.

NOTE: There will never be pending revoke requests or in-progress auto-grant requests for technical role assignments because Identity Governance always removes and fulfills technical role assignments immediately.

Here is one scenario where an auto-grant request inconsistency could occur:

1. User A becomes a member of BR1 that authorizes permission X and specifies that X should be auto-granted. Identity Governance does not issue an auto-grant request because user A already has permission X.
2. The application that contains permission X removes permission X from user A without Identity Governance issuing any request to do so. This can happen because external applications might assign or unassign resources to or from users without receiving any request from Identity Governance to do so.
3. Identity Governance collects and publishes the application that contains permission X and updates its catalog to reflect that User A no longer has permission X. After the publication, Identity Governance triggers business role detection. However, Identity Governance does *not* issue an auto-grant for user A to have permission X, because detection did not see any authorization changes (the fact that the business role authorizes the user to have permission X did not change), and detection does not check to see if there were assignment changes.

   This results in an inconsistency between the auto-grant policy and the assignment state with respect to user A and permission X.

Auto-revoke request inconsistencies occur under the following conditions:

- A user either has a resource (permission, technical role, or application) or will have the resource in the future due to a pending grant request that is not currently authorized by any business role the user is a member of. In this context, Identity Governance considers only pending grant requests that have been configured as compensatable.

- The user was at one time a member of a business role that auto-revokes the resource. When checking for revoke inconsistencies, Identity Governance only considers the business roles the user was a member of within the last N days. Memberships held earlier than the last N days are not considered.
- There is no in progress auto-revoke request that would revoke the resource from the user.

NOTE: There will never be pending grant requests or in progress auto-revoke request for technical role assignments because Identity Governance always removes and fulfills technical role assignments immediately.

Here is one scenario where an auto-revoke request inconsistency could occur:

1. User A is a member of BR1 that authorizes permission X and specifies that X should be auto-revoked.
2. User A's attributes change in a way that causes the user to lose membership in BR1. The real-time collection process in Identity Governance detects the change. After it processes the change, Identity Governance triggers a business role detection. The detection causes Identity Governance to issue an auto-revoke request to remove permission X from user A.
3. The application that contains permission X removes permission X from user A. Later, however, the application restores permission X to user A. Again, remember that external applications might assign or unassign resources to or from users without receiving any request from Identity Governance to do so.
4. Identity Governance collects and publishes the application that contains permission X. After publication, business role detection is triggered. However, Identity Governance does *not* issue an auto-revoke request to remove permission X from user A, because detection did not see any *authorizations* that were lost (user A is still not authorized by any role to have permission X) and detection does not check to see if there were permission assignment changes.

   This results in an inconsistency in the auto-revoke policy for permission X because user A at one time was a member of BR1, and it specified that permission X should be auto-revoked.

19.8.6 Creating Inconsistency Resolution Policies

Automatically checking for all inconsistencies and conflicts and establishing process authority during normal business role detection and resolving them might slow down the business role detection process. However, by creating inconsistency resolution policies, administrators can automatically detect and resolve inconsistencies based on specific business needs. When not sure how to define policies to optimize performance, administrators could first manually initiate inconsistency detections, download results, and analyze results, then define and schedule specific inconsistency policies based on the business needs.

To create policies, then monitor inconsistencies and resolutions:

1. Log in to Identity Governance as a Customer or Global Administrator.
2. Select **Policy > Inconsistency Resolution**.
3. Click Plus icon to create a new policy
4. (Optional) Enable policy to be activated when you save the policy details. If you choose not to activate the policy after saving the policy, you can later select **Activate Policies** from the **Actions** menu to activate the policy.

5 Add name and description.

6 Select Business Role Auto Grant/Revoke as the resolution type to detect and resolve inconsistencies in business role auto grants and revokes.

7 On the Detection Settings tab, select inconsistency types and specify additional conditions and rules.

8 On the Resolution Settings tab, select inconsistency types and specify additional conditions and rules.

9 On the Schedule Settings tab, configure the auto-detection and resolution schedule.

10 Save the policy.

11 (Optional) Click Run Policy icon next to the name of the policy to manually run the policy for policy validation.

12 (Optional) Click the gear icon to customize the column display. For example, to view last run time, select **Last run time** in the Available Column list.

13 (Conditional) Once a policy has run automatically or was run manually, click **Auto Resolutions** tab.

14 Click the number of detected inconsistencies to view the list of inconsistencies in a pop-up window.

15 (Optional) In the pop-up window search bar, specify a user name, a permission, or a business role name to search for related inconsistencies.

16 Click the number of resolved inconsistencies to view the list of resolved requests in a pop-up window.

NOTE: Identity Governance assigns a color code for the inconsistency grant requests when they are submitted for fulfillment indicating pending requests from them with no inconsistencies. Similarly, when the requests are denied and the violations are cleared the color code is removed, which means inconsistencies are back.

---

17 (Optional) Select the associated auto-resolution policy on the Auto Resolution Policies tab, then click **Actions > Run Policies** to recalculate and update the number detected and resolved inconsistencies

18 (Optional) Download all or selected grant and revoke requests with inconsistency detection results as a CSV file.

19.8.7 Manually Detecting and Resolving Inconsistencies

Identity Governance allows an administrator to manually find inconsistencies and issue new requests to resolve them if needed. It is not a given that you should resolve all such inconsistencies, so Identity Governance provides an option to not do it automatically. This is especially true of the auto-revoke inconsistencies. The fact that a user was at one time a member of a business role that specifies that a permission the user holds should be auto-revoked might or might not be sufficient reason to revoke the permission from the user. If needed, administrators can download inconsistency results, analyze results, and select which inconsistency to resolve. Based on their analysis and authorization, they can provide inputs and optionally configure Inconsistency Resolution policies for automated inconsistency detections and resolutions.

To find and resolve inconsistencies manually:

1. Log in to Identity Governance as a Customer, Global, or Business Roles Administrator.
2. Select **Policy** > **Business Roles** > **Manage Inconsistencies**.
3. (Optional) Enable use of alternate algorithm to use multiple queries instead of a single complex query.
4. (Optional) Disable detection of potential inconsistencies.
5. (Optional) Click the gear icon to customize the column display. For example, to view who started the inconsistency detection, select **Started by** in the Available Column list.
6. To start inconsistency detection, click the refresh icon in the Action column.
7. (Conditional) If there are auto-revoke types, specify the number of days to search for lost business role memberships.

   When searching for auto-revoke inconsistencies, Identity Governance searches for authorizations that specify auto-revoke in business roles that users were previously members of. It only looks for business role memberships that the user lost within the last *N* days. Identity Governance ignores business role memberships that were lost before *N* days.
8. Click the number of detected inconsistencies to view the list of inconsistencies in a pop-up window.
9. (Optional) In the pop-up window search bar, specify a user name, a permission, or a business role name to search for related inconsistencies.
10. (Optional) Submit grant or revoke requests for some or all inconsistencies to resolve them.

    NOTE: Identity Governance assigns a color code for the inconsistency grant requests when they are submitted for fulfillment indicating pending requests from them with no inconsistencies. Similarly, when the requests are denied and the violations are cleared the color code is removed, which means inconsistencies are back.

    ---
11. (Optional) Click the refresh icon to recalculate and update the number detected inconsistencies
12. (Optional) Download one or more detected inconsistencies or all inconsistency detection results as a CSV file.

19.8.8 Monitoring Business Role Detections

Identity Governance enables administrators and support personnel to troubleshoot issues by looking at the progress and results of business role detections.

During business role detection, in addition to various instance times, Identity Governance stores the number of memberships, authorizations, and auto-requests. You can enable the collection of more detailed information on the exact memberships, authorizations, and auto-requests that were generated during detection by setting the following configuration properties using the Identity Governance Configuration Utility. For more information about the utility procedures, see "Using the Identity Governance Configuration Utility" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

IMPORTANT: If you enable the collection of detailed information, business role detections slow down and consume more space in the database to store the detailed information. Generally, you should enable the collection of detailed information only if you are troubleshooting a problem and need more information to determine what is happening.

- `com.netiq.iac.brd.log.detected.members`

  When set to `true` this configuration property causes business role detection to store the list of users who were added to and removed from a business role during the detection.

- `com.netiq.iac.brd.log.detected.auths`

  When set to `true` this configuration property causes business role detection to store the list of authorizations that were added and deleted during the detection.

- `com.netiq.iac.brd.log.detected.autorequests`

  When set to `true` this configuration property causes business role detection to store the list of auto-grant and auto-revoke requests that Identity Governance issued during the detection.

To monitor business role detections:

1. Log in to Identity Governance as a Customer, Global, or Business Roles Administrator.
2. Select **Policy** > **Business Roles** > **Business Role Detections**.
3. (Optional) Specify a business role name in the search bar to search for the detection status and details such as the detection end time, the number of auto-revokes generated for a business role, and so forth.
4. (Optional) Select the number of business roles completed to view additional details such as the number of members that the system added or removed, the number of authorizations that the system granted or revoked, and so forth.
5. (Optional) Select detections to delete. You should *not* delete a detection that is currently running.

You can click the settings icon to customize the columns displayed on the Business Roles Detection tab. For example, to add a column that displays the action that triggered each Business Role detection, click the settings icon, and then select **Detection Triggered By**.

19.9 Downloading and Importing Business Roles and Approval Policies

You can download business roles, approval policies, and other referenced objects, and import them later into an Identity Governance environment. The download will either generate a single JSON file or a zip file depending on the options you select during download, such as associated applications and assigned categories. In addition to downloading the business role or approval policy definitions, you can download the list of objects as a CSV file. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

20 Creating and Managing Separation of Duties Policies

Separation of Duties (SoD) Administrators can create policies to enable Identity Governance to look for users and accounts holding too much access. Identity Governance creates cases when it finds violations, and policy owners review the cases and approve or resolve the violations.

20.1 Understanding Separation of Duties

When a single person in your organization has access to too many systems, you could have problems proving that your systems are safe from fraud when it is time for audits.

The SoD Administrator should be a business owner who understands the appropriate access levels for individuals in your organization. By creating policies to keep a single person from having too much responsibility, the SoD Administrator enables Identity Governance to identify users with access to company assets that should be reviewed. SoD policies put access control rules over your business systems to give you the ability to show auditors the automated protection that Identity Governance provides.

Active SoD policies in Identity Governance provide the ability to check for violations and warn of violations when executing actions, such as performing reviews, defining roles, requesting access, approving access, or examining manual fulfillment requests.

SoD policies enable you to identify SoD violations in your current data. The SoD Administrator or policy owners review the requests to determine whether to resolve or approve the violation. If, based on the global potential SoD violation approval policy or a specific SoD policy, potential violations do not require approvals, Identity Governance sends the requests directly to fulfillment.

Identity Governance allows you to assign an **SoD approval policy** to specified SoD polices. SoD approval policies provide approval criteria for resolution or approval of existing violations, required approval of potential SoD violations for access requests, or to prevent approval for SoD violations that occur due to a toxic combination of permissions that should never be allowed. You can also set a default SoD approval policy to control if potential SoD violations require approval before the set of access requests are fulfilled. To determine which SoD approval policy is set as the default, select **Policy** > **SoD**, click the **SoD Approval Policy** tab, then click **Default SoD Approval Policy**. You can also run an Insight Query to view all your SoD policies and the SoD approval policies assigned to them. For more information, see “Creating and Assigning Separation of Duties Approval Policies” on page 269.

If no SoD approval policy is specified, potential SoD violations do not require approval, and Global, SoD, and Customer Administrators -- along with SoD owners and approvers -- may resolve or approve detected violations. For any *actual* violations of the policies, Identity Governance creates cases and lists them on the **Policy > Violations** page. The SoD Administrator or policy owners review the cases to determine whether to resolve or approve the violation.

The SoD cases are similar to the standard review process. Instead of a review definition running on a regular schedule, SoD policies run as long as they are active and continuously create cases for violations. SoD violations are also shown in review item expanded view. For more information about reviews, see Section 25.1, “Understanding the Process Flow,” on page 324. For more information about SoD violations, SoD cases, and potential SoD violations, see Chapter 21, “Managing Separation of Duties Violations,” on page 277.

20.2 Understanding the Separation of Duties Policy Options

An SoD policy defines which conditions make up the policy, what happens when the policy is violated, and how to resolve the violation. Use the following information to create the SoD policies that work best in your environment.

20.2.1 Providing Resolution Instructions for the Separation of Duties Policies

When you create an SoD policy, you can add resolution instructions in the **Resolve** field, and you can embed HTML links in those instructions to point to additional information or instructions for a user to follow when reviewing an SoD policy violation. Providing these instructions is optional. If you provide resolution instructions, users can see what to do to solve the violations without having to wait for further instructions.

Identity Governance displays the SoD violations with any instructions you have provided on the **Policy** > **Violations** tab. Users with the proper access can access and review these violations and resolve or approve the violations.

20.2.2 Deciding what Occurs for Separation of Duties Violations

When users review and manage an SoD case, they can resolve the violation or allow the violation to continue for a certain period of time. A user can specify compensating controls for an SoD policy. When allowing a violation to continue, if compensating controls have been defined for the policy, the user can select one or more of them to specify what controls should be in place in order to allow the violation to continue.

When users allow a violation to continue, the user can select one or more of the defined compensating controls to enforce during the continuation period of the violation. They can also specify the amount of time that the violation can continue, but the time must be less than or equal to the maximum control period defined in the policy. The maximum time is 32,768 days.

You add these compensating controls when you create the SoD policy in the **Compensating Controls** field.

20.2.3 Defining Separation of Duties Conditions, User Conditions, and Account Conditions

An SoD policy requires you to define one or more conditions that specify which combinations of permissions and roles users are not permitted to hold. Most of the time, a single condition suffices, but in some scenarios, you must define multiple conditions to cover more complicated combinations.

You can also configure expressions for user conditions and account conditions to specify that the SoD policy applies to specified users or unmapped accounts, such as users in specified locations, or accounts with a specified category. If you create an SoD policy with only SoD conditions, the policy applies to all users. In addition, you can define user conditions and account conditions to exclude specified users or unmapped accounts from an SoD policy.

Identity Governance tests a user's permissions and roles against a condition to see if the user holds the combination of permissions and roles specified in the condition. The user violates the SoD policy only if the user's permissions and roles violate *every* condition defined in the SoD policy.

Identity Governance also tests unmapped accounts against the SoD policies. Unmapped accounts, or accounts with no associated users, may have permissions assigned to them. As with user accounts, Identity Governance tests whether the account has the combination of permissions specified in the condition. If the account's permissions match the condition, the account violates that condition. The account violates the SoD policy only if the account's permissions violate *every* condition in the SoD policy.

Many simple policies require only a single condition to specify permission and role combinations that are not permitted. More complex combinations require multiple conditions, but you will rarely need more than two conditions.

Conditions consist of two parts:

- A list of one or more of the following:
  - The SoD Condition, which includes one or more of the following:
    - One or more Entities made up of permissions, business roles, and technical roles that Identity Governance tests against a user's permissions, business roles, and technical roles, which can consist of all permissions, all roles, or a mixture of permissions and roles
    - One or more Permission Expressions that Identity Governance tests against a user's permissions
    - One or more Business Role Expressions that Identity Governance tests against a user's business role assignments
    - One or more Technical Role Expressions that Identity Governance tests against a user's technical role assignments, or who hold all the permissions of the role
  - The User Condition includes one or more expressions that Identity Governance tests against a user's identity information
  - The Account Condition includes one or more expressions that Identity Governance tests against unmapped account information
- A condition *type* specifies how Identity Governance evaluates the user's permissions and roles. There are three types of policy conditions:

  User has all of the following

  A user violates this condition if the user has all the specified user conditions, account permissions, and SoD conditions. This condition is the most commonly used type. You can use this single condition to specify most combinations of permissions and roles that a user is not permitted to hold.

  NOTE: When you create expressions with the "has all" condition type, the user must hold all the items matching the query. For example, if the expression specifies permissions with category "Finance," a user would be in violation only if the user holds all permissions with the "Finance" category.

  User has one or more of the following

  A user violates this condition if the user has at least one of the specified user conditions, account permissions, and SoD conditions.

  User has more than one of the following

  A user violates this condition if the user has two or more of the specified user conditions, account permissions, and SoD conditions. A condition of this type must list at least two permissions and roles. If the condition lists exactly two permissions and roles, it is equivalent to a **User has all of the following** condition with two permissions and roles.

When defining SoD conditions, you will see warnings and error messages when conditions need to be further refined. For a list of SoD-Conditions Messages, see *SoD Conditions Messages Technical Reference (https://www.microfocus.com/documentation/identity-governance/4.3/tech-refs/SoD-conditions-messages.pdf)*.

20.2.4 Examples of Conditions for Separation of Duties Policies

You can combine user conditions, account conditions, and SoD conditions to allow you to create more flexible and dynamic SoD policies, as illustrated in the following examples.

Using categories to create SoD policies that automatically update with changes to the categories:

You can create a category and assign it to a set of permissions, business roles, or technical roles that would cause a user to be in violation of the SoD policy. If the category assignments change after you create the SoD policy, the SoD violations are automatically updated without having to add the new permission, technical role, or business role to the SoD policy condition items.

To create an SoD policy for this example:

1. Log in as a Customer, Global, or Separation of Duties Administrator.
2. Select **Policy** > **SoD**.
3. Click the plus sign (+).
4. Provide a name, description, and owner for the SoD policy.
5. Under **SoD Conditions**, use the drop-down list to specify that "A user is in violation if" **User has one or more of the following:**, **All of the following:**, or **More than one of the following:**.
6. Next to **Add items**, click the plus sign (+).
7. Select **Add Permission Expression**.
8. In the Expression Builder, use the drop-down lists to specify **Categories** and **equal to**, then type the category name.
9. Define any additional conditions or filters.
10. Click **Save**.
11. Click **Save** to save the policy.

Combine conditions to exclude some users from defined account conditions or SoD conditions:

You can combine conditions to create an SoD policy of which a user is in violation only if the user does not match one of the defined conditions. For example, you can combine conditions to specify that users who are *not* in the Finance Department would violate a SoD policy if they hold any permissions from the "Finance Application."

To create an SoD policy for this example:

1. Log in as a Customer, Global, or Separation of Duties Administrator.
2. Select **Policy** > **SoD**.
3. Click the plus sign (+).
4. Provide a name, description, and owner for the SoD policy.
5. Next to **User Conditions**, click the plus sign (+).
6. In the Expression Builder, use the drop-down lists to specify **Department** and **not equal to**, then type `Finance`.
7. Click **Save**.
8. Under **SoD Conditions**, use the drop-down list to specify that "A user is in violation if" **User has one or more of the following:**, **All of the following:**, or **More than one of the following:**.

9 Next to **Add items**, click the plus sign (+).

10 Select **Add Permission Expression**.

11 In the Expression Builder, use the drop-down lists to specify **Application** and **equal to**, then type `Finance Application`.

12 Click **Save**.

13 Click **Save** to save the policy.

20.3 Creating and Editing Separation of Duties Policies

After you publish data, you can create separation of duties (SoD) policies that Identity Governance uses to alert you of possible violations. Active SoD policy definitions allow Identity Governance to list violations and create cases for you to review and approve, or to send to fulfillment for correction. Users with the Customer, Global, or Separation of Duties Administrator authorization can create and modify SoD policies.

NOTE: Until you publish data, no permissions are available to include as SoD Conditions for an SoD policy.

Once you create SoD policies, by default, Identity Governance enables authorized users to analyze SoD violations when they create technical and business or request access to applications, permissions, or technical roles. Additionally, for technical roles, you can also configure violation options.

To create an SoD policy:

1 Log in as a Customer, Global, or Separation of Duties Administrator

2 Select **Policy** > **SoD**.

3 Click the plus sign (+).

4 (Optional) Select **Active** to have Identity Governance discover violations of the policy and create SoD violations and cases.

5 Provide the requested information. For more information about defining SoD conditions, see "Defining Separation of Duties Conditions, User Conditions, and Account Conditions" on page 265. For more information about the policy option fields, see "Understanding the Separation of Duties Policy Options" on page 264.

NOTE: Policy names must be unique, but they are not case sensitive. Therefore, Identity Governance considers "SoD1" and "SOD1" to be equivalent.

---

6 (Optional) Specify a potential SoD violation approval policy for the current policy by overriding global policy.

7 (Optional) On the **Violation Conditions** tab, define **User Conditions** and **Account Conditions**, then define one or more **SoD Conditions**.

8 On the **Violation Conditions** tab, define the one or more required **SoD Conditions**. For more information about defining these conditions, see "Defining Separation of Duties Conditions, User Conditions, and Account Conditions" on page 265 and Section 20.2.4, "Examples of Conditions for Separation of Duties Policies," on page 267.

9 (Optional) Specify one or more compensating controls and a maximum control period. Identity Governance displays these compensating controls in SoD cases as a selection for approving a violation to continue for a certain time period.

10 (Optional) Click **Estimate Violations** to see an estimate of the number of violations of this policy.

11 Click **Save**.

If, after you create and activate a policy, some of the permissions or authorizations listed in the policy's conditions are deleted, the policy is marked as invalid, and all the currently open SoD cases for the policy are put on hold. If the policy is not active, deleting its permissions or authorizations has no effect, since no detection is being done for the policy. You can avoid this situation by using categories in SoD policies. For more information, see Section 20.2.4, “Examples of Conditions for Separation of Duties Policies,” on page 267.

You can select any SoD policy and click **Edit** to modify the policy and its conditions.

Note that a deactivated technical role is excluded from the SoD policy detection. If the role becomes active later and matches the detection condition, then it is included in the detection process. If a technical role is referenced by an SoD policy, then Identity Governance will not allow you to delete or deactivate the technical role, unless the technical role is removed by the administrator from the list of all policies that references this technical role and prevents deactivation.

20.4 Downloading and Importing Separation of Duties Policies

You can download SoD policies and import them later into an Identity Governance environment. The download will generate either a single JSON file or a Zip file, depending on the options you select during download, such as associated applications and referenced roles. In addition to downloading the SoD policy definitions, you can download the list of SoD policies as a CSV file. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

20.5 Creating and Assigning Separation of Duties Approval Policies

Identity Governance allows you to create, edit, import, download (export), and assign SoD approval policies to specified SoD polices. SoD approval policies provide approval criteria for the following:

- Resolution or approval, by one or more people, of detected SoD violations
- Required approval, by one or more people, of potential SoD violations for access requests
- Prevention of approval for SoD violations that occur due to a toxic combination of permissions that should never be allowed

Identity Governance provides the following SoD approval policies, which you can either use as configured, or edit to customize for your organization:

Auto Deny

This SoD approval policy is configured to prevent requesting any resources that violate the SoD policy conditions or approval of any existing or potential SoD violations. The approval policy can be used if an SoD violation is considered to have toxic combinations that should never be allowed. For more information, see "Creating an SoD Approval Policy for Toxic SoD Violations" on page 271

SoD Administrators

This SoD approval policy does not require approval for potential SoD violations, but allows any detected SoD violations to be mitigated by users with permission to manage SoD policies, such as SoD Owners, Global Administrators, Customer Administrators, or SoD Administrators.

SoD Owner Approval

This SoD approval policy requires SoD Owners to approve any potential SoD violation, and allows any detected SoD violations to be mitigated by users who can manage SoD policies, such as SoD Owners, Global Administrators, Customer Administrators, or SoD Administrators.

NOTE: Identity Governance does not require approval of a potential SoD violation if the violation already exists and if the violation is not toxic.

When you configure an SoD approval policy Identity Governance sends email notifications to alert or remind approvers of outstanding tasks, and provides support for escalation if the approvers do not complete tasks within a specified period.

You are not required to assign an SoD approval policy to SoD policies. However, if you do not assign an SoD approval policy to SoD policies, SoD owners are required to resolve or approve detected violations. For more information, see "Assigning a Default SoD Approval Policy" on page 274

20.5.1 Creating and Editing SoD Approval Policies

Identity Governance allows you to create SoD approval policies, and also provides three SoD approval policies that cover general situations.

To create an SoD approval policy:

1. Log in as a Customer, Global, or Separation of Duties Administrator.
2. Select **Policy** > **SoD**, then click **SoD Approval Policies**.
3. Click **SoD Approval Policies**, then click the plus sign (+).
4. Provide a name and description for the SoD approval policy.

5 (Conditional) If you want to create an SoD approval policy that specifies an SoD violation as having toxic combinations and should never be allowed, specify the **Toxic user condition** and/or the **Toxic account condition**. For more information, see "Creating an SoD Approval Policy for Toxic SoD Violations" on page 271

6 Next to **Approval Steps**, click the plus sign (+).

7 Click **Approval Step #1, Approvers; Supervisors**, then provide the requested information for:

- Approvers - Select one of the following to specify the approver:
  - **Violator supervisor**
  - **SoD policy owner**
  - **Select users and groups**

  NOTE: If you specify multiple users or a group as the approver, only one potential approver of those specified is required to complete the approval step.
- Notifications
- Approval Escalation

  NOTE: The escalation approver is added to the approval task only if the approval step is not complete by the specified escalation period.

8 (Conditional) If you need to require multiple approvers for potential SoD violations, see Section 20.5.3, "Requiring Multiple Approvals for SoD Violations," on page 272.

9 Click **Save**.

After saving the SoD approval policy, you can click the **SoD Approval Policies** tab to immediately assign the SoD approval policy to an SoD policy. If you want to assign the SoD approval policy at a later time, you can do so using the **Separation of Duties Policies** tab. For more information, see "Assigning SoD Approval Policies" on page 273.

You may edit the SoD approval policies, including those provided by Identity Governance, as needed.

To edit an SoD Approval policy:

1 Log in as a Customer, Global, or Separation of Duties Administrator.

2 Select **Policy** > **SoD**, then click **SoD Approval Policies**.

3 Click **SoD Approval Policies**.

4 Click the SoD approval policy you want to modify, then click **Edit**.

5 Make the desired changes to the SoD approval policy, then click **Save**.

20.5.2 Creating an SoD Approval Policy for Toxic SoD Violations

Identity Governance normally raises potential SoD violations to the SoD Administrator or the SoD Owner specified in the SoD policy, but does not prevent them from temporarily approving the request and allowing the violation to occur for a specified period of time. In some cases, however, your organization may want to designate the combination of user and/or account conditions defined

in an SoD policy as **toxic** to ensure that no request that violates the SoD policy may be granted under any circumstances. You may use or edit the provided Auto Deny SoD approval policy, or you may configure your own.

Identity Governance allows you to configure an SoD approval policy to make the SoD policy toxic for all users, all accounts, or to create expressions that would make the SoD policy toxic for specific sets of users or orphaned accounts. For example, you can use the Expression Builder to specify that an SoD policy is toxic if the violating user is in a specified department or works under a specified supervisor.

To configure an SoD approval policy for toxic SoD conditions:

1. Log in as a Customer, Global, or Separation of Duties Administrator.
2. Select **Policy** > **SoD**, then click **SoD Approval Policies**.
3. Click **SoD Approval Policies**, then click the plus sign (+).
4. Provide a name and description for the SoD approval policy.
5. Specify the **Toxic user condition** or the **Toxic account condition** as one of the following:
   - Always Toxic
   - Expression

   NOTE: If you select **Expression**, use the Expression Builder to create expressions from one or more conditions and filters that define the toxic attributes for the violator or the account.
6. Click **Save**.

After you save the SoD approval policy, you can click the **SoD Policies** tab to immediately assign the SoD approval policy to an SoD policy, or you can assign the SoD approval policy at a later time. For more information, see "Assigning SoD Approval Policies" on page 273.

20.5.3 Requiring Multiple Approvals for SoD Violations

Identity Governance allows a Customer, Global, or Separation of Duties Administrator to create and configure multi-step approval processes that require at least two people to approve an SoD violation. Configuring an SoD approval policy to use this **four-eyes principle** ensures that a violation is approved by multiple people. It also ensures that any user who approves the SoD violation at one step is excluded as an approver for subsequent steps, and it prevents users from approving their own SoD violations.

To configure multiple approvals for SoD violations:

1. Log in as a Customer, Global, or Separation of Duties Administrator.
2. Select **Policy** > **SoD**, then click **SoD Approval Policies**.
3. Click **SoD Approval Policies**, then click the plus sign (+).
4. Provide a name and description for the SoD approval policy.
5. Specify the **Toxic user condition** or the **Toxic account condition** as:
   - None
   - Always Toxic
   - Expression

NOTE: If you select **Always Toxic** for both the **Toxic user condition** and the **Toxic account condition**, you are creating an SoD approval policy for toxic conditions, and cannot assign approval steps.

NOTE: If you select **Expression**, use the Expression Builder to create expressions from one or more conditions and filters that define the toxic attributes for the violator or the account.

6 Next to **Approval Steps**, click the plus sign (+).

7 Click **Approval Step #1, Approvers; Supervisors**, then provide the requested information for:

- Approvers - Select one of the following to specify the approver:
  - **Violator supervisor**
  - **SoD policy owner**
  - **Select users and groups**

  NOTE: If you specify multiple users or a group as the approver, only one potential approver of those specified is required to complete the approval step.
- Notifications
- Approval Escalation

  NOTE: The escalation approver is added to the approval task only if the approval step is not complete by the specified escalation period.

8 Repeat Steps 6 and 7 for each additional approver required for the SoD potential violation.

9 Click **Save**.

After you save the SoD approval policy, you can click the **SoD Policies** tab to immediately assign the SoD approval policy to an SoD policy, or you can assign the SoD approval policy at a later time. For more information, see "Assigning SoD Approval Policies" on page 273.

20.5.4 Assigning SoD Approval Policies

Identity Governance allows you to assign an SoD approval policy to specified SoD polices that provide approval criteria for resolution or approval of existing violations, required approval of potential SoD violations for access requests, or to prevent approval for SoD violations that occur due to a toxic combination of permissions that should never be allowed. You can also set any SoD approval policy as the default approval policy for the SoD policies that are not assigned an SoD approval policy.

You are not required to assign an SoD approval policy to SoD policies. If you do not assign an SoD approval policy, and if you do not set a default SoD approval policy, SoD owners will be required to resolve or approve detected violations.

To assign an SoD approval policy from the Separation of Duties Policies tab:

1 Log in as a Customer, Global, or Separation of Duties Administrator

2 Select **Policy** > **SoD**.

3 On the **Separation of Duties Policies** tab, select one or more SoD policies.

4 **Select Action** > **Assign approval policy**.

5 Search for, and select, an SoD approval policy to assign to the specified SoD policies.

6 Click **Assign**.

Identity Governance also allows you to assign an SoD approval policy from the **Separation of Duties Approval Policies** tab. This functionality allows you to assign the SoD approval policy to an SoD policy immediately after you save the approval policy.

To assign an SoD approval policy from the Separation of Duties Approval Policies tab:

1 After you save an SoD approval policy, click the **SoD Policies** tab.

2 Click the plus sign (+).

3 Search for, and select, the SoD policies to which you want to assign this SoD approval policy.

4 Click **Add**.

20.5.5 Assigning a Default SoD Approval Policy

Global, Customer, and SoD Administrators can set any SoD approval policy as the default approval policy to govern the SoD policies that are not assigned an SoD approval policy. The selected default SoD approval policy will be used for both SoD violation resolution or approval, as well as potential SoD violations.

You are not required to assign an SoD approval policy to SoD policies. If you do not assign a default approval policy field, Identity Governance requires SoD owners to resolve or approve detected violations. However, requested items that may result in a violation will not require SoD owner approval before fulfillment.

To assign a default SoD approval policy:

1 Log in as a Customer, Global, or Separation of Duties Administrator.

2 Select **Policy** > **SoD**, then click **SoD Approval Policies**.

3 Click **Default SoD Approval Policy**.

4 Search for, and select, the SoD approval policy you want to assign as the default policy.

5 Click **Add**.

The default SoD approval policy does not appear in the **SoD Approval Policy** column on the **Separation of Duties Policies** page. To determine which SoD approval policy is the default, select the **SoD Approval Policies** tab, then click **Default SoD Approval Policy**. You can also run an Insight Query to view all your SoD policies and the SoD approval policies assigned to them. If you do not set a default SoD approval policy, then no potential SoD violation approval is required, and SoD Owners, Global Administrators, and Customer Administrators may resolve or approve SoD violations.

20.5.6 Downloading and Importing SoD Approval Policies

Identity Governance allows you to download a list of all SoD approval policy descriptions as a CSV file, download SoD approval policy definitions as JSON files, and import the SoD approval policy definitions.

You can view or manage downloaded files using the downloads icon on your browser, or through the Downloads directory of your computer. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

20.6 Configuring SoD Violation Options for Technical Roles

By default, Identity Governance calculates SoD violations for both detected and assigned technical roles. You can choose to calculate SoD violations only for detected roles using the **Violation Options** tab. Identity Governance automatically removes technical role assignments when authorized administrators resolve SoD violations that were generated during calculation of violations for both detected and assigned technical roles. You can choose to enable or disable automatic removal of technical role assignments when you specify calculation of violations only for detected roles.

To configure SoD Violations Options for Technical Roles:

1. Log in as a Customer, Global, or Separation of Duties Administrator.
2. Select **Policy** > **SoD**.
3. On the **Violation Options** tab, specify whether Identity Governance should calculate violations for detected and assigned technical roles or only detected technical roles.
4. (Conditional) When specifying SoD violation calculations only for detected technical roles, enable or disable automatic removal of role assignments.

21 Managing Separation of Duties Violations

Identity Governance allows you to define and activate separation of duties (SoD) policies so the system can look for actual and potential violations of the policies. SoD policies let you identify combinations of permissions and authorizations that no one person should be granted.

When you have active SoD policies, Identity Governance monitors your environment for violations and creates cases when it finds violations. SoD administrators and policy owners, as well as step approvers specified in SoD approval policies, can either approve the violation for a time period or remove enough access to resolve the violation. When you remove access, Identity Governance creates a **changeset** for fulfillment. For more information, see Section 14.6, “Fulfilling Changesets,” on page 170.

21.1 Separation of Duties Violation Versus Separation of Duties Case

The terms “SoD violation” and “SoD case” are sometimes used interchangeably. Both refer to a specific user or account violating a specific SoD policy. However, Identity Governance can detect an actual SoD violation multiple times, because of the variety of events that trigger an SoD violation detection. For example, publishing identities and accounts, creating, changing, or deleting roles all trigger an SoD violation detection. Identity Governance creates a new SoD violation record for each of those detections and also notifies the SoD Policy Owner of these violations. All represent the same SoD violation, with different detection times. In addition, the following situations affect SoD approvals and detections:

- If an SoD policy is deactivated and later reactivated, or if conditions defined in the SoD policy change, Identity Governance starts the approval process again.
- Publications and changes to business role memberships that occur after Identity Governance detects an SoD violation could change the violation, so Identity Governance runs the detection process again for all active SoD policies, or for SoD policies that reference the business role.
- Publications and changes to business role memberships could add contributing items to an SoD violation. In this case, Identity Governance does not restart the SoD approval process. If the approval process has not completed all the steps of a multiple-step approval process, the process remains at the current step. Step approvers always see the items currently causing the

SoD violation and be able to approve or resolve the violation. The contributing items, however, could change from step to step, depending on whether the change was due to a user gaining permissions from a publication, or a change to a user's business role membership.

- If publications and changes to business role membership result in an SoD violation no longer existing, Identity Governance terminates the SoD approval process, closes the SoD case, and records the reason for closing the SoD case.

An SoD case is the entity that tracks all of the information about an SoD violation, including all of the times the violation was detected. It also keeps track of the actions which users have taken with respect to the violation (approve, resolve). An SoD case is closed when Identity Governance no longer detects the violation. In a sense, an SoD case is the history of an SoD violation from the time it is first detected to the time it is no longer detected.

21.2 Listing Separation of Duties Violations and Cases

Identity Governance includes multiple places where actual SoD violations may be listed and the associated SoD case managed. Which you use depends on your needs.

To view SoD violations for a particular user or account:

1. Select **Catalog** > **Identities** (or **Accounts**).
2. Select the user or account you want to see.
3. Select the **Separation of Duties Policy Violations** tab.

NOTE: Identity Governance only displays this tab for a user or account if they have active violations. This tab shows only the SoD violations whose associated SoD case is currently open.

To view SoD violations for a particular SoD policy:

1. Under **Policy**, select **Violations**.
2. Filter on SoD case state list by selecting any of the state icons. For example **Total**, **Not Reviewed**, or **Approved**. You can also perform advanced searches. For more information, see Section 12.4.3, “Using Advanced Filters for Searches,” on page 134.

21.3 Viewing SoD Case Details

After you have a list of the actual SoD violations or SoD cases, you can expand them to see the associated SoD case information. The information displayed is:

- Information about the user or account that is in violation
- Information about the SoD policy being violated, including the conditions
- Information about the SoD case, including status
- If applicable, the current step approver

You can see the list of actions taken by selecting the count in **# Actions**.

While viewing SoD details, if you have appropriate rights and the SoD case is still open, you can resolve or approve the violation.

21.4 Understanding SoD Case Status

Identity Governance tracks and records all decisions and selections during the life cycle of an SoD case. The following table provides a brief description of the possible status of an SoD case.

SoD Case Status	Description
Not Reviewed	When Identity Governance first detects an SoD violation, it creates an SoD case, which is put into this state. This indicates that nobody has yet determined what to do about the violation. Users may have looked at it, but they have not determined whether to approve it or request that certain permissions be removed in order to resolve it. If the SoD violation requires multiple approvers, and if they have not all completed their approval steps, Identity Governance displays the current approval step and the total number of approval steps (Step Approval x of y).
Approved	A user has reviewed and approved the SoD case. Approval means the user determined that the SoD violation could continue for a certain period of time – the control period. There might be one or more compensating controls that were specified. Compensating controls are basically the conditions under which the approval was granted. It is expected that the compensating controls will be in effect during the approval period.
Approval Expired	A user approved the SoD case at one time, but the control period has expired.
Resolving	A user reviewed the SoD case and determined that one or more permissions should be removed in order to resolve the SoD violation. Change requests will have been initiated to remove one or more permissions. The SoD case will be in the resolving state until Identity Governance detects that the permission(s) have actually been removed. The resolving state can also be overridden if a user later on decides to approve the case instead of resolving it.
On Hold - Policy Inactive	SoD case is on hold because the policy has been deactivated.
On Hold - Policy Invalid	SoD case is on hold because the policy has become invalid. A SoD policy would become invalid if any of the permissions or technical roles it specified were deleted from the catalog.
Closed - Policy Deleted	SoD case has been closed because the SoD policy has been deleted. Thus, there is no longer an SoD policy to violate.
Closed - Policy Conditions Changed	SoD case has been closed because the SoD policy's conditions were changed.

SoD Case Status	Description
Closed - Permissions or Roles Removed	SoD case has been closed because the violating user or account no longer has one or more of the permissions or technical roles that was causing the violation.
Closed - User Deleted	SoD case has been closed because the violating user is no longer found in the catalog.
Closed - Account Deleted	SoD case has been closed because the violating account is no longer found in the catalog.

21.5 Approving or Resolving an SoD Violation

When you approve an SoD violation, Identity Governance records that a designated user recognized the violation and gave approval to allow the violation to continue for a specified time period. A comment is required when approving a violation. You must also specify the time period (expressed in number of days) that the violation is allowed to continue. If the SoD policy includes defined compensating controls, you can select one or more controls. Doing so allows you to state which controls you want to be enforced while the violation is allowed to continue.

If a potential SoD violation requires multiple approvers (as designated by an SoD approval policy configured to use the "four-eyes" principle), the violation is not approved until all specified approvers complete their respective approval steps. After an approver provides their approval, they may not participate in subsequent approval steps. However, they may resolve the violation, which completes the approval process. An approval step must be completed before Identity Governance notifies the approver(s) specified in the following approval step of their approval task. If an approver does not complete their SoD approval step by the expiration interval defined in the SoD approval policy, Identity Governance adds the escalation approver defined in the approval step to the list of available approvers for that step.

NOTE: If an approval step specifies either a group, or more than one user as an approver, only one potential approver of those listed is required to complete the approval step.

To approve an SoD violation:

1. Select **Policy** > **Violations**.
2. Select the user name with an SoD violation you want to approve.
3. Click **Approve**.
4. Provide the required information.
5. Click **Approve**.

Resolving an SoD violation allows you to specify which permissions or roles you want removed from the user. From the Separation of Duties Violations page, you can select the name of a user who is in violation of an SoD policy to view details about the violation, including the policy name and the permissions, roles, or expressions that violate the policy. Clicking **Resolve** allows you to view the details of the permissions and roles causing the violation, and allows you to remove the permissions or roles from the user. In addition, if a policy expression is causing the violation, you can click the expression to view its permissions and roles and remove them from the user. When you resolve an

SoD violation by removing permissions and roles from the user, Identity Governance generates a request to remove the permission or role, which appears in Fulfillment. You can visit the fulfillment pages to perform the fulfillment actions. For more information, see Section 14.6, “Fulfilling Changesets,” on page 170.

NOTE: If the SoD policy violation requires multiple approvers, any of the step approvers may resolve the violation as their step action. Resolving the SoD policy violation completes the approval process, and any subsequent approval steps are no longer required.

IMPORTANT: If a violation is either in progress or not yet resolved, and the SoD policy is assigned to an SoD approval policy that designates the combination of user and/or account conditions defined in the SoD policy as toxic, the current "in-progress" violation will not change, and the approval process can continue. When the control period specified during this approval expires, the violation will be up for approval again, but with the toxic condition described by the changed SoD approval policy. In that case, you will not be allowed to resolve the violation. The only option available for toxic violations is to remove one or more of the violating permissions.

To resolve an SoD Violation:

1. Select **Policy** > **Violations**.
2. Select the user name with an SoD violation you want to resolve.
3. Click **Resolve** to display the permissions and roles, and the expressions containing permissions and roles, that caused the violation.
4. Remove one or more permissions or roles from the user that would resolve the SoD violation.

   NOTE: To automatically remove technical role assignments (included permissions) when removing a detected technical role to resolve a SoD violation, configure SoD Violations for detected and assigned roles using the **Violation Options** tab or if calculating SoDs for only detected roles, make sure **Remove role assignments** is enabled.

   ---
5. Provide a comment that describes for the fulfiller the actions needed to resolve the SoD violation.
6. Click **Resolve**.

IMPORTANT: Closing an SoD case is not the same as the resolve action. It does not occur automatically because a resolve action has been performed. The resolve action simply initiates fulfillment tasks and notifies appropriate users of the need to perform removal actions and what specific removals are being requested. It does not actually remove permissions or roles. It might be that nobody ends up performing the fulfillment tasks, or rejects them and nothing changes, in which case the SoD violation does not go away and the SoD case remains open.

Resolved SoD violations appear as fulfillment requests that you can view by selecting **Fulfillment** > **Requests**.

21.6 Closing an SoD Case

Identity Governance automatically closes an SoD case under any of the following conditions:

- Identity Governance detects that enough permissions and roles have been removed from the user or account that is in violation so that the SoD violation is no longer detected.
- Someone deletes the SoD policy. All SoD violations for the SoD policy cease to exist when the policy does not exist.
- Someone changes the conditions of the SoD policy such that the SoD violation no longer exists.
- The violating user or account is no longer found in the catalog.

21.7 Understanding Potential SoD Violations

A **potential SoD violation** refers to a scenario where an access request might violate previously defined SoD policies when fulfilled. Identity Governance automatically detects potential SoD violations if Customer, Global, or SoD administrators have previously defined SoD policies. It also enables Customer, Global, or Business Role administrators to enable potential SoD violation detections for business role auto-grant requests.

When Customer, Global, or SoD Administrator create SoD approval policies and assign them to SoD policies, they can also specify whether potential SoD violations require approval before the set of access requests are fulfilled. They can also set an approval policy as the default SoD approval policy that will apply to any SoD policy with no SoD approval policy assigned.

If no SoD approval policy is assigned, and no default SoD approval policy is set, potential SoD violations do not require approval, and Customer, Global, or Separation of Duties Administrators — along with Separation of Duties owners and approvers — may resolve or approve detected violations.

21.8 Approving or Resolving Potential SoD Violations

Access requests might cause new potential SoD violations or they might contribute to existing SoD violations. If approval is required for potential SoD violations (as specified in the SoD policy or through a global policy), the access request items that contribute to the potential SoD violation will *not* advance to their next phase (approval or fulfillment) until *each* potential SoD violation they contribute to has been either resolved or approved by the approvers in the SoD approval policy assigned to the violated SoD policy or SoD administrators.

When there is another request item contributing to the existing SoD violation, a potential SoD approval request will not be triggered even when the SoD or global policy requires approval. This is because the decision made for the existing SoD violation will automatically resolve the potential SoD violation. However, if you want every potential SoD violation to require approval regardless of existing SoD violations, you can enable `com.netiq.iac.sof.psodv.alwaysRequireApproval` property using the **Administration > Advanced** menu by setting the value to `true`.

When potential SoD violations approval is required for access requests that have existing SoDs, then:

- Current SoD violations that have been approved will take the new potential SOD approval control period when the associated potential SoD violation is approved, the request is fulfilled, and a collection and publication is performed.
- Current SoD violations that are in a Not Reviewed state, will use the preapproval information for the last potential SoD violation approval and will be marked as approved.

Separate requests that create potential SoD violations will create multiple potential SoD violation approval tasks. When approving the SoD violation, Identity Governance will use the control period from the last approved potential SoD violation. Users can always change the control period in the SoD violation when the current approval expires.

If a potential SoD violation requires multiple approvers (as designated by an SoD approval policy configured to use the "four-eyes" principle), the violation is not approved until all specified approvers complete their respective approval steps. An approval step must be completed before Identity Governance notifies the approvers specified in the following approval step of their approval task. If an approver does not complete their SoD approval step by the expiration interval defined in the SoD approval policy, the approval step is assigned to the escalation approvers defined in the approval step.

NOTE: Any of the step approvers may resolve the violation as their step action.

All request items that contribute to the potential SoD violation must either be approved or denied to clear the potential violation. Denying request items might cause the potential SoD violation to be resolved. A potential SoD violation is considered to be **resolved** if it would no longer exist after denying one or more of the request items that contribute to it. No further action is required if a potential SoD violation is resolved.

If, on the other hand, the potential SoD violation still exists, and all approval steps are complete, the potential SoD violation is considered **preapproved**. Identity Governance will prompt the authorized approvers and administrators to provide the following information that will be used to automatically approve the actual SoD violation if the potential SoD violation becomes an actual SoD violation:

- **Preapproval expiration period**. If the potential SoD violation is detected as an actual SoD violation within this period, the SoD violation will be automatically approved. If the SoD violation is detected after this period, it is *not* automatically approved and must be resolved or approved manually by the SoD policy owner or the SoD administrator.

  NOTE: The actual SoD violation could be the result of someone fulfilling these specific requests, or because of other provisioning actions that were taken by users. Regardless of the reason, if the SoD violation occurs, preapproval will be given if the SoD violation occurred in the specified preapproval time period.

- **Reason for SoD approval**. Justification for approving a potential SoD violation.
- **Approval control period (days)**. If the preapproved violation is detected before the expiration period, the violation will be approved for the number of days specified here. When there are multiple approvers, subsequent approvers in a potential SoD violation approval process can reduce the control period but cannot increase the previously-specified control period.
- (Optional) **Compensating Control**. If compensating controls were specified in the SoD policy, the selection here indicates which compensating controls apply to the preapproval.

IMPORTANT: Identity Governance prevents preapproval of potential toxic SoD policy violations. For more information see “Creating an SoD Approval Policy for Toxic SoD Violations” on page 271.

NOTE: If an SoD policy changes its conditions, is deactivated, or is deleted, all potential SoD violation approval tasks associated with the SoD policy will be automatically finalized and submitted. Request items that were tentatively approved will be marked approved, items that were tentatively denied will be marked denied, and items where no decision was made will be marked as cleared. Items that were marked approved or cleared and were not associated with other potential SoD violation approval tasks will be advanced to their next phase (approval or fulfillment). For more information about viewing request status, see Section 24.2, “Requesting Access,” on page 314.

22 Calculating and Customizing Risk

Identity Governance allows custom definition of risk based on your policies and risk tolerance. Customized risk ranges and levels allow Identity Governance to calculate risk scores for your organization, users, applications, business roles, and permissions. Use risk scores to focus reviews and measure impact. Risk scoring supports better context for decision-makers who conduct reviews prioritized by risk scoring based on attribute value, group membership, management relationship, application, permission, cost, risk, and other criteria. For more information about conducting reviews based on risk, see Chapter 26, “Creating and Modifying Review Definitions,” on page 343.

22.1 Understanding Risk Levels and Risk Scoring

Identity Governance provides **risk levels** to help you classify and label risk factors that matter to your organization. You can configure the number of levels, size of levels, and names of levels to make them appropriate for your organization and stakeholders. **Risk scoring** provides a means for manually setting or calculating risk for the entire organization as well as for catalog objects and policies.

Identity Governance administrators can customize the following risk policies:

- Risk level configuration
- Governance risk score
- Application risk score
- User risk score
- Risk score schedule

Users with the following authorizations can manage and customize risk settings for your Identity Governance environment:

- Customer, Global, or Data Administrator
- Auditor (read only)

See the following sections for more details about how Identity Governance helps you manage risk in your environment:

22.1.1 Risk Levels

Identity Governance gives you the flexibility to create a risk scale of your own choosing. If your environment requires a high level of granularity, you can specify up to 10 risk levels. When you set the risk level size, Identity Governance automatically divides the risk levels in even increments and sets the maximum risk value for calculated values to the maximum value specified in your settings. You can further customize the risk levels by providing your own naming system to the levels. A color-code is assigned to each level ranging from blue at the low end to red at the high end.

22.1.2 Risk Scoring

A risk score quantifies the level of risk that an entity, such as a user or account, exposes an organization to. A higher risk score indicates that you have identified that item as riskier to your organization. You can **manually set** risk scores by collecting risk score attributes along with objects you collect or by using Identity Governance to assign risk scores to individual objects.

You can collect risk scores or assign risk scores to the following items:

- Users
- Accounts
- Applications
- Permissions
- Technical roles
- Separation of duties policies
- Business roles
- Certification policies

A **calculated** risk score is based on risk factors and the relative weighting of those factors that you define. You can configure Identity Governance to calculate the following risk scores, either on demand or on a regular schedule:

Governance (your overall system score)

Represents the current level of risk related to access and security that your organization is exposed to based on the risk factors and risk weights you have defined.

Application

Represents the current level of risk related to access and security of each application that your organization is exposed to based on the risk factors and risk weights you have defined.

User

Represents the current level of risk related to access and security for each user that your organization is exposed to based on the risk factors and risk weights you have defined.

NOTE: Objects and policies whose risk was not set are *not* considered in calculations. Only objects and policies with zero or greater than zero value is included in calculations. For example, if a user has two accounts with 50 and “Not set” as respective risk value, then the average **Base Score** calculation for **Risk of accounts assigned to the user** will be 50 as the second account will be ignored as its value was not set.

22.1.3 Risk Factors

Risk factors, metrics that affect a risk score, apply to specific items and can have a positive or negative impact on the item's risk score. The weight of a risk factor is the percentage of an item's risk that the factor comprises. The maximum value for any risk factor component is the maximum risk score for the item multiplied by the percentage weight of the factor. For example, an organization specifies that user risk score has a maximum value of 1000 and 3 risk factors of equal weight. Each risk factor can only account for one third of the user's risk score.

For some risk factors, Identity Governance uses either the average value or the maximum value for that factor, based on which one you select. Other risk factors use a range of values that you set. When you assign a weight to a risk factor, such as **Number of unmapped accounts**, Identity Governance then looks at the range you have specified. If the value of the risk factor is at or above the high range, Identity Governance applies the full weight for that risk factor to the risk score. If the value is below the high range, Identity Governance applies a percentage of the weight that is appropriate to the percentage of the high range for the value. If a risk factor value is at or below the low range, that factor does not add anything to the risk score.

You can use the following risk factors to control how Identity Governance calculates risk scores in your environment.

Governance Risk Factors	Risk Factor Type
User risk scores	Average or Max
Application risk scores	Average or Max
Account risk scores	Average or Max
Business role risk scores	Average or Max
Technical role risk scores	Average or Max
Permission risk scores	Average or Max
Number of unmapped accounts	Low to high range
Number of unauthorized assignment (permission and technical role)	Low to high range
Number of outstanding SOD violations	Low to high range
Number of expired certification violations	Low to high range
Total number of certification violations	Low to high range
Number of no decision certification violations	Low to high range
Number of not reviewed certification violations	Low to high range

Application Risk Factors	Risk Factor Type
Risk of assigned permissions in application	Average or Max
Risk of accounts in application	Average or Max
Number of unmapped accounts	Low to high range
Number of permissions in the application	Low to high range
Number of exceptions (access not authorized by policy)	Low to high range
Number of expired certification violations	Low to high range
Total number of certification violations	Low to high range
Number of no decision certification violations	Low to high range
Number of not reviewed certification violations	Low to high range
Collected application risk score attribute	Application attribute. Typically, application risk.

User Risk Factors	Risk Factor Type
Risk of permissions assigned to user	Average or Max
Risk of accounts assigned to user	Average or Max
Number of outstanding SOD violations	Low to high range
Number of exceptions (access not authorized by policy)	Low to high range
Number of permissions assigned to the user	Low to high range
Number of business roles the user is in	Low to high range
Collected user risk score attribute	Value
Number of expired certification violations	Low to high range
Total number of certification violations	Low to high range
Number of no decision certification violations	Low to high range
Number of not reviewed certification violations	Low to high range
Days past expired certification	Impact

22.1.4 Risk Score Calculation Details

Identity Governance performs separate calculations to determine an overall governance risk score and overall risk scores for each application and user.

NOTE: Large data sets can result in long calculation times. Identity Governance allows you to click **Cancel** to stop a risk score calculation in progress. If you have a large data set, consider scheduling risk score calculation at a time outside of normal business hours. See Section 22.4, "Setting and Viewing Risk Calculation Schedules and Status," on page 293.

The calculations use the following variables:

- **RFV:** raw risk factor value
- **LL:** lower boundary (typically 0)
- **UL:** upper boundary (100)
- **URL:** upper risk level value from risk level configuration
- **FW:** factor weight as a percentage
- **RRFV:** ranged risk factor value
- **RIS:** raw impact score. This is set to the impact value of the first interval range that matches the RFV.
- **NPA:** number of assigned permissions

Calculations include the following scores:

- **FRS:** factor risk score
- **RS:** overall entity risk score calculated as sum of all configured risk factor scores for the specific entity with FW > 0

Count risk factor score

FRS = RRFV * FW/100 where:

- RRFV = URL if (RFV - LL) > 0 is true and (RFV - UL) >= 0 is true
- RRFV = 0 if (RFV - LL) > 0 is false
- RRFV = RFV*URL/(UL-LL) if (RFV - LL) > 0 is true and (RFV - UL) >= 0 is false

Example

When:

- RFV is equal to NPA
- LL = 0
- UL = 50
- URL = 500
- FW = 100

Then:

- For NPA = 15, RFV = 15 and 15 - 0 > 0 is true and 15 - 50 >=0 is false; RRFV = 15*500/(50-0) = 150 and FRS = 150*100/100 = 150

- For NPA = 50, RFV = 50, and 50 - 0 > 0 is true and 50- 50 >=0 is true; RRFV = 500 and FRS = 500*100/100 = FRS = 500
- For NPA = 0, RFV = 0, and 0 - 0 > 0 is false; RRFV = 0 and FRS = 0*100/100 = 0

Aggregate risk factor score

FRS = RFV * FW/100

Interval based impact risk factor score

NOTE: This score is supported only for the overdue violations risk factor.

FRS=RIS * FW/100

Example

User has the following types of certification policy violations:

- No decision violation - 1
- Overdue 5 days violation - 1
- Overdue 15 days violation - 2
- Overdue 100 days violation - 3

Interval is configured as:

- Impact 200 for violations overdue 1 to 100 days
- Impact 400 for violations overdue over 101 days

FW is set to 100.

Based on the above conditions:

- RFV will be set to 100 because the certification policy violations max number of days overdue is 100
- RIS will be set as 200 because RFV = 100 is within the first interval range
- FRS = 200*100/100 = 200

Overall entity risk score

RS = SUM(FRS) where FW > 0

Keep in mind the following notes about raw score values:

- For **average or max risk factor types**, the raw score will be set to either the average or maximum value of all values for a specific calculation. For example, if the administrator has configured that the risk of permissions assigned to users be averaged, Identity Governance averages the permission risk values for each user in the catalog and reports this number as the raw score.
- For **low to high range risk factor types**, the raw score will be the value for a specific measure. For example, for the **Number of outstanding SOD violations** risk factor, the base score will be equal to the total number of outstanding SoD violations.
- For **value risk factor types**, the raw score will be set to a value. For **Collected user risk score attribute** factor it will be set to the value of the user attribute configured in the risk factor. For the **Risk** attribute it will be set to the collected risk value. For any other attribute, it will be set to the collected or curated value at calculation time.
- For **impact risk factor types**, the raw score will be set to a number of days.

Keep in mind the following notes about ranged scores:

- For **low to high range risk factor types**, the ranged score will depend on upper and low boundaries configured for a factor. The upper boundary is the value at which risk is maximal. Risk level has a boundary and factors have a boundary.

  The calculation compares the value to the upper bound to scale it. If the value is at or above the bound, it will apply the full weight to the target raw risk score. If the value is below the upper bound, it will determine the percentage of the upper bound (max risk) that the raw score represents and use that to determine the range to apply.

  The lower bound indicates that this factor is below threshold and should not have any effect on the risk score.
- For **impact risk factor types**, the raw score will be evaluated against the configured interval and proper impact will be determined.

22.1.5 Visualizing Risk

Identity Governance provides several ways you can visualize the risk factors in your environment. In most areas, you can also drill down to details that show you more context for how Identity Governance has assessed the risk.

- As a separate tab on **User** and **Application** details pages
- As a governance risk score, and trend graph if multiple scores exist, displayed on the Governance Overview dashboard
- As a governance risk score and context information on the Risk policy administration page

Identity Governance assigns a color code to each risk level ranging from blue at the low end to red at the high end. These colors display with risk scores to help you further understand how the score fits into your customized risk level ranges.

22.2 Configuring Risk Levels

Identity Governance provides five risk levels in 20-point increments by default. You can set risk values for most objects in the catalog and for separation of duties policies and business roles. Identity Governance lets you customize the number, size, and name of each risk level. For example, if you set four risk levels with a size of 25, Identity Governance creates four equally sized risk levels of 0-25, 26-50, 51-75, and 76-100.

1. Log in as a Customer, Global, or Data Administrator.
2. Under **Policy**, select **Risk**.
3. Expand **Risk Level Configuration**.
4. Specify the number of risk levels and the size for each level.
5. (Optional) Select a risk level label, such as **Low** or **High**, and type the desired value to customize the label.

When you set risk values on objects and policies, Identity Governance displays these risk level names so you can easily see whether an object has a risk score associated with it and the risk level label as defined in your environment.

22.3 Configuring Risk Scores

You can customize the way Identity Governance summarizes the risk in your environment, either through manual or calculated risk scores. Governance risk score measures risk across your entire system, application risk score measures risk for each application, and user risk score measures the risk for each user. You can assign risk scores manually by editing values in the catalog, either individually or through bulk data updates. If you edit extended attribute risk values that had been collected, Identity Governance uses the edited values for extended attributes for risk calculation instead of the collected values. For more information, see Section 12.3, “Editing Attribute Values of Objects in the Catalog,” on page 127.

To have Identity Governance calculate risk scores for your environment, you select which factors contribute to risk calculation, configure how much weight each risk factor carries in calculations, and then direct Identity Governance to start the calculation process by clicking **Calculate**. Some risk factors that you can select, such as Certification policies, require that you actually have the factor configured for your environment to have Identity Governance use that factor in the risk score calculation. For more information, see “Creating and Editing Certification Policies” on page 365.

To configure risk scoring:

1. Log in as a Customer, Global, or Data Administrator.
2. Under **Policy**, select **Risk**.
3. Click the gear icon on a risk score badge to customize it.
4. For the governance risk score, you must assign weights and risk factor ranges to enable Identity Governance to calculate risk.

   NOTE: The governance risk score depends on application and user risk scores.

5. For applications and users, in **Risk scoring**, select **Calculated** to show the risk factors and weights.

   NOTE: The application risk score depends on user risk score.

6. For each risk factor that you want to use, specify the weight for that risk factor and customize the range values you want to use. When setting a range, any value below the low range will have zero risk set. Any value above the high range will have the maximum risk value set. For more information, see “Risk Factors” on page 287.
7. Continue assigning weight values to risk factors until your risk factor weights add up to your desired amount.
8. Select **Save** and then select **Calculate**.

   Identity Governance shows status when calculation is in progress and completed.
9. View calculated risk scores in the appropriate catalog section, such as users or applications, or on the Governance Overview dashboard for the Governance risk score. In the catalog, individual items have a **Risk Factors** tab, if applicable, that shows the calculated risk score details, such as risk score, last calculated date, and risk factors used in the calculation.

22.4 Setting and Viewing Risk Calculation Schedules and Status

You can set a regular schedule for Identity Governance to calculate risk scores in your environment.

1. Log in as a Customer, Global, or Data Administrator.
2. Under **Policy**, select **Risk**.
3. Expand **Risk Score Schedule**.
4. (Optional) View status of recent risk score calculations. Each risk score section also contains the calculation status for that section.
5. Select **Active** and then set the details for Identity Governance to calculate risk in your environment, such as start and end date and time details and whether to repeat on a regular schedule.

22.5 Viewing Calculated Risk Scores

After you configure Identity Governance to calculate risk scores, you can view risk scores of items in the catalog and your overall governance risk score on the Governance Overview dashboard.

1. Log in as a Customer, Global, or Data Administrator.
2. (Conditional) If you have configured Identity Governance to calculate the Governance risk score, view the Governance risk score for your organization on the Risk tab of the Governance Overview dashboard.
3. (Optional) Select the score to display the risk factors and other details of how Identity Governance calculated this score.
4. (Optional) Select **Edit** to change the factors of this calculation.
5. Under **Catalog** select **Users** or **Applications** and select a user or application to see the user's or application's risk score displayed on the right side of the window.
6. Select **Risk Factors** to display the configured details for how Identity Governance calculated the risk score, along with the raw and weighted scores calculated for each risk factor.

   Base Score

   The score for a risk factor based on the configured type, such as average or specified range. For example, if the administrator has configured that the **Risk of permissions assigned to user** be averaged, Identity Governance averages the permission risk values for each user in the catalog and reports this number as the base (raw) score.

   Weighted Score

   The calculated score for a risk factor based on the configured weight for that risk factor. For example, if the administrator has configured that the average value of **Risk of permissions assigned to user** be 50% of the total risk score for each user, Identity Governance takes 50% of the base score and reports this number as the weighted score.

22.6 Exporting and Importing Risk Policies

Once you have configured your risk levels, scores, and schedule, you can also export all the configured policies as a JSON file, edit it if required, and import it into another Identity Governance environment. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

23 Administering Access Request

The Customer, Global, or Access Request Administrator must create policies that govern who can request access and who can approve access requests in your environment. For example, administrators can make access to an application available for anyone in your organization to request. Upon request, the access might be automatically granted based on the requester's business role membership or routed to another person for approval, such as the requester's supervisor or the application owner.

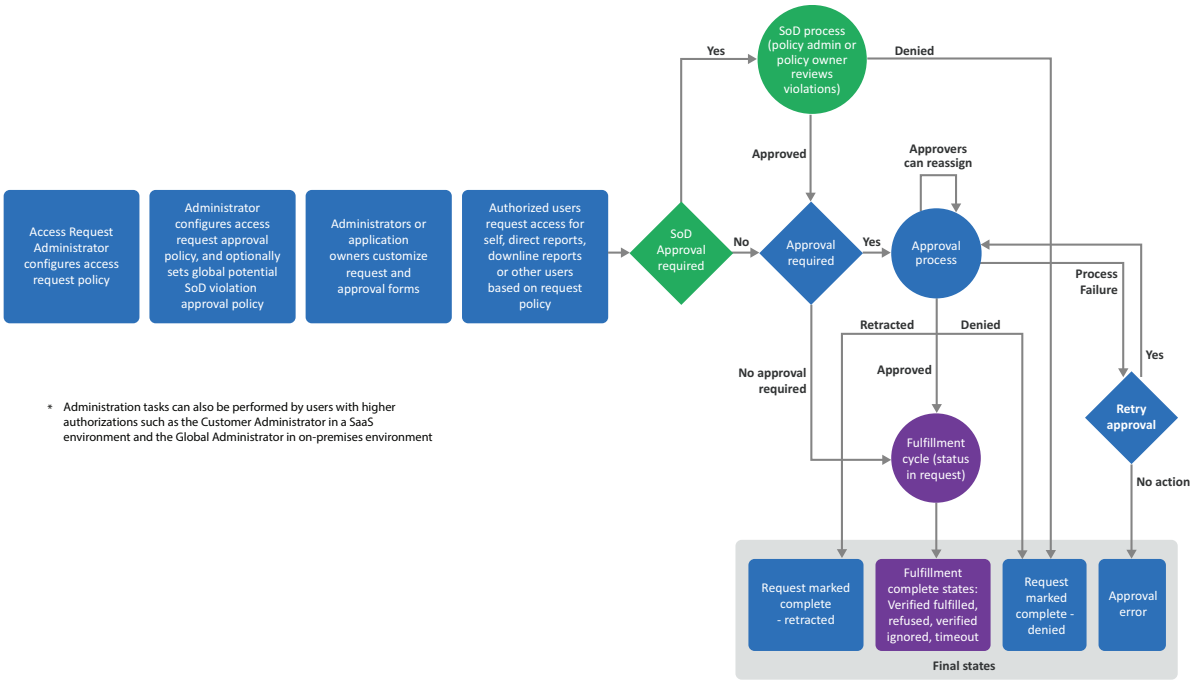
Request policies define which applications, permissions, technical roles, and business roles access can be requested in the Access Request interface. Request approval policies define the approvals needed when users request access.

In addition to creating policies, administrators can also customize the request and approval forms for permissions and applications and simulate the request and approval workflow.

For more information about using the Access Request interface, see Chapter 24, "Instructions for Access Requesters and Approvers," on page 313.

23.1 Understanding Access Request

Figure 23-1 *Access Request Process*



The Access Request capability allows administrators, application owners, supervisors, and other users to perform various tasks based on their authorizations. The Identity Governance users can perform the following tasks based on their runtime authorizations and the request and approval policies:

- Review their current access or the access for other users
- Review access that is recommended for them based on business role policies
- Search or browse and request application access that is available to request
- Search or browse and request technical roles to request a group of permissions in a single step
- Search or browse and request business role membership
- Specify effective (future start) and expiration (future end) dates for requests
- Retract access request
- Retry failed request after fixing the cause of the error
- Compare access of multiple users when authorized by request policy
- Specify workflow as approver
- Edit or create custom workflow for approval
- Approve requests when assigned as an approver in approval policy
- Approve or resolve potential SoD violations when assigned as an approver in SoD violation policy

- View a list of current access requests, status of each request, and a timeline of all related events including fulfillment and reassignment details
- View a list of completed requests and approvals

In addition to the above tasks, users with Access Request Administration authorization can:

- Create, edit, preview changes, compare to draft, simulate workflow, and publish customized request and approval forms for permissions and applications
- Configure default request policy and create additional request policies to specify who can request what
- Create approval policies to specify requests that need approval or that enable requests to be pre-approved or automatically routed for approval

23.2 Configuring Access Request for Identity Governance Users

The method for giving Identity Governance users the ability to request and approve access varies. It requires administrators to configure request and approval forms and policies, and optionally, business roles and technical roles. Find next an overview of the various Access Request activities, configuration methods, and required authorizations.

Access Request Activity	Configuration Method	Configured By
Search **NOTE:** Authorized administrators can enhance search performamce by modifying advanced configuration properties. For more information, see Section 23.3, “Optimizing Access Request Search Performance,” on page 299.	Configure the Default Access Request Policy, or create an access request policy and add items to the policy.	Customer, Global, or Request Administrator
Add items to Browse list	Configure the Default Access Request Policy, or create an access request policy and add items to the policy.	Customer, Global, or Request Administrator
Add items to Recommended items list	Add business roles to a request policy. Note that the Business Role Administrator must have defined business roles for you to add the roles to the Access Request policy.	Customer, Global, or Request Administrator
Specify approval rules for request Items	Set up your approval steps in the approval policy and assign permissions, applications, or roles (technical roles) to that policy either while editing the policy definition or in the catalog using the bulk select menu.	Customer, Global, or Request Administrator

Access Request Activity	Configuration Method	Configured By
Specify coverage map for request approvals	Create coverage map using **Policy > Coverage Maps** menu, and then specify approvers in a request approval policy as coverage map.	Customer, Global, or Request Administrator
Specify Workflow for request approvals	Select a workflow as approver in the approval policy.	Customer, Global, or Request Administrator
Edit or create workflows	After assigning applications and permissions to a approval policy that has workflow as a approver, launch Workflow editor from the associated application or permission Custom Forms tab in the catalog.	Customer, Global, or Request Administrator who is also assigned as the Workflow Administrator
Configure request item text or icons	Edit the permission or application in the catalog.	Customer, Global, or Data Administrator
Create, edit, download, or import custom request and approval form	Create, edit, download, or import the permission or application in the catalog.	Customer, Global, or Request Administrator, or Application Owner
Create, edit, download, or import default application or permission custom request and approval form	Create, edit, download, or import the default permission or application forms in the Access Request Policies area.	Customer, Global, or Request Administrator, or Application Owner
Manage how requests are fulfilled	Identity Governance **Fulfillment > Configuration.**	Customer, Global, or Fulfillment Administrator
Manage who can request on behalf of others	Specify requesters in the Access Request Policy.	Customer, Global, or Request Administrator
Manage email notifications for request approvals	Specify notifications frequency and additional recipients in the approval step of the appropriate Access Request Approval Policy	Customer, Global, or Request Administrator
Allow requesting collections of authorizations	Assign technical roles to a Access Request Policy or add business roles that include technical roles as requesters in the policy.	Customer, Global, or Request Administrator
Control approval decision support information	Similarity profile settings in Identity Governance **Configuration > Role Mining and Analytics Settings**.	Customer, Global, or Request Administrator

23.3 Optimizing Access Request Search Performance

Depending on your data and access request and approval policies, searching for users, groups, or roles might result in too many requestable items and might take considerable time. Authorized administrators can enhance search performance by setting values for the following advanced configuration properties using the Advanced Menu.

- `com.netiq.iac.ui.userpicker.paging.strategy.has.more`

  This property specifies search result paging behavior, and is set to `false` by default. If you change it to `true`, Identity Governance searches for requestable items more quickly.

- `com.netiq.iac.ui.userpicker.paging.strategy.min.search.chars`

  This property configures the number of minimum characters you need to type in the search box before Identity Governance starts searching the catalog. By default, this property is set to `0`, but you can change this to a higher value. The more characters you type in, the less time is needed to narrow the search results.

- `com.netiq.iac.ui.cx.search.preventAutoQuery`

  After you click **Search**, Identity Governance displays all request items, but you can set this property to `true` to prevent Identity Governance from loading all requestable items.

- `com.netiq.iac.ui.cx.search.typeaheadDelay`

  This property controls the time within which Identity Governance queries the database and displays search results. The default `typeahead` value for the property is 500 milliseconds.

23.4 Creating Access Request Policies

To allow users to request access, an administrator must create request policies or edit the default request policy provided by Identity Governance. Request policies define what access can be shown and requested in the Access Request interface. Users with the Customer, Global, or Access Request Administrator authorization can configure a default request policy and additional request policies based on their business needs. The default policy enables users to request all permissions, applications, or roles that are not directly assigned to an access request policy.

- Section 23.4.1, “Configuring Default Access Request Policies,” on page 299
- Section 23.4.2, “Creating Additional Access Request Policies,” on page 300

23.4.1 Configuring Default Access Request Policies

To configure a default access request policy:

1. In Identity Governance, select **Policy > Access Request Policies**.
2. Click **Edit**.
3. (Optional) Edit name and description.
4. Specify which type of request items are included in this policy. For example, when instead of individually assigning permissions to a policy, you want specified users to request all permissions, select the permissions check box.

5 Specify who can request access for whom.

5a To define who all users can request access for by default, click **Add request for** and select an option in the All Users section. For example, if you want all users to be able to request access for themselves, select **Self**. If you want all users to request access for other users who meet a set of criteria, select **Users matching query**, then define the criteria using the Expression Builder.

NOTE: Granting ability to request access for **All Users** automatically provides the user with the ability to request for **Self**, **Direct Reports**, and **Downline Reports**. Granting the ability to request for **Downline Reports** automatically provides the ability to request for **Direct Reports** as well.

5b (Optional) For more granular control of who can request for whom:

5b1 Select allowed users, groups, or business roles, then click **+** to add the users, groups, or business roles.

5b2 For the selected allowed entity, click **Add request for** and select an option. For example, if you added group A in the previous step, then added a request for group A, all members of group A would be able to request access for all other members of the group.

NOTE: If the request policy allowed all users to request access for all users, these settings will be ignored.

5c For exclusions to the All Users settings, specify disallowed users and groups.

5d (Optional) Create additional access request policies.

5e Save the policy.

23.4.2 Creating Additional Access Request Policies

To create additional access request policies:

1 In Identity Governance, select **Policy > Access Request Policies**.

2 On the **Request Policies** tab, scroll down and expand the Request Policies panel.

3 Click **+** to create a new policy.

4 Type name and description.

5 Specify who can request for whom.

6 Save the policy.

7 Assign applications, permissions, technical roles, and business roles to the policy.

IMPORTANT: Only Business Roles that were defined as requestable and published will be available for selection.

---

8 (Optional) Select the gear icon in the **Applications**, **Permissions**, and **Roles** (technical roles) tabs to customize column display. For example, in **Permissions** tab you can drag and drop **Authorized By** column to view if a permission is from an Identity Manager role or application or from an Identity Governance role.

23.5 Creating Request Approval Policies

To require approvals for requested access, an administrator must create request approval policies. Identity Governance provides a default request approval policy. Users with the Customer, Global, or Access Request Administrator authorization can either edit the default policy and configure it for auto-approval based on specific conditions. They can also create new request approval policies to further define the approval policies for various situations.

If there was an auto-approval based on conditions, that auto-approval will show up in the request timeline, and it will show why it was auto-approved. You can configure automatic approval and automatic denial at the policy level and at the approval step level.

Criteria in the conditions are not limited to the recipient. A **request** has a recipient, a resource (such as a permission, technical role, or application), and a requester. The criteria can be any combination of attributes of the recipient, requester, and resource. If the resource is a permission, criteria can also be the application to which the permission belongs. Approval conditions for approval steps can also include attributes of the approvers.

23.5.1 Configuring Default Approval Policy

The out-of-the box default approval policy does not require approval, so requests for permissions, technical roles, and applications associated with the default approval policy are not routed through any approval workflow, but are sent directly to fulfillment. For an approval policy that does not require approval, the request timeline will not show *any* approval as having occurred. It will simply show that the request items were sent directly to fulfillment.

To configure the default request approval policy:

1. In Identity Governance, select **Policy > Access Request**.
2. On the **Approval Policies** tab, click **Edit** to edit the default approval policy.
3. (Optional) Edit the name of the policy.
4. (Optional) Configure automatic approval or denial at the policy level.
5. Add one or more approval steps, depending on how many levels of approval you require. For each approval step:
   - (Optional) Configure automatic approval or denial at the approval step level
   - Specify approvers

   NOTE: You can use self, recipient supervisor, item owners, users, groups, or coverage maps or workflow to specify approvers. For information about coverage maps, see “Using Coverage Maps” on page 28. For information about workflows, see Section 23.8, “Using Workflows to Approve Requests,” on page 309.

- View notification emails, and optionally set reminder email frequency and add recipients
- Set escalation period and specify escalation approvers
- Set expiration period and assign default action at the end of the expiration period

6 {Optional} Drag and drop the default Step 1 Potential SoD Violation Check Approval as needed to specify when Potential SoD violation approval should occur.

7 Add or remove applications, permissions, and technical roles assigned to the policy.

8 Save the policy.

23.5.2 Creating Additional Request Approval Policies

To create additional request approval policies:

1 In Identity Governance, select **Policy > Access Request**.

2 On the **Approval Policies** tab, click **+** to add an Access Request approval policy.

3 Type a name for the policy.

4 (Optional) Configure automatic approval or denial at the policy level.

5 Add one or more approval steps.

6 Save the policy.

7 Assign applications, permissions, and technical roles to the policy.

23.5.3 Configuring Automatic Approval or Denial at the Policy Level

You can configure an access request approval policy at the approval policy level to:

- Automatically approve requests matching specified conditions
- Automatically deny requests matching specified conditions
- Automatically approve requests matching one set of specified conditions while denying requests matching another set of specified conditions
- Automatically approve requests where the resource is authorized to the recipient by one or more business roles

To configure automatic approval and denial at the approval policy level:

1 In Identity Governance, select **Policy > Access Request**.

2 On the **Approval Policies** tab, click **+** to add an Access Request approval policy.

3 Enter a name for the policy.

4 Select one of the following conditions for auto approve, auto deny, or both:

- **None** (Disables the feature)
- **For Grant requests** (Requests to add a permission, a technical role, or an application)
- **For Revoke requests** (Requests to add a permission, a technical role, or an application)
- **For Grant and Revoke requests** (For all requests)

NOTE: Identity Governance applies the condition only to requests of the specified type.

---

5 Use the Expression Builder to specify the conditions for automatic approval or denial. For more information see Section 5.1, “Using the Expression Builder to Create Advanced Filters,” on page 59.

6 Save the policy.

As mentioned earlier, in addition to settings auto approval via conditions, administrators can also set automatic approval for resources that are authorized for the recipient by one or more business roles. Administrators can set this option also either at the policy level or at the approval step level. Identity Governance automatically approves a request if the system submits a request for a user, and a business role authorizes the resource for that user.

If you choose to automatically approve a request by business role at the policy level, the choice is no longer available at the approval step level. Automatic approval by business role configured at the approval policy level ends the process, and does not get routed to the approval step level, so approval by business code at the approval step level is not needed. In addition, if a condition fails the test for approval by business role at the approval policy level, it would also fail at the approval step level, so automatic approval by business role at the approval step level is redundant.

To configure automatic approval by business role at the policy level:

1 In Identity Governance, select **Policy > Access Request**.

2 On the **Approval Policies** tab, click **+** to add an Access Request approval policy.

3 Type a name for the policy.

4 Select one of the following conditions for **Auto approve items authorized by business role**.

- **No** (Disables the feature)
- **For Grant requests** (Requests to add a permission, a technical role, or an application)
- **For Revoke requests** (Requests to remove a permission, a technical role, or an application)
- **For Grant and Revoke requests** (For all requests)

5 Save the policy.

23.5.4 Configuring Automatic Approval at the Approval Step Level

An access approval policy could need additional approval steps if the access is not authorized by company business policies. Configuring automatic approval at the approval step level allows an administrator to configure the approval policy to skip an approval step under specified conditions, but require approval for any subsequent approval steps.

A request approval policy can be configured at the approval step level to:

- Automatically approve requests matching specified conditions
- Automatically approve requests authorized by business roles

To configure automatic approval at the approval step level:

1 In Identity Governance, select **Policy > Access Request**.

2 On the **Approval Policies** tab, click **+** to add an Access Request approval policy.

3 Type a name for the policy.

4 On the **Approvals** tab, click **+**.

5 Click the approval step, then click **Approvers**.

6 Select one of the following for **Auto approve condition**:

- **None** (Disables the feature)
- **For Grant requests** (Requests to add a permission, a technical role, or an application)
- **For Revoke requests** (Requests to remove a permission, a technical role, or an application)
- **For Grant and Revoke requests** (For all requests)

7 Use the Expression Builder to specify the conditions for automatic approval. For more information see Section 5.1, “Using the Expression Builder to Create Advanced Filters,” on page 59.

8 Select an approver.

9 (Optional) Add more approval steps.

10 Save the policy.

To configure automatic approval by business role only at the approval step level:

1 In Identity Governance, select **Policy > Access Request**.

2 On the **Approval Policies** tab, click **+** to add an Access Request approval policy.

3 Type a name for the policy.

4 Do not select **Auto approve items authorized by business role** at the policy level.

NOTE: If you select **Auto approve items authorized by business role** at the policy level, you cannot enable it at the approval step level.

---

5 On the **Approvals** tab, click **+**.

6 Click the approval step, then click **Approvers**.

7 Select one of the following conditions for **Auto approve items authorized by business role**.

- **No** (Disables the feature)
- **For Grant requests** (Requests to add a permission, a technical role, or an application)
- **For Revoke requests** (Requests to remove a permission, a technical role, or an application)
- **For Grant and Revoke requests** (For all requests)

8 Select an approver.

9 (Optional) Add more approval steps.

10 Save the policy.

23.5.5 Assigning and Removing Resources

After you have created request or approval policies, you can assign resources to them, such as applications, permissions, and technical roles. Note that adding application to a policy does not automatically include the application permissions. To request permissions and to require approval for permission requests, you must also assign the permissions to the policy.

If a technical role is referenced by an access request or an approval policy, then Identity Governance will not allow you to delete or deactivate the technical role, unless the technical role is removed by the administrator from the list of all policies that references this technical role and prevents deactivation.

1 In Identity Governance, select **Catalog > Applications**, **Permissions**, or **Roles**.

2 Select the applications, permissions, or roles.

3 In **Actions**, select the option you want. You can:

- Assign access request policy
- Remove access request policy
- Assign approval policy

You can also import assignments, assign resources to a policy, or remove resources from a policy while editing the policy definition.

1 (Conditional) If you have an assignments file that you had chosen to export when exporting a access request policy, click **Import Assignments** in the policy details page to import assignments.

NOTE: If you import more than the preconfigured threshold for assignments, you cannot import assignments using the assignments file and will need to import the policy from the policies list page.

---

2 Alternately, assign resources.

2a Select the **Applications**, **Permissions**, or **Roles** tab.

2b Select **+** under the tab to select resources of the specific type to assign to the policy.

3 (Optional) Specify if a request for a technical role access should be approved at the role level or at the individual permission level.

3a Select one or more technical roles.

3b Select **Actions > Set Role Level Approval** to enable approval of all requests for permissions included in the technical role as a group.

Or

Select **Actions > Set Permission Level Approval** to enable approval of each permission included in the technical role individually.

4 Select the resources to be removed using the check box next to the ones you want to remove.

5 Select **Remove** to remove the selected resources.

NOTE: You cannot remove resources from the default approval policy in this way. A resource can only be removed from the default approval policy by assigning it to another approval policy. Also, removing a resource from a policy other than the default approval policy will re-assign the resource to the default approval policy.

23.6 Understanding the Default SoD Approval Policy

Identity Governance uses Separation of duties (SoD) approval policies to control potential SoD violation approvals and govern the approval process for SoD violations. If you set a default SoD approval policy, it applies to any SoD policy with no SoD approval policy assigned. Identity Governance allows you to view which default SoD approval policy is set by selecting **Policy** > **Access Request Policies** > **Potential SoD Violation Approval**. You can also run an Insight Query to view all your SoD policies and the SoD approval policies assigned to them. If default SoD approval policy is not set, then potential SoD violation approval is not required, and SoD Owners, Global Administrators, and Customer Administrators may resolve or approve SoD violations. To set the default SoD approval policy, coordinate with the Global, Customer, or Separation of Duties administrator. For more information about SoD policies and SoD violations, see "Creating and Managing Separation of Duties Policies" on page 263 and "Managing Separation of Duties Violations" on page 277.

23.7 Creating and Editing Request and Approval Forms

Identity Governance provides default request and approval forms for applications and permissions access. When more complex forms are required, authorized administrators, application owners, or their delegates can also customize the default forms or create customized forms for one or more applications and permissions using Forms Builder and Forms Renderer. **Forms Builder** enables you to design forms; add and validate data; edit JSON forms directly in the application; and seamlessly pass the user and approver submissions to Identity Governance request and fulfillment workflows. **Forms Renderer** uses the form JSON schema to render the forms and generate corresponding APIs.

For a detailed description of Forms Builder and its procedures, see the *Form Builder Guide*.

23.7.1 Customizing Default Application or Permission Forms

Identity Governance provides form sets (request and corresponding approval form) by default. On the Application Default Forms or Permission Default Forms tabs on the Access Request Policies page, you can choose a sample application or permission respectively, and preview forms to review default forms. If you want to customize the default forms, you can use Form Builder to customize them.

IMPORTANT: When you customize a default request form, you also need to add the corresponding controls to the default approval form to facilitate data flow. For example, if you want to add a Supervisor field to the request form, you must also add that field to the default approval form.

To customize default application or permission request and approval forms:

1. Log in to Identity Governance as a Customer, Global, or Request Administrator or an Application Owner.
2. Select **Policy** > **Access Request Policies**
3. Select **Application Default Forms** or **Permission Default Forms**.
4. Click the default request form to launch Form Builder in a new browser tab.
5. Drag and drop form components, configure related settings, and save the form. For Form Builder procedures, see the *Form Builder Guide*.
6. Select the Identity Governance browser tab to return to the policy page.
7. Click the approval form to launch Form Builder.
8. Duplicate the changes you made to the request form and save the form.
9. Select the Identity Governance browser tab to return to the policy page.
10. Publish forms individually or select **Actions > Publish Forms** to publish the request and approval form.
11. Compare the draft to published forms.

    NOTE: Inline scripts in forms are published to the global javascript context. When inline scripts are used as helper functions in the Form Builder, comparisons might be displayed incorrectly. This occurs because two forms are sharing the same inline function.

    ---
12. If needed, make additional changes or revert changes.
13. (Conditional) If you had previously created custom forms for permissions or applications, you can select additional actions such as **Change form set**, **Copy existing form set**, or **Assign form set**. For information about creating form sets, see Section 23.7.2, “Creating Custom Forms for One or More Permissions and Applications,” on page 307
14. (Optional) Select **Actions** and rename forms.

23.7.2 Creating Custom Forms for One or More Permissions and Applications

In addition to customizing the default forms, you can further customize forms for specific permissions or applications. As stated earlier, *when you customize the request form, you also need to add the corresponding controls to the approval form to facilitate data flow*. For example, when you add Select Box and Reason components to your Custom Request Form for laptop permission, you also need to add them to the Custom Approval Form so that the user selection and reason is passed to the approval form.

To create a custom request and approval form:

1. Log in to Identity Governance as a Customer, Global, or Request Administrator, or an Application Owner.
2. Select **Catalog > Applications > *Application Name*** or select **Catalog > Permissions > *Permission Name***.

3 Create a new custom request and approval form:

3a Select **Actions > Add form set**.

3b Click **Create Form Set**.

3c Click the request form to launch Form Builder in a new browser tab.

3d Drag and drop form components, configure related settings, and save the form. For Form Builder procedures, see the *Form Builder Guide*.

3e Click the approval form to launch Form Builder.

3f Duplicate the changes you made to the request form and save the form.

4 Select the Identity Governance browser tab to return to the catalog page.

5 (Conditional) If you had previously created a custom form set, change, assign, or copy an existing custom form to another permission or application:

5a In an application's Custom Forms tab, select **Actions > Copy existing form set** or **Actions > Assign form set**.

5b In a permission's Custom Forms tab, select **Actions > Change form set**.

5c Select a form set from the list of custom form sets, rename the form set and forms' names, and create the new forms.

6 Select **Actions > Publish Forms** to publish the request and approval form.

7 Compare the draft to published forms.

8 (Optional) Rename a custom form or a custom form set by selecting **Actions > Rename form** or **Actions > Rename Form Set** respectively.

NOTE: If needed, you can always revert to the default forms or default form set by selecting **Actions > Revert to default form** or **Actions > Revert form set to default** respectively.

23.7.3 Editing Custom Form Components and Forms

In addition to the ability to create custom forms using basic, advanced, and custom Form Builder components, you can also edit each form component and edit the form itself using JSON and JS (JavaScript) editors. For example, you can use the editors to construct instructions for fulfillment for laptop permission by adding JSON objects such as `flowdata`, which contains request data.

IMPORTANT: The JSON editor is meant for use by developers and advanced users to customize forms. Do *not* use it if you do not have JSON experience.

For more information about editing form components and using the editors, see the *Form Builder Guide*.

23.7.4 Downloading and Importing Forms

Identity Governance enables you to download and import the request and approval forms for use in other environments. You can download and import:

- Default forms for all applications
- Default forms for all permissions

- Custom forms for a specific application
- Custom forms for a specific permission

For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

23.8 Using Workflows to Approve Requests

When additional logic is required to approve a request, Identity Governance enables you to use workflows that supplement your out-of-the-box approval processes. Use the provided workflow templates as a starting point to include essential elements and activities for your workflow. The workflow associated with the policy will be activated when one or more resources are assigned to the associated access approval policy. You can debug these workflows and simulate a request workflow. Based on your authorization, you can also create or edit a workflow using Workflow Administration Console.

TIP: We recommend that you use the Identity Governance workflows provided to you. Create a new workflow only when you need a custom workflow beyond the provided approval flows. Proceed with caution when making any changes to the provided workflows. Each workflow template includes multiple activities that references a form on the catalog view of Workflow Administration Console. Multiple workflows might share the same workflow form. This means if you change the form content, all workflows using that form will be affected. If you do not want this, make a copy of the form and change your workflow to use the form copy before editing your form content. When changing the form reference within the workflow editor (also known as Workflow Builder), copy the data item mappings within the Workflow Builder. Use the workflow catalog to tell you which workflows are referencing any particular form.

To assign a workflow as an approver and to create and edit a workflow for approvals:

1. Log in to Identity Governance as a Customer, Global, or Request Administrator who also has Workflow Administrator authorization.
2. In Identity Governance, select **Policy > Access Request**.
3. On the **Approval Policies** tab, add a new policy or edit an existing policy.
4. When adding or editing approval steps, specify the approver as **Workflow**.
5. Use * or enter the workflow name to search for a workflow.
6. (Conditional) If a workflow does not exist, create a sample approval workflow.
   - **6a** Click **Create Sample Approval Workflow**.
   - **6b** Enter an identifier and name. Note that special characters and spaces are not allowed in the identifier field.
   - **6c** Select a template.
7. (Optional) Click **Edit** and customize the template as needed in Workflow Administration Console but do *not* change the default form in the Start Activity pane.

IMPORTANT: To ensure that proper integration happens between Identity Governance and your custom approval workflow process, you must use the default IGA approval request form in Workflow Administration Console. Using any other form for your approval workflow activity might result in unpredictable behavior because Identity Governance requires `entityType`, `entityId`, `igApprovalFlowdata`, `reason`, and `isAdd` fields.

As mentioned earlier, proceed with caution when editing workflows. For additional information about creating and editing workflows, see the "Using Workflow Builder to Create Workflows" chapter in the *Workflow Administration Guide*. For additional information about exporting and importing workflows, see the "Exporting and Importing Workflows" section in the *Workflow Administration Guide*.

8 Save the policy.

9 Assign resources to the policy.

10 Access the assigned resource to debug the workflow and to customize the workflow as needed.

10a Select the name of a assigned application or permission.

10b Select the Custom Forms tab.

10c (Optional) Click the workflow identifier to launch the workflow in the Workflow Administration Console.

10d On the Select **Debug** to debug the workflow in the Identity Governance catalog view without impacting your production data.

10e Simulate request workflow to view the workflow debug status.

NOTE: The approval form displayed on the Custom Forms tab when running the simulator is different from the workflow IGA approval request form. The request approval form on the Custom Forms tab on the Identity Governance catalog page is a specialized Identity Governance defined form used for approvals when the approver type is **Self**, **Supervisor**, **Item owners**, **Coverage maps**, or **Select users or groups**.

23.9 Downloading and Importing Access Request and Approval Policies

Once you have configured your request and approval policies, you can download all the configured policies as a zip file containing multiple JSON files and the policy list as a CSV file to back up your policies or to import the exported definition files into an Identity Governance environment. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, "Exporting and Importing," on page 387.

23.10 Disabling the Access Request Service

You can prevent displaying the Access Request pages in Identity Governance by disabling the Access Request service. When you disable the service:

- All Access Request options are removed from navigation
- Users with no rights in Identity Governance will not be redirected to Access Request

- All REST API calls for access request will return errors
- Users directly accessing the Access Request interface will see the following error message after login: `Access request services are disabled. Contact your system administrator.`

NOTE: This setting does not affect request and approval polices. Users still will be able to administer and view policies.

To disable the Access Request service:

1. Start the Identity Governance Configuration Utility in console mode.
   - **Linux:** Default location of `/opt/netiq/idm/apps/idgov/bin`, then enter `./configutil -console -password` *`database_password`*
   - **Windows:** Default location of `c:\netiq\idm\apps\idgov\bin`, then enter `configutil -console -password` *`database_password`*
2. Disable the Access Request service:

   ```
   config> add-property GLOBAL com.netiq.iac.access.request.enabled false
   ```
3. Exit the console and restart tomcat.

24 Instructions for Access Requesters and Approvers

Access Request allows you to request access and access removal for the following types of items:

- Applications
- Permissions
- Technical roles
- Business roles

Application access request enables you to request login privileges to that application. Permission access request enables you to request rights within an application. Technical role access request enables you to request rights to a group of permissions based on the requested technical role definition and assigns you the technical role. Business role access request enables you to request membership in a business role and grants you the related authorizations.

Identity Governance administrators define the policies that govern who can request access, what they can request for, for whom they can request for, and any required approvals. Approvers are notified by email of pending requests according to the approval policies, which allow you to configure the frequency of these notifications. Access Request approval policies may also designate CC and BCC email recipients, as well as an escalation policy in case the approver does not act in a timely fashion.

This section provides instructions for individuals using the Identity Governance Request interface to request or approve access for themselves or others.

24.1 Reviewing Current Access and Requesting Access Removal

Current Access lists your permissions, technical role, and business role assignments. If you have permission to view access for others, you can change to another user to see that user’s access items. Additionally, you might also be allowed to remove access items for yourself and others.

1. In the Access Request interface, select **Current Access**.
2. Review your permissions, technical roles, and business roles. Dynamic resources appear as a link that you can select to show additional information on assignment details.

3 (Optional) Click the permission, technical role, or business role to view more information.

4 (Conditional) If you have permission to view other users, click your name under Current Access and change to the other user to review that user's permissions, technical role, and business role assignments. Optionally, click Settings icon on the User Selection window to select user attributes that will be visble on the window, then search using an attribute value to narrow the list of users.

NOTE: The current list of access items is always for the user listed under Current Access.

---

5 (Optional) Remove access, type a reason, then select **Add removal request to cart**.

If there is no **X** next to an item, that item is not removable.

NOTE: When you remove technical role access, Identity Governance removes the technical role assignment and issues requests to remove the permissions of the role held by the user.

When you remove business role access for a user who was assigned to a business role via access request assignment, Identity Governance removes the assignment. When you remove business role access for a user who meets the business role membership criteria, Identity Governance creates a fulfillment request for a business role administrator to modify the business role definition or change the user attributes so it no longer meets the membership criteria.

---

6 (Conditional) If you have any items in the shopping cart, select the shopping cart, then click **Submit**.

NOTE: Selecting **X** next to a request in the shopping cart immediately removes the request from the cart, but the request is not automatically submitted. You must submit the request for Identity Governance to process the request.

24.2 Requesting Access

Identity Governance request policies determine who can request access and what items they can request. Permissions, technical roles, and business roles already assigned to you will not be available for request and can be viewed on your Current Access page. If the request policy authorizes you to request an application, the application will be available to request even if you have the application account or permission.

Identity Governance supports time-based requests. Requesters can specify an effective date and an expiration date for each request. You can view the effective and expiration dates on the Requests page that displays list of all pending and completed requests. When expiration date is specified, Identity Governance will generate additional expire requests that will be effective on the expiration date. Users can change the expiration date or remove expiration request as needed when viewing list of requests that have been submitted.

When authorized to request by a request policy, you can request an application, application permission, technical role, and business role access for yourself or a user for whom you are authorized to request access. Technical roles enable you to request multiple permissions in a single step. When requesting access, you can search or browse for request items, or select recommended items.

To request applications, permissions, or technical role assignments or business role membership:

1 Select the request method.

To	Do this
Search request items by name, categories, applications, request status, request item type, or advanced filters	◆ Select **Request > Search**. ◆ (Optional) Sort items by clicking on column names. ◆ (Optional) Group items by application or category. ◆ Type partial or complete request item name in search bar, and select additional criteria as needed to narrow your results. For example, to search all permissions for a specific category, select a category from categories drop-down list, click **More filters**, then select permissions as the item type. To select request items in more than one category, click **Category**, then use typeahead search to find and select categories. **NOTE:** Authorized administrators can further enhance search performamce. For typeahead search delay, requestable items display, and other configuration properties that can optimize search performance, see Section 23.3, "Optimizing Access Request Search Performance," on page 299.
Browse request items in table or tile view and search request items by name or description	◆ Select **Request > Browse**. ◆ (Optional) Select ***Your Name*** **> My Settings > Enable tile view** to view the Application, Technical Roles, and Business Roles as tiles and use the same settings to switch back to the default table view. ◆ Click on respective tabs to view applications, technical roles, and business roles. ◆ Click an application name to view and search permissions.

To	Do this
Select recommended request items	Select **Request > Recommended**. **NOTE:** You *might* see recommended items to request only if Identity Governance administrators have created and assigned business roles in your environment. Assigned technical roles and requestable businness roles will not be included in the recommended list.

When you review permissions available to request, items might have the following icons signifying the state of the item.

Shopping cart

Item was requested and is in the shopping cart, but the request has not yet been submitted.

Lock

Requested item needs approval.

Clock

Item was requested and is awaiting fulfillment or approval.

Check mark

User already owns the item.

2 Select a item you want to request and add a reason.

3 (Conditional) If Identity Governance warns you of SoD violations, either change your request to resolve the violation or submit the request with the violations for an SoD administrator, SoD policy owner, or SoD or Access Request policy to approve or resolve the violation.

4 (Conditional) If requesting dynamic resources, a specific type of permissions or permissions with custom forms, provide additional inputs. For example, if the dynamic resource is a phone, you might have to select a phone model.

5 (Conditional) When requesting a permission for a user who has multiple accounts, select an account to which the permission should be associated.

6 (Conditional) When requesting a technical role that includes one or more permissions belonging to one or more applications where the recipient user has multiple accounts, select an account for each application to which the permission should be associated.

7 (Optional) Add effective and expiration dates.

NOTE:

- When you specify an expiration date for the access item, Identity Governance will create related pending expiration request items that will become effective on the expiration date. The expiration request is created only *after* all approvals have been given for the request item. If a request item is denied during the approval process, expiration request will not be created.
- While specifying the effective and expiration dates, use the left or right arrow on the calendar date picker to select previous or next month.

8 Click **Add to request**.

9 Repeat above steps as needed to add more items to your cart.

NOTE: When you request access to a technical role, Identity Governance will generate requests for the missing permissions of the technical role and also assign the technical role to the user. The badges that display the technical roles will display a check mark icon if the technical role is already assigned and a warning icon if the technical role is assigned to the user, but the user is missing one or more permissions of the technical role.

A warning is displayed on the request panel when requesting access to a business role for a user specifically excluded from membership. The role can be requested, however membership will not be granted until the exclusion is removed.

10 (Conditional) If you have rights to request on behalf of others:

10a Select the current user to change it to the user for whom you are making the request. Optionally, click Settings icon on the User Selection window to select user attributes that will be visble on the window, then search using an attribute value to narrow the list of users.

10b Select items and click **Add to request**. Repeat this to add more items.

10c (Optional) Select a different user to review and request items for that user.

11 After you have requested items for all users, select the cart to review your choices.

NOTE: Selecting **X** next to a request in the shopping cart immediately removes the request from the cart.

12 Click **Submit** to submit your requests.

If one or more requested items in the cart create a combination of permissions for the user that are considered toxic (strictly forbidden), Identity Governance prevents you from submitting the cart until you remove one or more items from the request to resolve the toxic combination. Click the red caution symbol next to the permissions identified as toxic to learn more about the toxic SoD policy violated, and to help determine which permission(s) to remove from the request. For more information, see "Understanding Separation of Duties" on page 263.

24.3 Monitoring, Retracting, or Retrying Your Requests

Identity Governance enables you to search, view, sort, and refresh a list of your current and completed access requests. You can also retract or retry a failed request. The status column displays details of the request, approval, and fulfillment events.

24.3.1 Monitoring Requests

NOTE: Select the **Refresh** icon next to **My Requests** to refresh the status. Do not refresh the browser because it might lead to an error condition or require you to log in again. Additional administrator actions might also be required for the status to be updated.

To view a list of your requests, their status, and timeline:

1 Select **Requests > Requests**.

TIP: Requests that violate SoD policies have a warning icon next to the request name. Click the icon to view violated SoD policies.

---

2 Select the calendar icon to specify a date range for your search.

3 (Optional) Sort request items using accounts or item ID.

4 (Optional) Search for specific request items using typeahead search or advanced filters.

5 (Optional) Use page control (if shown) to page through all requests.

6 Select a request item status to view the timeline of underlying events associated with the request, including approver reassignments, approver feedback to requester, and fulfillment information.

Identity Governance updates the request fulfillment status when fulfillers fulfill a request, and when the application or a Customer, Global, or Data Administrator collects and publishes the application data source. For example, after a request is manually fulfilled, the fulfilled waiting verification status on the request timeline will change to verified only after a collection and publication.

7 (Optional) For expire request items, change the expiration date.

Expiration date also gets approved when a request is approved. Changing the expiration date will ultimately cause a new expiration request to be submitted that will then go through the same approval process as the original request.

8 (Optional) For expire request items, remove expiration.

Removing (retracting) an expiration request effectively cancels the expiration of the original request, and no approval process is possible. Hence, only Access Request, Customer, or Global Administrator are authorized to remove an expiration request.

9 (Optional) Click **Show completed requests** and specify a date range to view historical requests.

You can view only historical requests that are still in your operational catalog and have not been purged. The time period of items in the operational catalog depends on your company's data retention policies.

10 (Conditional) If you have the authorization to view other users' request, click **View all requests** at the top corner of the page to view all the requests.

24.3.2 Retracting Access Requests

When you might need to retract an access request that has not been fulfilled, you can revoke it directly in the application. A retracted request item moves from a tentatively retracted state to a completed retracted state.

NOTE: You can revoke a request only for a request item that is either in an approval pending or failed state. After fulfillment, use procedures in "Requesting Access" on page 314 to remove or add access.

---

1 In the Access Request interface, select **Request > My Requests**.

2 (Conditional) If the **Status** of a request item is Approval Pending or Approval Failed, click **Retract**.

Occasionally, when you retract a request with a pending workflow approval task, the Workflow Approvals page might not immediately remove the pending approval task. The delay occurs because the scheduler responsible for deleting the data runs as per the interval specified in the Pending Process Interval field on the Workflow Administration ConsoleEngine and Cluster configuration page. For more information, see Configuring Workflow Engine and Cluster Settings.

24.3.3 Retrying Failed Access Requests

Occasionally, access requests can fail. For example, if OSP is configured for HTTPS, but the server where the request workflow is running does not have the proper certificate in the cert store to be able to communicate with, the request will fail. After you have fixed the issue, you can retry the failed request item.

1. In the Access Request interface, select **Request > My Requests**.
2. Check the error message for information about the request item with Approval Failed status.
3. Fix the issue or contact your system administrator to fix the issue.
4. After the issue is fixed, click **Retry**.

24.4 Approving Access Requests and Monitoring Approvals

If the Access Request policy specifies you as an approver for requests, you might have to approve requested items. Your Access Request administrators define these policies and specify items as needing further approval. You can reassign your tasks and view reassignment details.

Approval for technical role requests will display a single approval for the role if the Access Request Approval policy is configured for role level approval. Approving a role with role level approval, approves all permission requests associated with the role. If the approval policy is configured for permission level approval, approval requests will be generated for each permission the user does not hold. Those permissions will need to be approved individually.

Some administrators require business role members, a person's supervisor, or an application owner to approve requested items, and some items might require multiple approvers. In these situations, you must approve items before the next designated approver receives them.

1. In the Request interface, select **Approvals** and then select the type of approvals available to you based on your authorization.

   NOTE: Approvals and SoD approvals tasks are tasks that were generated based on requests made by users and processes of your Identity Governance system. Approvals also include Workflow approvals tasks that are generated when a approval request policy assigns workflow created using the Workflow service as an approver.

   ---

2. (Optional) Search for specific request items using typeahead search or advanced search filters using the expression builder.
3. (Optional) In the title bar, select ***Your Name*** **> My Settings > Enable tile view** to view the Application and Technical Roles as tiles.

NOTE: Once you enable the tile view, you can switch from table to tile view on both request and approval pages.

4 (Optional) Select **Reassign** to delegate an approval task.

5 (Optional) Select **View reassignments** to view reassignment status of the current task.

6 (Optional) In the title bar, select ***Your Name*** **> My Settings > Delegate Mappings** to delegate all your approval tasks.

7 To approve or deny all items within an approval request:

7a Expand the request and review details such as permission type, application, and request reason.

7b Select all items included in the specific approval request.

7c Select **Actions** and approve or deny requests to make a decision without providing additional information. Or approve or deny with additional information such as fulfillment instructions.

NOTE: Some approval forms for specific resources might have required parameters. In those cases, the only bulk option for that resource will be the approve or deny with info options because you are required to provide a value. When there is a required field, clicking the approve or deny buttons on the right hand side will also open up the approval form.

8 To approve or deny requested items individually:

8a Select a requested item and review the details about the request, including information that might be helpful in making a decision.

NOTE: By default, Identity Governance enables decision support information such as application name, permission type, risk, and business role authorization status. If you do not use business roles, and if you are also an administrator, you can disable the business role authorization status display by deselecting the **Administration > Analytics and Role Mining Settings > Show business role authorization status** option.

8b (Optional) Provide fulfillment instructions or feedback to the requester. These instructions are mainly used for manual fulfillment.

8c Select **Approve** or **Deny** for each requested item.

9 Select **Submit items**.

10 (Conditional) If you have the authorization to view other users' approval tasks, click **View all approvals** at the top corner of the page to view all the approval requests.

24.5 Approving Potential SoD Violations

Only users with Customer, Global, or SoD administrator authorization, or users assigned as SoD policy owners can approve or deny potential SoD violations. Administrators can view all approval violations by clicking **View all SoD approvals**. Note that administrators cannot approve or deny permissions that a user already has as part of a business role. Identity Governance prevents approval of potential toxic SoD policy violations. For more information see Section 20.5.2, "Creating an SoD Approval Policy for Toxic SoD Violations," on page 271 and Chapter 21, "Managing Separation of Duties Violations," on page 277.

NOTE: By default, all approval policies include potential SoD violation check and approval as step one of the approval steps. Users cannot delete this step. However, authorized users can drag and drop this step as needed to change the sequence of the approval steps.

24.6 Comparing Access of Multiple Users

If you have permission to see and request items for others, you can also show multiple users with their permissions listed to compare their access. When you are comparing a user to other users, you can request items for the first user in the list, making it easy to ensure that users in the same job role have the same access.

1. In the Access Request interface, select **Compare**.
2. Under **User Access Comparison**, select the user whose access you want to compare with others.
3. Select the permissions tab or the technical roles tab to compare permissions or technical role assignments.
4. Select **Compare to** for a list of users to compare with the first user.
5. (Optional) To continue adding to the table, select **Compare to** and choose additional users.

   As you add users to compare with the first user, Identity Governance adds permissions or technical roles in the first column to reflect the listed users' permissions or technical roles, adds check marks in the appropriate columns to show that a user owns a permission or technical role, and includes a link to add or remove permission or technical role for the first column for any permission or technical role you are allowed to change for that user.
6. (Optional) Select **Add** or **Remove** to change the permissions or technical roles for the first user in the table, enter a reason, and select **Add to request** or **Add removal request to cart**.

   NOTE: Dynamic resources might require additional input. For example, if the dynamic resource is a phone, you might have to select a phone model.
7. (Conditional) If you added access or removal requests to your cart, select the cart and submit the requests.

   NOTE: Selecting **X** next to a request in the shopping cart immediately removes the request from the cart, but does not submit the request.

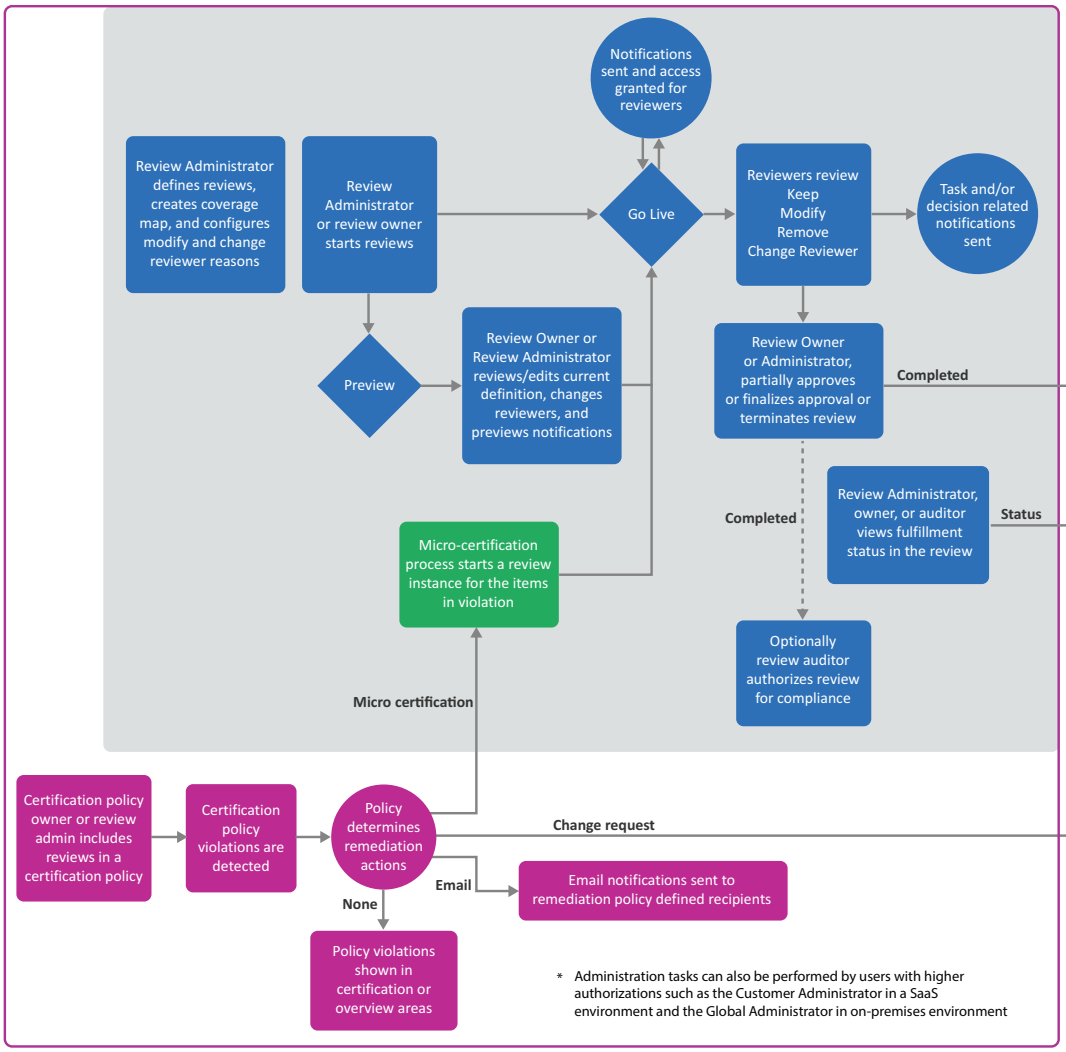
25 Understanding the Review Process

In Identity Governance, reviews are performed to verify details such as a user's level of access, permissions, reporting relationships. Review Administrators create **review definitions** for a particular set of users, accounts, or roles that need review. A single instance of a review definition is a **review run** or review campaign, which has a Review Owner. Once the Review Owner initiates a review run, Identity Governance assigns tasks for the assigned reviewers. Reviewers review their assigned set of review items and decide whether the items should be kept, modified, or removed. The tasks move to the Review Owners queue who approves the changes.

The following figure shows the review process flow:

25.1 Understanding the Process Flow

Figure 25-1 *Review Process*



Reviews provide a way to monitor access to your business systems. Many users take part in the overall review process:

- Review Administrators create review definitions, preview review definitions, and manage reviews.
- (Optional) Review Administrators can request Data Administrators to configure additional selection criteria such as custom identity, permissions, permission assignment, or business role attributes for selecting review items and refine review definitions.
- Review owners start, preview, monitor, complete, and terminate reviews.
- Reviewers, such as supervisors and application owners, act on review items.
- Escalation reviewers review items in the exception queue
- Fulfillers manage change requests.

- Auditors accept or reject completed reviews.
- Review or Data Administrators create certification policies to check for violations and set remediation action which triggers remediations including micro certifications (focused reviews)

For more information about Identity Governance authorizations, see Chapter 2, “Adding Identity Governance Users and Assigning Authorizations,” on page 19.

NOTE: The Identity Governance server needs a 30-minute gap between runs of the same review. For example, you terminate a scheduled review that is in progress. To schedule that review to run again, allow at least 30 minutes to lapse after terminating the previous run. Otherwise, the second run fails to start and Identity Governance does not notify you of the failure.

25.1.1 Viewing the Catalog

Before creating or editing review definitions, reviewing the data in the catalog will help determine who needs to be included in the reviews and which items should be reviewed. Some examples of the information a Review Administrator, Customer Administrator, or Global Administrator can look for are:

- Attributes of the user that may not be available in the **Quick Info** (view of an item, such as a user or a role, when you click on it) to help determine whether the person should be included in a review or not
- The last review date of an account

  NOTE: This date reflects the date when an account was last reviewed as part of an **Account Review**. Review of a user's access to an account as part of a **User Access Review** does not impact this date.

- Risk levels of users or permissions
- Association with an application
- Group, business role, or technical role membership
- Certification status of a user, specifically the date the user was last certified, and details of last review decisions and certification policy violations

25.1.2 Understanding Review Definitions

You can run a review once or multiple times either by starting the review manually or by scheduling it to start at the specified time or interval. Each review is based on a **review definition** that is based on a specific type of **review object** and defines all parameters for that particular review. Review Administrators, Customer Administrators, or Global Administrators create review definitions using the provided default review definitions with preselected criteria. These definitions enable you to select what you want to review. For example, you can select review objects such as User profiles, Technical role assigned to users, Accounts and their permissions, or Business roles assigned to users. These review objects are specific to a **review type** (review template). Each review type provides selection criteria that help Review Administrators to focus their reviews based on varying combinations of identity, application, account, permission, permission assignment, or business role attributes. For example, you can focus the User profiles review by specifying that reviewers should review users with risk greater than 80. Identity Governance provides a default list of attributes for selection when creating review definitions. Review Administrators can request Customer, Global or Data Administrators to add other attributes as selection criteria. Items that do not meet the specified criteria in a review definition are filtered out of the review.

Review definitions also assign reviewers based on their relationship to the review items. Often, administrators use review definitions to split up responsibility for reviewing items to prevent bottlenecks and overloading reviewers. Review definitions can also be referenced in certification policies to enable a comprehensive view of your organization's compliance with specific certification controls such as Sarbanes-Oxley Act (SOX) or Health Insurance Portability and Accountability Act (HIPAA).

TIP: For information about certification policies, see Chapter 30, “Creating and Managing Certification Policies,” on page 365. Once a review definition is referenced in an active certification policy, it cannot be deleted. For detailed procedures about creating review definitions, see Section 26.1, “Creating a Review Definition,” on page 343

25.1.3 Understanding Default Selection Criteria

For Review Object:	For Review type:	Specify review items by:
Permissions assigned to accounts	Account Access Review	◆ Accounts ◆ Permissions ◆ Users ◆ Applications **NOTE:** *Specifying identities or applications first* will enable Identity Governance to determine if users mapped to accounts or custodians of accounts will be reviewed. For more information, see Section 25.1.5, “Expanding and Restricting Review Items,” on page 329.
◆ Accounts ◆ Accounts and their permissions **NOTE:** Permissions are grouped by accounts in this type of review. ◆ Accounts, unmapped only	Account Review	◆ Accounts ◆ Permissions ◆ Users ◆ Applications **NOTE:** *Specifying identities or applications first* will enable Identity Governance to determine if users mapped to accounts or custodians of accounts will be reviewed. For more information, see Section 25.1.5, “Expanding and Restricting Review Items,” on page 329.

For Review Object:	For Review type:	Specify review items by:
Business role definitions	Business Role Definition Review	◆ Business roles You can choose to review membership and authorizations for the specified business roles. ◆ Business role attributes Administrators with Data Administration authorization must have selected **Allow to be reviewed** for an attribute in the **Data Administration > Business Role Attributes** page to be available in the review definition page as an option.
User direct reports	Direct Reports Review	Users
Business roles assigned to users	Business Role Membership Review	Business roles
Business role authorization	Business Role Authorization Review	Business roles
Technical role definitions	Technical Role Definition Review	◆ Roles You can choose to review permissions for the specified technical roles. ◆ Technical role attributes
Global authorizations	Global Authorization Assignment Review	Global authorizations **NOTE:** It is always important to carefully consider the implications when removing any authorization and ensure that the action aligns with your policies.
◆ Permissions and accounts assigned to users ◆ Permissions assigned to users ◆ Technical roles assigned to users ◆ Technical roles detected on users ◆ Users' permissions, accounts and assigned roles ◆ Users' permissions, accounts and detected roles	User Access Review	◆ Accounts ◆ Permissions ◆ Users ◆ Applications ◆ Roles (Technical roles) **NOTE:** Optionally, you can further expand or restrict your review items to include items that have been authorized by a business role. For more information, see Section 25.1.5, “Expanding and Restricting Review Items,” on page 329.

For Review Object:	For Review type:	Specify review items by:
User profiles	User Profile Review	◆ Users ◆ User attributes Attribute selection is required for this review type. You can only select attributes such as title, department, and job code that have been previously selected as **Allow to be reviewed** in **Data Administration > Identity Attributes** by an administrator with Data, Customer, or Global Administrator authorization.

25.1.4 Adding Selection Criteria for Review Items

In addition to the default selection criteria, Identity Governance provides the ability to enable other attributes including custom attributes as selection criteria. In the attribute definition editor of the catalog, an administrator with Data, Customer, or Global Administrator authorization can specify whether an attribute can be used as a review criteria by selecting an attribute in the **Data Administration > *Attributes*** pages and specifying **Display in review item selection criteria**. For example, in the Identity Attributes page, a Data Administrator can enable Job Code as selection criteria and then a Review Administrator can create a review of users based on Job Code value. In the Permission Assignments page, a Data Administrator can enable Assignment Type and then a Review Administrator can create a review of permissions based on assignment type.

TIP: When you specify a boolean attribute in your review criteria and there are null attribute/column values in the database these records will be ignored. Customer, Global, or Data Administrators will need to ensure that there are no null values if you intend to use the attribute as review criteria or add transformation code to convert a null to be true or false or use bulk data update settings to change the null values to true or false. For more information see, "Editing Attribute Values in Bulk" on page 130.

25.1.5 Expanding and Restricting Review Items

In addition to preselected options for specifying review items and additional options based on your review type, you can modify the preselected options and expand or restrict items being reviewed in a User Access Review, an Account Review, or an Account Access Review. The following table provides a few examples of available options and special conditions if any.

If you want to...	Select
Restricts review items to users as account custodians or mapped accounts	Users first, select type of accounts, and specify if the selected users are mapped users or account custodians. **NOTE:** The ability to indicate if the selected users are mapped users or account custodians will be available only if you select users first and then accounts.
Restrict review items to items that were not authorized by a business role or to items that were authorized by a business role	**Review only items that have not been authorized by a business role** or **Review only items that have been authorized by a business role**.

NOTE: For an account to be authorized by a business role, the application to which the account belongs to should be added as an authorized resource for the business role. Estimate impact calculations display an *approximate* number of review targets and do not include additional options such as business role authorizations in the review target calculations. Start the review in preview mode to get an accurate preview of review items based on all review item selection criteria.

25.1.6 Specifying Self-Review Policy

Identity Governance enables administrators to specify self-review policy when creating review definition based on the following review types:

- User Access Review
- User Profile Review
- Account Review
- Business Role Membership Review

When specifying the self-review policy, you can choose to:

- Allow self review in all stages regardless of the specified reviewers
- Send all items that will result in a self review to the exception queue
- Prevent self review, but allow other reviewers to complete review actions when a review item is assigned to multiple reviewers in a specific review stage

25.1.7 Specifying Reviewers

When defining a review, you assign users and roles to perform the review. Depending on the type of review, you can specify any or more than one of the following options as reviewers.

For Review type	Reviewers
User Access	◆ Supervisor of the individual being reviewed ◆ Owners of the applications being reviewed (not available for role reviews*) ◆ Owners of the permissions being reviewed (not available for roles reviews*) ◆ Owners of the technical role being reviewed (available for role reviews*) ◆ Holder of the permission or role being reviewed, called self review ◆ Selected users or groups ◆ Coverage maps ◆ Business role *Role reviews are two variations of the User Access Review: Technical Role Assigned to Users and Technical Role Detected on Users.
User Profile	◆ Supervisor of the individual being reviewed ◆ User whose profile is being reviewed, called self review ◆ Selected users or groups ◆ Business role
Accounts	◆ Supervisor of the individual being reviewed ◆ Owner of the application being reviewed ◆ Selected users or groups ◆ Business role ◆ Account custodian ◆ Coverage map **NOTE:** To specify coverage map as a reviewer for unmapped accounts, make sure **All unmapped accounts** is selected as review items and then specify **Review by Coverage Map** as the reviewer.

For Review type	Reviewers
Accounts Access	◆ Owner of the permission being reviewed ◆ Owner of the application being reviewed ◆ Selected users or groups ◆ Business role ◆ Account custodian ◆ Coverage map
Business Role Membership	◆ Supervisor of the individual being reviewed ◆ Business role owner ◆ Selected users or groups ◆ Business role
Business Role Definition	◆ Business role owner ◆ Selected users or groups ◆ Business role
Technical Role Definition	◆ Technical role owner ◆ Selected users or groups
Business Role Authorization	◆ Business role owner ◆ Selected users or groups ◆ Business role
Global Authorization Assignment	◆ Supervisor of the global authorization administrator who is being reviewed ◆ User whose profile is being reviewed, called self review ◆ Selected users ◆ Business role
Direct Reports	◆ Supervisor of direct reports or supervisors ◆ Selected users or groups ◆ Business role

For more information about owners of applications and permissions, see Section 12.2, “Understanding Identity, Application, and Permission Management,” on page 124. For more information about coverage maps, see “Using Coverage Maps” on page 28.

For additional verification or approvals, you might specify more than one reviewer stage. If you specify more than one stage for reviews, the reviewer assignment workflow will vary based on the specified stages. For more information about multistage reviews, see Section 25.1.17, “Understanding Multistage Reviews,” on page 337.

To ensure a timely review process, you can also specify an **Escalation Reviewer**. Escalation Reviewer resolves all review tasks that are not completed on time. You can specify users, groups, and business roles as Escalation Reviewers. If you do not specify an Escalation Reviewer, the Review Owner is the

default Escalation Reviewer. Escalated review items also appear in the Exceptions stage. If Identity Governance detects any escalations at the start of a review, all of the review items appear in the Exceptions stage.

For more information about authorizations including Escalation Reviewer, see Section 2.1.2, “Runtime Authorizations,” on page 23.

25.1.8 Setting Review Expiration Policy

Review definitions contain an expiration policy. Review Administrators and owners specify the actions that Identity Governance takes when a review expires without being completed:

- Complete the review with any final decisions that have been made and send these to fulfillment and the auditor, if these are defined, and leave all other items with no decision
- Complete the review with any final decisions that have been made and send these to fulfillment and the auditor, if these are defined, and keep all other items with no user profile changes or with assigned accounts, permissions, roles, or direct report relationship
- Complete the review with any final decisions that have been made, assign remove or remove assignment decision to all other items, and send all to fulfillment and the auditor, if these are defined

  NOTE: This option is not available for User Profile Review, Business Role Definition, and Technical Role Definition Review.

- Extend the review for a grace period that will continue to renew each time the review expires without being completed or terminated
- Terminate the review and discard all decisions

For Identity Governance 2.0 and later, review definitions have the default expiration policy set to complete the review. For review definitions migrated from earlier versions of Identity Governance, review definitions have the default expiration policy set to terminate the review and discard any decisions.

25.1.9 Setting Review Notifications

Email notifications let reviewers, escalation reviewers, owners, and others know when a review is at various stages of a review run. The **Notifications** area of a review definition allows you to set up several standard notifications to go to whomever you specify during the various phases of a review. Standard notifications include **Review start**, **Review end**, **Reviewer task past due**, and **Review completion**. Review the details of the email notification and update it as needed.

You can click an email name to view who will receive the email, why they will receive it, when they will receive it, and how often they will receive it. You can either accept the default settings or change the settings and add other recipients based on relationships. You can view the name of the email source, preview the email, and email the notification to a specified email address. If you change the default settings, we recommend that you also change the description of the notification. For example, if you change who receives the notification, change the recipient name in the description.

Regarding notifications received by escalation reviewers, when a review item is escalated, Identity Governance sends the reminder notification to the escalation reviewer as it would to any other next reviewer. By default, the escalation reviewer will not receive the **Reviewer task past due** notifications

as these are typically emailed to the reviewer and reviewer's supervisor when overdue tasks remain in the reviewer queue. However, you can add an escalation reviewer as a recipient in the CC field if needed.

In addition to changing the settings when defining a review, you can also remove a default notification, customize the template of a default notification, and add new notifications by selecting an email template provided by Identity Governance. For information about customizing the templates, see Section 4.4, "Customizing Email Notification Templates," on page 46. For information about disabling email notifications such as notification when a running review is terminated or notification when permissions are revoked, see "Disabling Review Email Notifications" on page 53.

25.1.10 Scheduling a Review

Identity Governance calculates a schedule based on a specified start time, time interval, the time of the day, and the time zone. You can specify the time interval to be hourly, daily, weekly, monthly, or yearly. For all schedules, the time end date is adjusted automatically based on the Java `add` calendar method. For weekly and monthly schedules, the next review is determined based on the specified day of the week or day of the month. The following table provides a few examples of weekly and monthly schedules.

Start time	Run every	Run on	Time of day	Next scheduled start time
Tue Sept 14 02:00:00 PM IST 2021	1 month	First Tuesday of every month	02:00:00 PM	Tue Oct 05 02:00:00 PM IST 2021
Mon Sept 20 09:30:00 AM EST 2021	1 month	The last day of every month	10:00:00 AM	Sun Oct 31 10:00:00 AM EST 2021
Wed Sept 15 05:30:00 PM IST 2021	3 weeks	Friday	06:00:00 PM	Fri Oct 08 06:00:00 PM IST 2021

NOTE: ◆The Identity Governance server needs a 30-minute gap between runs of the same review. For example, if you schedule a review to run at frequent intervals, allow at least 30 minutes to lapse between the runs. Otherwise, the subsequent runs might fail to start and Identity Governance does not notify you of the failure. To control the gap, a Global or a Bootstrap Administrator must set the value for the global property `com.netiq.iac.scheduling.minTimeBetweenRuns`to `true`.

- For schedules where you select the option **after review ends**, Identity Governance considers the review period, and schedules the next review cycle based on the end date of the review period. For example, if you schedule a weekly review to run on September 20th 2021, and thereafter run every two weeks, then the next review will be scheduled for October 18th 2021, considering a review period of two weeks.

25.1.11 Previewing a Review

Administrators can start a review run, or **review instance**, in preview mode or live mode. In preview mode, administrators can:

- Preview review definition version, assigned reviewers, review items, and notification emails

- View the name of the person who started the review on demand, on schedule, or by micro certification
- Change review properties such as review owner, auditor, review options, or duration properties
- If needed, change reviewers per review item or in bulk
- Preview recipients of notifications
- Export review items to CSV
- Track details of review assignment changes
- Go live

NOTE: Review description and reviewer changes made in preview mode will apply only to the current review instance. Changes made to the **Reviews > Definitions**, will apply to future review run instances.

25.1.12 Modifying a Review Definition

Administrators can modify the attributes of a review definition at any time, including the Review Owner. If there is a running review instance at the time, that running review instance is not affected by changes to the definition. Identity Governance creates a new version of the definition with the changes and only future runs started since the modified definition will reflect the change.

If you have a review currently running, modifying the review definition does not change the attributes of the current review. The running review always points to the version of the review definition that you used to start the review.

If you assign a new owner to a running review instance, both the previous and new owners can access that specific instance of the review. The previous owner continues to see review runs from before the ownership change and future review runs. The new owner sees only that review run. You can also change the review end date and time for a running review.

25.1.13 Reviewing Items

When a review run or **review instance** is live, the server generates **review items** based on the criteria. Assigned reviewers look at the review item details, decide what action to take on each review item and submit their decisions. If allowed, by the review definition, reviewers might reassign items to a different reviewer instead of making a decision.

In a review with multiple reviewers for each review item, Identity Governance shows decisions made when the first reviewer submits actions for any of the review items. When any reviewer has submitted a decision for a review item, the other reviewers cannot take any action on that item unless the reviewer has authorization as an administrator. Review items with no actions remain in each reviewer's list until someone submits actions for them.

In a review with multiple stages, reviewers must act on review items in the order that the stages are defined in the review definition. For more information about multistage reviews, see Section 25.1.17, "Understanding Multistage Reviews," on page 337.

NOTE: When Identity Governance cannot determine an identity associated with an account or functional assignment, such as supervisor, to assign a review item to a specific person, the review owner becomes the assignee for the review item. All review items assigned in this way show in an exceptions section in the list of reviewers on the review owner view.

While reviewing items the reviewers have the option to see the assignment details such as, if the assignment was direct or inherited, assignment start and end time, assignment value and risk. If the permission collector is an AD or an eDirectory collector, then during collection, they must enable the option **Populate Nested Permission Assignments** to collect these details.

Time-based assignment information such as removal or expiration of permissions, technical roles, or business role with assignment can also be viewed while reviewing items. Reviewers and review owners of user and account access review, account reviews with account permissions, and business role membership reviews can review the assignment details and decide to keep or remove the assignments before the scheduled time. If they remove any assignment, and the review item is approved, Identity Governance removes the time-based assignment from the pending requests list. Review items with a clock icon next to it indicates that it has time-based assignment information.

25.1.14 Downloading Reviewers and Review Item Lists

Identity Governance enables you to download all or a filtered list of review items assigned to you as reviewers. In addition, Review Administrators and owners can download list of all reviewers, a list of review items in a specific reviewer's queue, and a list of all review items. You can download these lists as a CSV file for manual review and comparison.

The list of reviewers includes rows for each reviewer by queue type. For example, if a reviewer is a supervisor and also an exception reviewer, you will see two rows for the user in the downloaded file. When review items are assigned to multiple reviewers, for example when a reviewer is a group, you will see a row for each reviewer with the same number of review items. In all the scenarios, each row will include columns of all the user attributes that were enabled to display in the quick info view in the **Data Administration > User** menu including custom attributes.

The list of review items you download from the **Review Items** tab will always include all review items. Except for User Profile Review, all other review item lists will include final decisions made on the review items. User Profile Review will include only the original values of the selected attributes.

The list of review items you download from the **Your Review Items** tab includes rows for review items assigned to the reviewer with columns that you, as an administrator, included in the **Configuration > Review Display Customization** menu. You can filter the review items and download only the items you want to review manually.

NOTE: The download list items count will not match the actual number of review items in an Account Review that includes permissions. The count only reflects the number of accounts that match the search criteria. However, all the permissions under each account will also be included in the download resulting in more review items than the number displayed on the review page.

All downloaded files will be saved to a download folder. You can then click the Download icon on the application title bar to access the saved file and download the file to your local machine.

25.1.15 Understanding Reviewers and Escalation

When you initiate a review run, Identity Governance generates tasks for the assigned Reviewers. The Reviewers are responsible for reviewing a set of users and deciding whether the current user access should be maintained or revoked, or, in some cases, modified. Identity Governance can send reminders to the Reviewer or escalate the review items to the Escalation Reviewer, if one was specified in the Review Definition, or to the Review Owner who is the default Escalation Reviewer. Also, review items in the exception queue (unmapped accounts) are automatically assigned to the Escalation Reviewer if an escalation reviewer was specified for that review. In a multistage review, Identity Governance forwards the task to the next reviewer before it finally moves the tasks to the Escalation Reviewer or Review Owner queue.

Reviews that contain reviewers specified by a coverage map can result in an escalation if no matches could be found from the coverage map. For more information about reviewers, see Section 25.1.7, “Specifying Reviewers,” on page 331. For more information about managing Reviewers, see Section 28.2.4, “Managing the Progress of Reviewers,” on page 358. For more information about performing a review, see Section 29.1, “Performing a Review,” on page 361.

25.1.16 Escalating Review Items

Identity Governance provides escalation options to help Review Owners and Administrators ensure that the review process proceeds in a timely manner. You can set one or more escalation reviewers, and a timeout value to instruct Identity Governance to **escalate the process** and move pending review items to escalation reviewer queues. If a review definition does not set escalation reviewers, the review owner is the default escalation reviewer and in a multistage review, review items will be escalated to the next reviewer in the queue.

NOTE: If a review definition specifies a group as the reviewers and a member of the group is the person being reviewed, Identity Governance uses the self-review policy to determine which group members can review the item. The self-review policy can either allow users to review their own items (self review), send self-review items to the exception queue, or prevent self review but allow other reviewers to complete the item if it is assigned to multiple reviewers in the same stage. For more information about the self-review policy see Section 25.1.6, “Specifying Self-Review Policy,” on page 330.

25.1.17 Understanding Multistage Reviews

If you specify more than one reviewer stage, the reviewers must complete the review in the assigned order. For example, you might want the permission holders to verify that they continue to need the assigned permission, then the individual’s supervisor can approve that ongoing need. As a final step, the permission owners can review the assigned permission. In this case, you would specify **Self review**, **Supervisor**, then **Permission owners** as the reviewers. Each stage shows as a separate group of review items to the review owner. When you select **Self Review**, users can review their access for that stage only, unless the Review Options are set to **Allow self review in all stages**.

If you specify more than one reviewer (such as a set of users or groups), each reviewer shares the responsibility for submitting a decision within a single reviewer stage. For example, you might want the permission holders to verify that they continue to need the assigned permission, then you want a group of users called **Super group** to approve the ongoing need. In this case, you would specify **Self review** then **Review by Selected Users: Super group** as the reviewers.

You can also specify that a stage is skipped if the prior stage decision is **Keep** or **Remove**. By default, you cannot specify the same reviewer in consequent stages.

At any point during a review run, Identity Governance might not be able to resolve a reviewer. For example, if you specify **Permission owners** as one of the reviewers and no permission owner is actually specified in the catalog, Identity Governance cannot resolve the reviewer to an identity. When this happens, the review item is escalated to the Escalation Reviewer, if one exists, or to the Review Owner, and this reviewer must complete the remaining review tasks for the item. In this situation, the review owner sees an exception section with the review items with the unresolved review items.

Secondary reviewers in a multi-stage review can confirm the previous decision or they can override the decision. For Technical Role and Business Role Definition review they can make additional changes to the review definition or undo or discard the changes.

25.1.18 Completing or Terminating a Review

Aside from letting the expiration policy complete the review run, a review run concludes in one of several ways:

- All specified reviewers submit actions for their review items, and the Review Owner approves or terminates the review run.
- Reviewers do not submit actions for all their review items, and the Review Owner completes the review run.
- Reviewers do not submit actions for all their review items, and the Review Owner terminates the review run.

After reviewers have made decisions and submitted all review items, the Review Owner approves or terminates the review run and Identity Governance moves the review run details to a list of completed reviews.

A Review Owner has the option to complete an in-progress review even if reviewers have not submitted decisions for all review items. When a Review Owner completes a review, Identity Governance takes the following actions:

- Forwards any final decisions that reviewers have made to fulfillment. In multistage reviews, a decision is considered final only when all multi-stage reviewers of a review item have submitted their decisions.
- Marks the remaining review items **Keep**, **Remove**, **Keep Assignment**, **Remove Assignment**, **No profile changes** or as no decision made based on the review definition expiration policy.
- Shows the review status as a percentage of completion in review history.

A Review Owner also has the option to terminate an in-progress review. When a Review Owner terminates a review, Identity Governance takes the following actions:

- Does not forward anything to fulfillment
- Marks the review run as terminated

25.1.19 Understanding the Fulfillment Process for Review Changes

The source of the identities, permissions, accounts, and roles under review drives how review-related request changes are fulfilled. The fulfillment process can be manual tasks, automated actions in Identity Manager, actions sent to help desk services, or actions initiated by workflows in Identity Manager. The **fulfillment** process begins when a review run completes or when a Review Owner or Administrator modifies or removes a review item, it generates a change request which are then sent to fulfillment for approval. Each review item generates separate change request. However, for Business Role Authorization Review, the review items are consolidated into a single change request, which is then forwarded to fulfillment.

Note that, for Global Authorization Assignment review types, Identity Governance fulfills the change requests through its internal process and does not initiate a separate request.

Identity Governance, however, does not generate change requests for review items for entities, such as a role, permission, account, or user if they are deleted before approval. In such cases, Identity Governance marks the deleted entities with a strike-through line across the text and also provides the reason for not generating the fulfillment request under View Fulfillment Status.

For Technical Role Definitions review, when you generate a fulfillment request due to attribute change or permission revocation, Identity Governance automatically fulfills those requests on approval. But there are scenarios when Identity Governance sends requests for manual fulfillment. Following are those scenarios:

- When the value of a single-valued attribute, for example, risk has changed since the review started
- When a category marked for removal is no longer associated with the role
- When a permission marked for revocation is no longer assigned to the role
- When internal fulfillment is not enabled
- When special fulfillment instructions are specified

Sometimes multiple changes per review items are split between automatic and manual fulfillment. In such scenarios, Identity Governance fulfills some changes automatically and sends the remaining for manual fulfillment.

If you are a Global Administrator, you can set the global property `com.netiq.iac.fulfillment.techrole.manualonly` to `true` to send all requests for manual fulfillment.

There are scenarios when Identity Governance forwards request items for manual fulfillment. For example, when the fulfillment target is Active Directory, and there is a request to remove an inherited permission from a user. When a user is assigned a permission to a group because they are a member of that group, it is a direct assignment. However, there are times, when a user is assigned permission to a group even when they are not a direct member. This happens when the groups are embedded. In such scenarios, the user inherits the permission and Identity Governance fails to automatically fulfill the request since the user is not part of the group. To collect these permission assignments, you must enable the option **Populate Nested Permission Assignments** while configuring the Identity Governance **AD Permission** and **eDir Permission** collector templates.

Review Owners and Administrators can view the fulfillment status of review items automatically fulfilled and verified by internal processes as soon as a review run is partially or fully approved.

For more information about fulfillment, see Section 15.1, “Understanding the Fulfillment Process,” on page 175.

25.1.20 Managing the Audit Process

Some review definitions require a Review Auditor to certify the results of the review run. Review Auditors are individuals who have read-only access to a review run. They cannot modify or delete decisions. They can:

- View the review definition used for the review run
- View reviewers and decision statistics
- View review items and related activity
- Download list of reviewers and their respective queue statistics as a CSV file
- Download list of all review items as a CSV file
- Accept the review
- Enter comments for rejection and reject the review

NOTE: All decisions and run history are retained even if the review is rejected.

Usually, Identity Governance sends an email notification to the Review Auditor when a review run is waiting for acceptance. The Review Auditor can then log in and can review all details and **Accept** or **Reject** the review. The Review Auditor must enter comments when rejecting a review.

25.1.21 Creating Certification Policies and Remediating Violations

A Customer, Global, Review, or Data Administrator creates certification policies and sets remediation action for violations. Identity Governance calculates violations and after initial setup automatically triggers remediation action. Remediation actions include email notifications, change requests, or micro certification.

For more information about micro certification and certification policies, see Section 25.2, “Understanding Micro Certification,” on page 340 and Chapter 30, “Creating and Managing Certification Policies,” on page 365.

25.2 Understanding Micro Certification

Micro certifications are focused event-driven reviews which involve a smaller number of review items. For example, a micro certification review could involve review items such as users, accounts, permissions, permission assignments, or roles that violated a certification policy or a data policy. Micro certifications are designed to reduce or eliminate the need for full-scale access certification processes which require significant time and effort from business users.

A micro certification review inherits reviewer assignments and settings from the specified review definition and follows a similar life cycle as an on demand or scheduled review run. Currently, all review types support micro certification. Multiple micro certification reviews can run in parallel with on demand or scheduled reviews that use the same review definition.

NOTE: Any changes you make to the review definition when micro certification review is in progress will apply *only* to *subsequent* review instances based on these review definitions. The running review always points to the version of the review definition that you used to start the review. For example, if you change the micro certification review name when running remediation, the new name will be applied to subsequent micro certification reviews based on new violations and not to the micro certification review in progress.

A Customer, Global, or Review Administrator can view status and run history of micro certifications in the Review definition list area by selecting the number of micro certifications when Micro-certification in progress column is included as a display column. You can include the column in Review definition list area, by selecting the gear icon and dragging and dropping columns to the Available column area. Similarly, in the Review list area, you can include Started by column to view if a review was started by micro certification, on demand, or schedule. For more information, about customizing review display, see Section 26.2, "Customizing Review Display," on page 346.

NOTE: For information about setting up micro certification as remediation for policy violations, see "Detecting and Remediating Violations in Published Data" on page 119 and Section 30.5.3, "Remediating Certification Policy Violations," on page 369.

25.3 Improving Performance in Large Scale Reviews

Based on your data, reviews can take significant time and effort and occasionally may need to be terminated and restarted. To improve performance, administrators can either temporarily disable review statistics calculations or enable **materialized view**. Both of these options should be used with caution.

Disabling review statistics calculations

Use the Configuration Utility console mode setting `iac.update.stats.review.disabled` to disable review statistics calculations. If you choose to disable review statistics calculations, you will need to enable it again using the Identity Governance Configuration Utility.

Using materialized view/specialized tables

A materialized view is a snapshot of an instance of time which is used to optimize performance in large scale reviews. Materialized views are supported in Postgres and Oracle environments. When this view is enabled, you can cache user, account, permission, and role names to improve rendering time of review items by selecting **Monitor Reviews > Cache review item names** in a review definition. In MSSQL environment similar capabilities are implemented using specialized tables.

Use the Configuration Utility console mode setting `add-property GLOBAL iac.review.display.materializedViews.enabled true` to enable materialized view. In addition, in Oracle environment, assign the `GRANT CREATE MATERIALIZED VIEW TO IGOPS;` rights to the operations database (`igops`) and *optionally* specify tablespace. Use the command `add-property GLOBAL iac.materializedViews.oracleTableSpace` *`Tablespace`* (example, `add-property GLOBAL iac.materializedViews.oracleTableSpace USERS`) to specify the tablespace in which the materialized view is to be created. If you omit this clause, then Oracle database creates the materialized view in the default tablespace of the schema containing the materialized view. Only use this setting if the Oracle default is not sufficient, in most cases it is.

NOTE: If the materialized view is not initially enabled using the Configuration Utility, **Cache review item names** check box will not be displayed. For small scale reviews, caching of review item names is *not* recommended.

Once materialized view is enabled, the search and sort features will use the values at the time the materialized view was either created or last refreshed. As by definition, a materialized view is a snapshot, the data can become stale and out of sync with the catalog, and your search might not yield accurate results. You can refresh the snapshot data at any time by selecting **More** to expand review instance header, and then clicking **Refresh**. Also, you can **Enable** or **Disable** the caching of review item names for that review instance.

26 Creating and Modifying Review Definitions

After you have data in your catalog, and (optionally) have customized review display column and configured reasons for review actions, you can start creating review definitions based on your organization's requirements. The reviews enable a set of reviewers to examine who has access to what in their environment. In the review definition, you can assign runtime authorizations such as review owner and reviewers and specify review objects. Administrators can create review definitions for the following types of objects:

- Access permissions, accounts, or technical roles of a set of users
- Mapped and unmapped accounts
- Permissions assigned to the accounts
- Membership of a set of business roles
- Identity attributes that were previously configured as available for reviews
- Management assignments, specifically direct reports of supervisors
- Business role definition including authorizations, membership, and attributes that were previously configured for reviews

Only users with the Review Administrator, Customer Administrator, or Global Administrator authorization can create and modify review definitions.

26.1 Creating a Review Definition

The review definition enables you to define and schedule various types of reviews. It contains all of the information required to run a review. You can also modify the definition for subsequent review runs without the need to create additional review definitions. To create a review definition, the catalog must contain published data.

To create a review definition:

1. Log in as a Review Administrator.
2. Select **Definitions**.
3. Click **+** to create a new review definition.

4 Select the type of objects you want to review, or search based on review type then select type of objects.

5 Name the review and add description.

6 (Optional) Add instructions that explains to reviewers what they need to do. For example, `please review these items or reassign to someone else if necessary`.

7 Accept the default review item selection criteria or refine the selection criteria to focus the review based on your security and compliance needs. For example, you can review accounts based on account custodian or last account review date. Alternately, you can review users, business roles, or accounts based on risk.

Selection criteria for your entities or business roles include respective attributes that have been previously enabled as a selection criteria. When you choose the **Select** option to specify entities or business roles, click **+** to add conditions for your selection.

NOTE: In addition to default selection criteria for review items such as risk, you can request your Data Administrator to add other selection criteria including custom criteria for various reviews.

---

8 (Optional) Select **Estimate Impact** to view the approximate number of review items and depending on the selected review type, the approximate number of users, permissions, roles, accounts, or business roles. or click the **Download review targets as CSV** link to download the review items and review them offline.

NOTE: Identity Governance calculates the *approximate* number of review targets. Business role authorizations are not included in this calculation. Results in a running review will also vary based on review options and the most recent state of the catalog. Start review in preview mode when authorizations are also calculated, to see all review items.

Based on the number of review targets, you might need to revise the **Review period**. For example, a review with 15 items might be completed within days, but one with hundreds of items could require weeks to accomplish.

9 (Optional) For **Review Options**, select any additional options that apply to this review. For example, you can require comments for certain actions. When you select this option, a Reviewer or a Review Owner must enter a comment to complete the keep, remove, override or change reviewer actions. You can also allow or disallow reviewers from changing reviewers and configure self-review policy. For more information about the self-review policy, see Section 25.1.6, “Specifying Self-Review Policy,” on page 330.

10 (Optional) Specify the reviewers you want to participate in the review.

For more information about types of reviewers, see Section 25.1.7, “Specifying Reviewers,” on page 331.

11 (Optional) To create a serial, multistage review, select **Add Reviewer**.

This allows you to specify multiple individuals who review the review items in the order listed in the definition. For more information, see Section 25.1.17, “Understanding Multistage Reviews,” on page 337.

12 (Optional) For **Monitor Reviews**, specify the review owner and auditor.

If you do not specify the review owner, the person who created the review definition becomes the review owner by default. If you do not specify an auditor, the review will not go through the audit acceptance phase.

(Conditional) If the materialized view is enabled, select **Cache review item names** to cache user, account, permission, and role names to improve performance in large scale reviews.

WARNING: If you enable caching, periodically **Refresh** cache review items to synchronize the review with changes to the catalog. For more information, see Section 25.3, “Improving Performance in Large Scale Reviews,” on page 341.

---

13 (Optional) For **Task Due Date and Escalation**, select one of the following options:

- **When review is scheduled to end**

  Select this options where you want the reviews to end based on **Duration** settings.

  NOTE: Review Administrators or Owners can change review end date to a specific date and time when they start the review run.

- **Specify maximum queue time**

  Select this option if you want reviewers to have a due date for their items. This due date can trigger notifications and when review items are past their due date show that the items are overdue. Even if this is a multi-stage review, review items will not leave the current reviewer's queue when items reach their due date.

  For **Maximum time in queue**, specify the number of days, weeks, months, or years allowed for the reviewers to complete their tasks. You must use whole numbers for the value. If the review started at the time when the review definition was created, this would be the due date. Secondary reviewer due dates are calculated based on the time the item enters the reviewer's queue.

- **Specify maximum queue time and escalation reviewer**

  Select this option when you want review items to escalate if not completed by the due date. In the case of multistage reviews, items will escalate to the next reviewer. In the case of multistage reviews where the review item is in the final reviewer's queue or in the case of single-stage reviews, the review items will escalate to the specified Escalation Reviewer if not completed by the due date.

  Specify **Maximum time in queue** and the **Escalation Reviewer**. The Escalation Reviewer is the final reviewer in the escalation process. When tasks are past due and no further review stages are defined, all open tasks will move to this reviewer’s queue. The Escalation Reviewer can either be the Review Owner or selected users specified by searching and selecting identities, groups, or business roles.

14 (Optional) For **Duration**, set or change any of the following options:

14a For **Review period**, specify the length of time allowed for the review run.

14b For **Expiration policy**, specify what happens when a review expires without being completed.

14c For **Partial approval policy**, specify whether partial approvals are allowed and if so, whether or not partial approvals will occur automatically.

NOTE: You cannot partially approve a policy for Business Role Authorization review, because for this review type multiple authorizations are aggregated into one change request and sent for fulfillment.

14d For **Validity period**, specify the period of time before the certified items need to be reviewed again. For example, specify `6 months` if you intend to run the review again after six months from the current review schedule.

NOTE: After completing a review, the review renewal data value might display a different time unit than the validity time period specified in the review definition because as the review approaches its next cycle, the time period changes. For example, a validity period of 2 weeks might display a renewal date of 14 days or less to indicate the number of days before the review starts its next cycle.

---

15 (Optional) For **Notifications**, add notifications based on provided email source templates, view notification description and settings, or remove default review notifications. Customize default notification schedule including recurrence schedule, and add email recipients.

NOTE: Typically, you can specify only one recipient in the **To** field and multiple recipients in the **CC** field. You can specify recipients of CC by specifying relationship and identity attribute for the selected relationship. However, the read-only **Review terminated notice** which is based on the Certification Terminated email source template goes to reviewers, review owners, escalation reviewers, and auditors when a review ends. You cannot change the recipients.

Click **Email source preview** to preview email HTML source and to specify a recipient for the rendered version of the email. For more information, see Section 25.1.9, “Setting Review Notifications,” on page 333.

16 (Optional) For **Schedule**, if you want the review runs to begin automatically and repeat automatically, select **Active** and select the appropriate schedule. Make sure there will be at least a 30-minute gap between runs. Select **Start scheduled review in Preview mode requiring manual go live** to start a review in preview mode. For additional information about scheduling reviews and 30-minute gap requirement between runs, see Section 25.1.10, “Scheduling a Review,” on page 334.

17 Save the review.

18 (Optional) After saving the review definition, set the default columns for the current review definition by editing the review definition and specifying **Default Reviewer Display Preferences**. Otherwise, the default grouping and default sort for the reviewer display will use the **Configuration > Review Display Customization** settings you had set for each review type as the default display preference.

NOTE: If needed, the reviewer can change the default grouping for their review instance by using the **Show All** drop-down list, change the sort order by clicking on headings with descending or ascending arrow, and change the column display by using the display options settings menu.

26.2 Customizing Review Display

Identity Governance customizes the review display based on user authorization and the context of your action. It also enables you to customize the review display by:

- Specifying attributes that can be displayed as columns by review type, setting the default number of rows per page for reviewers, and setting whether to display completed reviews using **Reviews > Review Settings > Review Display Customization** options

- Selecting default grouping, sort, and reviewer columns using **Review Definition > + > Default Reviewer Display Preferences** options

---

NOTE: Only attributes selected in **Review Display Customization** will appear as a column in **Default Reviewer Display Preferences**.

- Selecting column options in the review definition and review items list areas by clicking the gear icon and viewing list of columns available for display

To customize review display:

1. Log in to Identity Governance as a Customer, Global, or Review Administrator.
2. Select **Reviews > Review Settings > Review Display Customization**.
3. Specify whether you want the **Completed Reviews** section on the Reviews page to be shown expanded by default.
4. Type the default number of rows per review items page.

NOTE: Reviewers can change this setting for their display as needed. The recommended maximum number of rows is 50.

---

5. For each review type, add or remove a column from reviewer display and rearrange columns as needed.
6. Click **Save**.

NOTE:
- To show attribute in expanded details, a Customer, Global or Data Administrator can select the attribute in the attribute type section of the **Data Administration** area, such as the Department attribute in **Data Administration > Identity Attributes**, and then select **Display in Quick Info views** under **Listable Options**.
- To have Generic Attributes 1-6 available for selection in the **Review Display Customization** options for user and account access review types, a Customer, Global, Data, or Review Administrator must first select **Data Administration > Permission Assignment Attributes**, select the attribute, then select the **Activate** check box.

26.3 Configuring Reasons for Review Actions

Identity Governance allows you to configure reasons for review actions for analytical and reporting purposes. Customer, Global, or Review Administrators can configure reasons for:

- Changing reviewers
- Modifying review items by specifying fulfillment instructions

Once the reasons are configured, they are available as drop-down list options when a review owner or a reviewer changes the reviewer for a review item, and when a reviewer selects **Modify** action in a **User Access Review** or selects **Modify with instructions** in an **Account Review**.

To configure reasons for review actions:

1. Log in to Identity Governance as a Customer, Global, or Review Administrator.

2 Select **Reviews > Review Settings**, and then click **Change Reviewer Reasons** or **Modify Review Item Reasons**.

3 To add a new reason, click **+** and specify a reason. For example, you can add a Reviewer is on vacation as a reason for changing reviewer or Assign account custodian as a reason for modifying a review item in Account Review.

4 (Conditional) If the modify review item reason requires user selection, click the **User selection required** check box.

5 Click **Save**.

6 To edit the reason, select the reason and edit it.

7 To delete a reason, select the reason and click **Delete**.

NOTE: Once a reason has been used in a review, you can see the number of times it has been used in reviews in the respective reason tab. If the reason has been used even once in any review, you can no longer edit or delete it. However, you can **Enable** or **Disable** the reason. Reviewers will not see the disabled reason as an option in the drop-down list.

26.4 Downloading and Importing Review Definitions

In addition to downloading reviewers and review items lists as CSV files, you can also download review definitions as JSON files and import the review definitions later into another environment.

For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

26.5 Creating a New Review Definition from an Existing Review Definition

Instead of specifying review options, reviewers, notifications, and escalation policies for each new review definition, you can now use an existing review that has a similar definition to create a new review definition.

To create a new review definition from an existing review definition:

1 Log in to Identity Governance as a Review, Customer, or Global Administrator.

2 In the Quick Info window, click **Copy to New**.

3 (Optional) Rename and edit the review definition.

4 Click **Save**.

27 Understanding Review Run

In Identity Governance, Review Administrators create **review definitions** for a particular set of users, accounts, or roles that need review. A single instance of a review definition is a **review run** or review campaign, which has a Review Owner. The Review Owners can see only the review runs that they own.

Reviews can be started either in a preview mode or a live mode, or when an event triggers micro certification. Review Administrators can set up a review to automatically start in preview mode or schedule for live review runs while creating a review definition. Live review runs can also start automatically when certification or data policy violation remediation is set to micro certification.

Identity Governance notifies any person or role specified in the Notifications settings of the review definition, once a review is initiated. After a Review Owner approves the review run or individual review items, Identity Governance notifies fulfillers if they have change items. For more information, see Section 28.2, “Managing a Review in Live Mode,” on page 354.

27.1 Understanding Review Run in Preview Mode

When the review owner initiates a review run in preview mode, or when a review run starts automatically in preview mode, the following activities occur:

1. Identity Governance generates lists of **Reviewers**, **Review items**, and **Notifications**.
2. The Review Owner previews the review definition for the current run and optionally, changes the review end date, review owner or auditor, and modifies review options and schedule.
3. The Review Owner reviews all the review items and assigned reviewers, or searches for specific review items to decide whether the items should be assigned to another reviewer.
4. The Review Owner also previews the emails notification templates and verifies that appropriate notifications are being sent to the correct recipients.

   NOTE: Any changes made by the Review Owner are applied only to the current run. If permanent changes need to be made to the review definition, or reviewers need to be changed for all subsequent runs, the changes must be made by editing the review definition itself.
5. Optionally, the Review Owner can download all or select review items as a CSV file to review it manually.

27.2 Understanding Review Run in Live Mode

When the owner initiates a review run in live mode, or when a review run starts by the schedule, or when a micro certification review is automatically started, the following activities occur:

1. Identity Governance generates tasks for the assigned Reviewers and notifies them as specified in the review definition.
2. Reviewers review their assigned set of review items and decide whether the items should be kept, modified, or removed. If a review item is assigned to multiple reviewers, the first reviewer who acts on that item becomes the decision maker, and the item continues to the next phase of the review. For more information, see Section 29.1, “Performing a Review,” on page 361.
3. (Conditional) If the review definition specifies that a permission requires multiple stages of approval, Identity Governance forwards the affected review items to the next assigned reviewer.

   For example, the application owner, permission owner, or Review Owner might be required to review the permissions and confirm decisions before action is taken to remove any permissions. Reviewers must complete the review in the assigned order.
4. (Conditional) If a Reviewer does not complete tasks in the specified time frame and the review definition specifies an escalation process, Identity Governance forwards the tasks to the assigned Escalation Reviewer. The Review Owner is the default Escalation Reviewer when an administrator does not specify the Escalation Reviewer in the review definition.

   If there are multiple reviewers, Identity Governance forwards the task to the next reviewer before it finally moves the tasks to the Escalation Reviewer or Review Owner queue.
5. The Review Owner approves the changes.

   NOTE: If specified in the review definition, Review Owners can override reviewer decisions at any point during a review run. When a Review Owner overrides a decision, the review item is locked and can no longer be modified by the reviewer.

   ---
6. Identity Governance initiates the fulfillment process to enable the requested changes.
7. (Conditional) In a manual fulfillment process, Identity Governance generates tasks that the assigned Fulfillers must complete and notifies them by email.
8. (Optional) An Auditor might be required to certify the results of the review run.

27.3 Completing Review Tasks

Identity Governance notifies reviewers by email when they have tasks for a review run. When you log in as a reviewer, you can see the assigned tasks for each review. Then you can evaluate the items in the task list. Usually, you either certify the permissions assigned to users for a particular application or the presence of unmapped accounts in the application.

After the reviewers have completed their tasks, a Review Owner must approve the changes to create a change list to be fulfilled. At this point, fulfillers and the review auditor, if one exists, get email notifications that they have tasks to complete in the review. For more information about these authorizations, see Section 2.1.2, “Runtime Authorizations,” on page 23. For automated fulfillment configurations, Identity Governance sends fulfillment changes to configured systems. For more information about automated fulfillment, see Section 14.2, “Configuring Fulfillment,” on page 157.

For more information about completing review tasks, see Section 28.2.5, “Approving and Completing the Review,” on page 358.

27.4 Verifying and Approving a Review Run

Review owners can review the decisions at any time during a review run. The owner can override the status of any decision if **Allow review owner to override decision** is enabled in the review definition. For example, if the review owner changes a `Remove` decision to `Keep`, that decision becomes the final decision for that item.

At any point during the review run, the review owner can end the run by selecting **Complete**, or **Terminate**. When selecting **Approve**, any decisions made before completing an in-progress review are retained and forwarded to fulfillment, if partial approval was allowed in review definition **Duration > Partial approval policy**.

28 Instructions for Review Owners

Identity Governance enables your organization to review and verify that users have only the level of access that they need to do their jobs. As a Review Owner, you are responsible for managing one or more reviews. You can view the details of any user, permission, role (technical or business), or application entity within the context of the review run. However, depending on your authorization assignments, you might not have access to the Identity Governance catalog which provides additional information about the user, permission, application, and technical role.

As a Review Owner you can decide if you want to preview the review or go live with the review. This section lists the tasks you can perform in preview and live mode.

28.1 Managing a Review in Preview Mode

As the owner or an administrator of a review, when the review is in preview mode, you can perform any or all of the following tasks:

To manage a review in preview mode:

1. In Identity Governance select **Reviews** > **Definitions**.
2. Under the Status column, select **Preview** > **more**.
3. (Optional) Click the **View review definition version used for this run** link to view version, review items, assigned reviewers, recipients of notification.
4. (Optional) Select the edit icon to change the following details for the current review run:
    a. Select **Duration** to change the review end date to a specific date and time, expiration policy, partial approval policy, or the validity period of the current run.
    b. Select **Monitor Reviews** to change the Review Owner or Auditor.
    c. Select **Task Due Date and Escalation** to change the Escalation Reviewer, escalation timeout period.
5. (Optional) Select the **Reviewers** tab to download list of all reviewers and their queue summary, list of review items in a selected reviewer’s queue, and list of all review items to CSV files.
6. (Optional) Select the **Review items** tab to change the following details:
    a. Click the gear icon to customize display settings for the review items.
    b. Click the **Change Reviewer** option to change reviewers individually or select all and then click **Actions** > **Change Reviewer**.

    NOTE: If the review definition states that the change reviewer action requires a comment, then you must enter a comment to complete the action.

7. (Optional) Select the **Notifications** tab to perform the following tasks:
   a. Search for email recipients by name.
   b. Click the **Notification** column to sort notifications by type.
   c. Click the **Send notification preview** option and enter the email ID of the recipient.

   NOTE: Notifications sent during review preview mode, which enable administrators and review owners to preview notifications, might have blanks for values, and names seen in the preview might not be the name that is sent in the real email.

   ---

8. (Optional) Click **Cancel preview** if review properties and items were not as expected and the review definition needs to be modified or **Go live**.
9. (Optional) Change the review end date and time.

28.2 Managing a Review in Live Mode

As the owner or an administrator of an active review, you can perform any or all of the following tasks:

To manage a review in live mode:

1. Understand the review process.
2. Start the review run if needed and optionally change the review date and time.

   NOTE: In addition to manually starting a review, you can initiate a review by schedule or micro certification.

   ---

3. Customize the review definition and the column display for the review items. For example, include the column Micro-Certification in progress to review details related to micro certification.
4. Modify the duration of the review.
5. Check the progress of each Reviewer.
6. Approve the actions taken by the Reviewers.
7. (Conditional) Check the status of manual fulfillment activities. If the process is automated or uses external workflows, Identity Governance sends the changeset to Identity Manager for processing.
8. (Conditional) If you have authorization to view fulfillment status in the fulfillment page, confirm the completion of all fulfillment tasks.
9. (Conditional) If a review run generated a changeset, collect and publish all identities and the application sources related to the review run.

   You might not have the authorization in Identity Governance to collect and publish. Someone with the Global Administrator or Data Administrator authorization can perform this action.
10. (Conditional) If you are the auditor, check the status of the review auditor.
11. View run history.

If you assign a new owner to a review, both the previous and new owners can access the review. The previous owner continues to see instances of a review run before the ownership change. The new owner sees only the instance of a review run after the ownership change.

If you assign a new Review Owner while a review run is in progress, the review definition does not change, and the new review owner is in effect for only that review run. The next review run that starts from the same review definition assigns the review owner specified in the review definition.

For example, a review definition specifies Mary Smith as the review owner. During an instance of the review, or a review run, the global administrator realizes that Mary is on vacation. To keep the review moving, the administrator changes the review owner to Sam Butler, who approves that review run when reviewers have submitted all their final decisions. Both Mary and Sam can see the details of this review run. The next time a review run starts from this review definition, Mary is assigned as the review owner.

28.2.1 Starting a Review Run

In Identity Governance, you can see all review definitions assigned to you, including the date that the Review Administrator specified the review should be run.

To start a review run:

1. In Identity Governance, select **Reviews > Definitions**.
2. (Optional) Click the gear icon to change column display options. For example, to add the micro certification column to your display drag **Micro-Certifications in progress** to the list of selected columns. You can then view the number of micro certifications and view the run history of the micro certification review.
3. In the Actions column, select **Start Review** on the row of the definition that you want to run.

   NOTE: For micro certification reviews, this step is not required and the Actions column is unavailable. Micro certification reviews are triggered automatically based on remediation setup and do not require manual action.
4. (Optional) Change the end date calculated based on your review definition duration settings to a custom date and time.
5. Click **Start and Go Live**.

28.2.2 Managing a Review Run

You can view the status of the review runs in progress, send reminder emails, change the assignments for reviewers and the auditor, override or approve reviewer decisions, complete or terminate the review run, and approve the completed review.

To manage a review run:

1. In Identity Governance, select **Reviews > Reviews**.
2. (Optional) Click the gear icon to customize column display. For example, you can drag **Started by** to the list of selected columns to view name of the person who started the review on demand, on schedule, or by micro certification process.
3. Select the review you want to manage.
4. To see the status of each review item, or see the count of the number of accounts reviewed when you select the option **Additionally review permissions for each selected account**, click the **Review Items** tab.
5. (Optional) Download list of reviewers, a reviewer's queue, or review items to a CSV file.
   - **5a** Select the **Reviewers** tab and click **Download reviewers** to download list of all reviewers with their queue summary.
   - **5b** Select the **Reviewers** tab, select the number of items in the **In Queue** column of a reviewer, then click **Download all as CSV** to download the reviewer's queue details.
   - **5c** Select the **Review Items** tab and click **Download all review items as CSV** to download all review items in the review. If the option **Show fulfillment status on download** is enabled in the **Review Settings > Review Display Customization** menu, you can also view the fulfillment status in the CSV file. Review items that generate multiple fulfillment requests have a line for each fulfillment-review item combination.
   - **5d** Select the **Your Review Items** tab, to download all review items assigned to you for review, selectively download review items by selecting a grouping option or searching for values for columns included in **Review Settings > Review Display Customization** menu. For example, if you want to review only items in exception queue, you can select **Group by exceptions**. If you want to include items whose decision you had previously submitted, you can select the filter icon and include submitted items.

NOTE: ◆ Type a meaningful description for your file, and save the file to the central download area of the application. Click the download icon on the application title bar and then download the file. For more information about downloading options and examples, seeSection 25.1.14, "Downloading Reviewers and Review Item Lists," on page 336.

◆ When review items for entities such as users, permissions, accounts, or technical roles are deleted, Identity Governance marks the deleted entities with a strike-through line across the text. One of the places where you can view these deleted entities is under the **Review Items** tab.

---

6. Act on review items either individually or by using the bulk selection options. Actions you can take depend on settings in the review definition and might include:
   - **View activity** to see review item details.
   - **Override** a Reviewer's decision when you agree or disagree with the decision or make a decision final and remove it from all reviewer queues. If the review definition states that the override action requires a comment, then you must enter a comment to complete the action.
   - **Change reviewer** to transfer the review item to another reviewer.

- **Approve** to move the decision to fulfillment while allowing the review to continue. Note that for Technical Role Definition review, fulfillment request resulting from attribute change or permission revocation are fulfilled automatically on approval.
- **View fulfillment status** to view the status of review requests such as removing a permission, or assigning a new user.

7 To complete the review in its current state, accepting all final decisions and marking items without final decisions as No decision or as other decision specified in the review definition's expiration policy, select **Complete** in the review completion overview at the top of the review.

8 To move all final decisions to fulfillment while allowing the review to continue, select **Approve** in the review completion overview at the top of the review.

9 To cancel the review, select **Terminate** in the review completion overview at the top of the review.

28.2.3 Modifying the Settings of a Review Run

As the Review Owner, you can edit the review time frame and escalation timeout; change the Escalation Reviewer, the assigned Auditor, and the Review Owner; and add multiple Review Owners. Depending on your authorization assignment, you might also be able to modify the full review definition. Any changes you make to the review definition when a review is in progress will apply *only* to *subsequent* review instances. However, this section explains how to perform simple modifications to an active review run.

To modify the settings of a review run:

1 In Identity Governance, select **Reviews > Reviews**.

2 Select the active review run that you want to modify.

3 To determine whether the number of review tasks can be performed in the specified time frame, complete the following steps:

3a Under the review name, select **more**, and then select the edit icon.

3b Observe the number of review items to be completed.

3c Compare the estimated number of review items with the date in **Review end**.

3d Change the end date for the review to ensure any new review items added to the catalog, since the time the review definition is created is considered in the review run.

4 Change the review owner if your authorization in the organization changes, or add review owners to make sure suitable individuals are assigned for the task.

5 Modify the appropriate settings, then select **Save**.

28.2.4 Managing the Progress of Reviewers

To ensure that the review run stays on schedule, you can view the progress of each Reviewer. You can also reassign tasks to a different Reviewer if the assigned Reviewer is sick or on vacation, or there are reviewers who can complete the tasks faster. You can override a Reviewer's action for a review item.

If the reviewer is listed as **Multiple Reviewers**, then more than one reviewer shares the responsibility for making a decision on the review item. You can see the members of the shared queue and send reminder emails to all of the members or delegates, if a mapping exists. When a reviewer of a review item in a **Multiple Reviewers** queue is changed, the item is no longer under shared responsibility.

Reviewers can change the reviewer for any items unless otherwise specified in the review definition.

To manage the progress of reviewers:

1. In Identity Governance, select **Reviews > Reviews**.
2. Select the active review run that you want to manage.
3. Under **Reviewers**, select the name of the Reviewer that you want to manage.
4. Observe the actions taken by the Reviewer.

   You can view the items that have not been completed or all review items. You can send reminder emails, using the **Nudge** option, for items not yet reviewed. You can also change sorting of the items based on the selectable column headers.
5. (Optional) Click **Nudge** to compose and send a reminder email to the Reviewer or select multiple reviewers and click **Actions > Nudge**.
6. (Optional) To assign a review item to a different Reviewer, select **Change Reviewer** or select multiple reviewers and click **Actions > Change Reviewer**. If the review definition states that the change reviewer action requires a comment, then you must enter a comment to complete the action.
7. (Optional) To review a Reviewer's decision, select **View Activity** for the task.

28.2.5 Approving and Completing the Review

Review Owners can complete, terminate, review, or partially approve the decisions at any time during a review run. If you want to modify or remove a review item, all access change requests are sent to fulfillment, which is the step where approved changes are implemented. Review Owners can view fulfillment status for review items that generate a change request. The approval process allows the Review Owner to confirm the actions taken by all Reviewers. After approval, a review can be optionally routed to a Review Auditor for legal acceptance.

To approve and complete the review:

1. In Identity Governance, select **Reviews > Reviews**.
2. Select the active review that you want to manage.
3. Observe the actions taken by the Reviewers.
4. (Optional) Override actions as needed.

5 To approve the decisions made in the review run, select **Approve** next to a review item or select multiple review items and select **Actions > Approve**. Note that if you remove any time-based review items before the scheduled date, when you approve the items, the removal request for the items are retracted from the pending requests list under **Access Request** > **Request**.

6 (Optional) Add a comment.

7 (Conditional) If the review run included changes to user accounts, ensure that the affected data sources are collected and published.

After the administrator collects and publishes the data sources, Identity Governance updates the status of the fulfillment items.

28.2.6 Viewing Run History

Identity Governance tracks all the reviews and maintains a history of review runs associated with a review definition. The run history is searchable and sortable, and displays:

- Start and end date of a review run
- Status including certification percentage
- Review owner
- Name of the person who started the review on demand, on schedule, or by micro certification
- List of review items and associated actions including change reviewer and modify actions, and remove comments if any
- Fulfillment status of each review item for review runs once they are partially or fully approved, and then continues to be updated until the completion of the fulfillment process

To view the run history:

1 Select **Reviews > Definitions**.

2 Search for the review definition and click the review name, or directly click the review name.

3 Select **View run history**.

29 Instructions for Reviewers

Identity Governance collects information from different identity and application data sources and adds them to your environment for your business needs. However, these data needs to be periodically reviewed and verified, and as a Reviewer, Identity Governance allows you to do so. You can confirm whether permissions or membership granted to a user or account should be kept or removed or, in some cases, modified. You can also confirm or request modification of business role memberships, supervisor assignments, user identity attributes such as title, email, and location, and business role attributes such as risk.

This section provides instructions on the activities you can carry out as a Reviewer:

29.1 Performing a Review

As a reviewer you might be assigned to review items in multiple active review runs. Depending on how the review is defined, Identity Governance might send you email notifications to remind you of incomplete tasks and approaching deadlines. This section provides the steps required for you to complete Reviewer tasks associated with a review run.

For more information about the Reviewer’s authorization and the review process, see Chapter 27, “Understanding Review Run,” on page 349.

1. In Identity Governance, select **Reviews**.
2. (Optional) Click the gear icon to view additional column options and customize column display. For example, you can drag **Started by** to the list of selected columns to view name of the person who started the review on demand, on schedule, or by micro certification process.
3. Select the review run on which you want to act.
4. (Optional) Adjust display options to help you manage your review items:
   - **4a** (Optional) Select **Include submitted items** to see all review items on the list.
   - **4b** Click **Show all** to see a list of grouping options. The grouping options are especially helpful when you have a long list of review items.
   - **4c** (Optional) Select a grouping option to sort review items by groups and to easily take action on all or selected review items within a group.
   - **4d** (Optional) Enter a search string such as user name, specific review item, or decision to filter review items, and to easily take action on all or selected review items within the filtered list.
   - **4e** Click the gear icon to change the display options by adding, removing, or rearranging columns.

NOTE: For Technical Role and Business Role Definition reviews you can click the **Review technical role definition** and **Review business role definition** option to review the role definitions and save the proposed changes, sort the columns, undo or discard the changes.

5 For each review item, click the review item link to view additional details that could help you make your decision, then select an action. You can also select multiple review items across pages and use **Actions** to select an action.

NOTE: The review type and definition determines which of the following actions are allowed for a review instance.

- (Conditional) **Keep** to specify that you believe that the user should have the permission, account, or role.
- (Conditional) **Assign**, if there are unmapped accounts, to map the account.
- (Conditional) **Modify,** if the review definition allows this option, to change attribute value or to provide modification instructions such as account needs an account custodian.
- (Conditional) **Keep assignment** to specify that the user should have the previously assigned supervisor when reviewing direct reports.
- (Conditional) **Change supervisor** to specify that the user should have a different supervisor when reviewing direct reports.
- (Conditional) **Remove assignment** to remove the supervisor when reviewing direct reports
- (Conditional) **Remove** to specify that the user should not have the permission, account, or role. In case of time-based assignments for access, account, technical, or business role reviews, remove the assignments before the scheduled date.

  NOTE: If you remove the Global or Customer authorization from a user who is the last Global or Customer administrator, only the Bootstrap will have the ability to reassign this authorization.

- (Conditional) **Review user profile** to review user attribute values and either modify values and **Save changes** or confirm **No profile changes**.

  NOTE: You cannot modify attribute values in bulk.

- (Conditional) **Review business role definition** to review memberships, authorizations, or attribute values and **Save changes** or confirm **No changes**.
- **View Activity** to decide what actions to take or what actions have been taken.
- **Change Reviewer** to pass the decision to another reviewer.

  NOTE:
  - If the review definition states that the change reviewer action requires a comment, then you must enter a comment to complete the action.
  - If you select User B, who has a delegate User C who has a delegate User B, as the new reviewer, Identity Governance will issue a warning and disable the **Change Reviewer** option to prevent cyclical delegation.

- **Download all review items as CSV** to download all or a selective set of review items as a CSV file for manual review. You can selectively download review items by selecting a grouping option or searching for values for columns included in the **Review Settings > Review Display**

Customization menu. For example, if you want to review only items for one application, you can select Group by application. If you want to include items whose decision you had previously submitted, you can select the filter icon and include submitted items. Additionally, for account and user access review if you include permission assignment attributes, such as assignment value, risk, and generic attributes you can download them as CSV, if those columns are configured in Review Settings > Review Display Customization menu.

NOTE: ◆The download list items count will not match the actual number of review items in an Account Review that includes permissions. The count reflects the number of accounts that match the search criteria, however, all the permissions under each account will also be included in the download resulting in more items than the number displayed on the review page.

- The Current Assignment Details link displays the assignment value if collected. To view the assignment value from IDM application sources a Global or a Bootstrap Administrator must set the global property `com.netiq.iac.show.idm.assignval` to `true`.

---

6 Review the changes to ensure accuracy.

7 Select Submit to confirm your actions on the review items.

This action locks your decisions and moves the items out of your queue. Identity Governance then moves the items to the next reviewer's queue if this is a multistage review and you are not the last reviewer. If you are the last reviewer, Identity Governance notifies the Review Owner that the review is ready for certification.

If one of your review items is in the Multiple Reviewers queues, your decision gets locked in when you Submit the decision. If you have not yet submitted a decision and another reviewer makes a decision and submits before you, it is the other reviewer's decision that gets locked. You can select Include submitted items if not previously selected and see the decision in the View Activity option.

29.2 Viewing Completed Reviews

Review Auditors can only view the instance of a review after it is completed and is waiting on acceptance, and after accepting or rejecting the review instance. Reviewers and Review Owners can view the details of a review instance and review items even after the review instance is completed and, if required, accepted.

Select Show completed reviews to view a completed, and completed and accepted, or rejected review's start and end date, status including certification percentage, and review items that you submitted. Optionally, sort review items by decision, and select View Activity to view actions related to the review item, including change reviewer and modify reasons, if any.

30 Creating and Managing Certification Policies

Certification policies allow you to produce a comprehensive view of your organization's compliance with specific certification controls, such as Sarbanes-Oxley Act (SOX) or Health Insurance Portability and Accountability Act (HIPAA). A Customer, Global, Review, or Data administrator creates certification policies against review definitions and Identity Governance evaluates the review items and other criteria defined in the policy and reports violations. From the Governance Overview dashboard, Identities catalog, and Certification page, you can drill down to see specific violations to policies when they exist.

30.1 Understanding Certification Policies

Identity Governance enables organizations to easily manage multiple compliance processes as a cohesive certification policy. For example, if you are required to review all access to applications that process data related to SOX, you can create a certification policy which could include all related reviews, set a validity period for the policy, and then periodically view all SOX related violations or search for a specific violation related to user access, account access, permissions, or business or technical role memberships. Specifically, a certification policy, can enable organizations to:

- Consolidate reporting and audit queries
- Schedule when certification policy calculation will occur
- Calculate violations and determine compliance status
- Detect items that should be reviewed based on change events since previous review run. Change events could include changes to catalog, risk levels, or review definitions.
- View the status of all access review processes included in the policy
- Get a more comprehensive governance risk overview when risk levels have been configured, and weight and range has been set for certification policy violations related risk factors

30.2 Creating and Editing Certification Policies

NOTE: Reviews should be defined before creating a certification policy. For information about review definitions, see Chapter 26, “Creating and Modifying Review Definitions,” on page 343.

After creating review definitions, create certification policies that Identity Governance can use to alert you of possible compliance violations. When a review has been completed, you can view the list of violations.

1. Log in as a Customer, Global, Data, or Review Administrator.
2. Under **Policy**, select **Certification**.
3. Select **+** to create a certification policy.
4. Specify the name of the certification policy, validity period, and single or multiple review definitions.

   NOTE: Policy names must be unique. When Identity Governance checks for uniqueness, case is not considered. Therefore, Identity Governance considers Hippa and HIPPA to be equivalent.

   TIP: Click the search icon to select single or multiple review definitions. You can also enter wildcard * to search for reviews, or just start typing the review name to view suggestions.
5. (Optional) Set risk.
6. (Optional) Specify policy administrator.

   NOTE: Policy administrator role will be functional in a future release of Identity Governance. Currently, Customer, Global, Data, or Review Administrator can function as a policy administrator.
7. (Optional) If you want to prevent Identity Governance to calculate violations automatically, deselect **Run will be triggered by event** and **Run when policy is saved**.
8. Save your settings.
9. Under **Policy**, select **Certification** to view the newly created policy listed with number of violations.
10. (Optional) Select **Set Remediation** to select remediation action. For more information about setting remediation, see "Remediating Certification Policy Violations" on page 369.
11. (Optional) Select the policy, then select **Edit** to edit the policy.
12. (Optional) Select a specific policy or multiple policies, then select **Actions** to delete policies, calculate policy violations, run remediation, or export policies.

30.3 Scheduling Calculations and Calculating Certification Policy Violations

Identity Governance automatically calculates policy violations when:

- An certification policy is defined or modified
- Identity or data application is published
- Reviews included in the policy are completed

In addition, you can also schedule when certification policy violation calculations will occur when defining a policy. However, you will need to manually calculate policy violations after events such as partial reviews and expiration of the certification policy validity period.

NOTE: If certification policy violations and related risk factors are configured, Identity Governance risk scores will be impacted. Therefore, calculate certification policy violations before calculating risk scores. For information about risk scoring, see Chapter 22, “Calculating and Customizing Risk,” on page 285.

To schedule certification policy violation detection:

1. Log in as a Customer, Global, Data, or Review Administrator.
2. Under **Policy**, select **Certification**.
3. Select **Schedule** tab, add and remove policies to the schedule, and set the schedule.

   NOTE: By default, all certification policies will be included in the scheduled detection process. However, once you remove a policy from the schedule, Identity Governance will detect violations only for the policies included in the schedule. To detect violation of other policies you can either manually calculate policy violations or add the policy to the schedule.
4. Select **Active** and then select **Save** to activate the schedule.

To manually calculate policy violations:

1. Log in as a Customer, Global, Data or Review Administrator.
2. Under **Policy**, select **Certification**.
3. In the **Policies** tab, select the policy for which you want to calculate policy violations.
4. Select **Actions > Calculate Policy Violations**.

   NOTE: When a certification policy includes multiple review definitions, and when an entity is included in more than one review definition, then the certification status is defined based on the last review. You can cancel calculations in progress by selecting **Cancel** next to the progress status.

30.4 Exporting and Importing Certification Policies

Once you have created your certification policies based on your business requirements, you can easily export the certification policies, entities list, and related review definitions as a zipped file and save it with your backup files. You can also use exported policies in another location or environment. For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

30.5 Managing Certification Policy Violations

Identity Governance provides the ability for you to define certification policies so that the system can look for violations to the policies. You can view a summary of these violations and last and next calculation dates on the Governance Overview dashboard. You can view a detailed list of these violations on the **Certification** page by selecting the number of violations and if you have access to the catalog, on the **Catalog > Identities > *Name* > Certification** tab.

30.5.1 Understanding Violation Types

Identity Governance groups certification policy violations based on the cause of violation. All violations are calculated based on the review definitions included in a certification policy and the certification period. Certification period is based on the validity period you specify in the certification policy settings. Types of violations include:

- **No decision**: Review items that were included in a review during the certification period, but had no decisions made on them when the review ended
- **Expired**: Review items in a review whose certification period had expired
- **Expired with no decision**: Review items that had no decisions made on them during review runs and whose certification period has expired
- **Not reviewed**: Review items that should have been reviewed based on the specified review definitions, but were never part of any running review because the related review was not run or because there were changes to catalog, risk level, or review definition
- **Review in progress**: Review items that were in violation, but are now included in a review run that is in progress. You cannot set remediation for these review items

30.5.2 Searching for Specific Violations

Identity Governance provides expression builders that enable you to select catalog attributes and custom values as search criteria and save them as filters. You can use these filters to search for certification policies on the Certification page. For more information, see Chapter 5, “Using Advanced Filters for Searches,” on page 59.

For each certification policy that has violations, you can review details by selecting the number of violations. Selecting the number of violations opens a searchable and sortable panel of violations where the tabs are based on the review item selection criteria in the review definition. In each tab of the violations panel, you can search for the related entity and also search violations for a selected entity by user, account, permission, application, role, or business role. You can also sort your search results by selecting a column heading. For example, if you want to search No decision violations for a user who has been assigned to a specific account, specify the user name in the top level search in the User tab, select the user name to expand the search results and to specify account at the second level search, and then click on Violations column heading to sort the results by violation type.

Administrators can also view the last certification date of an identity and violation details if any by selecting the total number in **Catalog > Identities > *Name* > Certification** tab.

30.5.3 Remediating Certification Policy Violations

Certification policy violations can be addressed and resolved by:

- Sending an email notification
- Reviewing items in violation or in other words creating a micro certification or focused reviews
- Creating change request

Once a micro certification is complete or once a change request has been fulfilled, Identity Governance recalculates the number of violations automatically. For more information about micro certification and fulfillment, see Section 25.2, “Understanding Micro Certification,” on page 340 and Chapter 15, “Instructions for Fulfillers,” on page 175.

If after the initial remediation type selection, administrators would like to change the remediation type for future violations then they can select the link under Remediation column on the Certification page and edit the remediation setup.

To remediate certification policy violations:

1. Log in as a Customer, Global, Data, or Review Administrator.
2. Under **Policy**, select **Certification**.
3. Select **Set Remediation**.
4. Select **Remediation Type**.
   - **4a** If you selected **Email Notification**, select **Email source** and enter or search and select user or group as recipient of the email.
   - **4b** If you selected **Change Request**, select violation types, and provide instructions for fulfilling the change requests generated for selected violation types.
   - **4c** If you selected **Micro Certification**, configure the following settings:
     - **Review Definition**: Identity Governance selects the first review definition of the certification policy. Leave the default review definition as is or select a review definition from the drop down list if the policy has more than one review definition.
     - **Review Name**: Specify a name for the micro certification.
     - **Violation Type**: Select violation types based on which violations you want to review.
     - **Start Message**: Provide message that will be displayed in the header area of reviews describing why the review was started.
     - **Review Period**: Leave this blank if you want to use the duration specified in the review definition. Otherwise specify a duration.
5. Select **Run Remediation on new violations when calculated** check box to automatically run remediation after saving your remediation setup.
6. **Click** Save.
7. To run remediation on demand, select **Actions > Run Remediation**.

31 Analyzing Data and Using Custom Metrics

Identity Governance provides out-of-the box queries to analyze your data and gather metrics. Additionally, it enables authorized administrators to configure and customize analytics and metric definitions and create custom metrics.

31.1 Understanding Analytics and Role Mining Settings

Identity Governance provides access to the Analytics and Role Mining Settings menu based on your authorization. Authorized users can use these settings to enable and disable decision support, configure business role mining settings, create custom metrics, and collect and schedule metrics collection.

31.1.1 Understanding Role Mining Settings

Roles in governance systems enable administrators to simplify security administration on systems and applications, by encapsulating popular sets of entitlements and assigning them as packages, rather than individually, to users. Identity Governance uses attributes specified in **Configuration > Analytics and Role Mining Settings** to provide recommendations for creating business roles. If the specifications do not meet certain conditions administrators may not see any recommendations when mining for roles. Only a Global, Data, or Business Roles Administrator can configure the role mining settings.

When specifying attributes make sure that:

- Specified attributes have values. User attributes with zero strength will not be displayed in the directed mining recommended attribute bar graph or visual attribute map.

In addition, in order for visual role mining to render recommendations make sure that:

- At least two attributes are selected. For example, “Title” and “Department”.
- Selected attributes share commonality. For example, departments A, B, and C have users with the same titles, such as Administrative Assistant and Department Lead.

NOTE: After customizing attributes, select **Business Role Mining metrics** and collect metrics to refresh data.

31.1.2 Understanding Metrics

Identity Governance tracks activities and key risk indicators so that authorized administrators can monitor activities and risk factors in your governance system and make improvements based on the collected metrics. The activities and key risk factors or facts extracted and collected from various data sources and user and entity events are stored in fact tables that are then used to calculate metrics and the results (metric tables) are published to the default or administrator-specified database.

Identity Governance default metrics analyze common risk factors and enable you to find answers for questions like how many average number of users are in an account, how many accounts are unmapped, and what proportion of your entitlements are assigned by policies versus assigned directly. Administrators cannot edit the default metrics but can view associated description and metric columns by selecting the metric name.

In addition to default metrics, authorized administrators can create custom metrics, using SQL statements and insight queries, to adjust metric calculations based on your business needs. For example, you can create a custom metric for calculating how many role policies are active. You can download custom metric definitions and import them.

Administrators can also download all metric results. You must collect metrics before downloading the results. All available metric results are not downloadable. You cannot download metrics if they were collected from a remote database. Role mining metrics are also not downloadable as they are only for use by internal processes.

The default schedule for all metric calculations is 24 hrs. Administrators can change the metric calculation schedule and set a start date for metric calculations by selecting **Actions > Set collection schedule**. Though Identity Governance allows administrators to schedule the collection of metrics, collections might be delayed because Identity Governance manages the number collections running concurrently to optimize performance. Some collections scheduled to run might be delayed until other collections have completed. Identity Governance also delays scheduled calculations after initial startup of the Identity Governance server.

Administrators can control how many metric collection can be collected simultaneously by using the Identity Governance Configuration Utility to configure `com.netiq.iac.fact.collection.thread.pool.size`. Currently, if an administrator chooses to run more than five metric collection then the first five collections will run simultaneously and the other collections will be queued and will run after the previous one finishes calculations. We recommend that administrators override the default 5 setting to a lower number if they observe metric collections impacting the system adversely. For more information about the Configuration Utility, see "Using the Identity Governance Configuration Utility" in the *Identity Governance 4.3.1 Installation and Configuration Guide*.

31.1.3 Understanding Supported Storages and Data Types

You can store metrics data in Identity Governance databases, Vertica, Oracle, PostgreSQL, Microsoft SQL Server (MS SQL), or Kafka. Identity Governance enables you to select generic data types and translates them to a specific data type based on the type of storage as shown in the table below.

NOTE: Identity Governance publishes facts to Kafka as JSON strings.

Data Type	Read from `igops` as	Published to Vertica as	Published to IG PostgreSQL as	Published to IG Oracle as	Published to IG MS SQL as
Boolean	BOOLEAN	BOOLEAN	boolean	number	bit
Long	INTEGER	INTEGER	integer	number	integer
Float	FLOAT	FLOAT	float	float	float
String	STRING	LONG VARCHAR	text	nclob	nvarchar(max)
Date	TIMESTAMP	TIMESTAMP WITH TIME ZONE	TIMESTAMP WITH TIME ZONE	TIMESTAMP WITH TIME ZONE	TIMESTAMP WITH TIME ZONE

31.2 Configuring Analytics and Role Mining Settings

Based on their business needs, authorized administrators can configure analytics, customize decision support visibility and role mining detection, create custom metrics, run metric calculations on demand, and download and import custom metrics in order to optimize your governance system.

To configure analytics and role mining settings:

1 Log in as a Global, Data, or Business Roles Administrator.

NOTE: A Business Roles Administrator does not have the same access permissions as a Global or Data Administrator, and can only configure role mining settings and collect business role mining metrics.

2 Select **Configuration** > **Analytics and Role Mining Settings**.

3 (Optional) Under **Decision Support**, specify if the following information is excluded or included in the guidance provided to reviewers, review owners, review administrators, and access approvers.

3a Deselect **Show business role authorization status** if business roles are not used or if the reviewer or access request approver does not need guidance about whether the review or request item was authorized by a business role.

3b Deselect **Show similarity statistics in reviews and access requests** if the reviewer of user reviews or access request approver does not need guidance about how many users have similar permissions.

3c Deselect **Show login statistics for review item users and accounts** if `Last Login` and `Number of Logins` attributes are not configured/collected/logged for the users and accounts.

3d Deselect **Show review list statistics** if the review related authorized user wants to hide the review item's prior completion details, such as date of completion, name of the review run that included the review item, and decision made about the review item.

4 (Optional) Under **Similarity Profile**, select additional attributes to use in the similarity profile so that Identity Governance can provide decision support.

TIP: Use wildcard * to search for attributes.

5 Under **Role Mining**:

5a Specify the maximum number of results that should be returned when mining business roles using the directed role mining approach.

5b Specify which additional user attributes should be used for both directed and visual business role mining. For more information about which attributes to select, see "Understanding Role Mining Settings" on page 371.

6 Specify the number of hours to retain the mining suggestions before they are deleted.

7 Select **Save** to save all the settings.

8 (Optional) Next to **Metrics Collection**, click the **+** icon to create custom metrics. For more information, see Section 31.1.2, "Understanding Metrics," on page 372 and "Creating Custom Metrics" on page 377.

9 Under **Metrics Collection**, select one or more items, and then specify **Actions > Set collection interval** to change the default setting of 24 hours between metrics collections or disable collection.

TIP: Click on an item name to view detailed information about the metric, including list of metric columns' aliases and corresponding data types.

10 Specify start date, time, and hours or deselect the **Active** check box to disable collection.

11 Click **Save**.

12 (Optional) Select one or more items and then select **Actions > Collect metrics** to initiate a metrics collection on demand.

TIP: Always collect metrics after a collection and publication to refresh charts on the Governance Overview dashboard and after modifying role mining settings to refresh business role mining related metrics.

13 (Optional) When a custom metric collection is running and you want to cancel it:

13a Select the item or items with an asterisk (*), and then select **Cancel Collection**

13b Click **Cancel Collection** to confirm the cancellation.

14 (Optional) Select one or more default and custom metric items and then select **Actions > Download Metrics** to download the metric results in CSV format.

NOTE: In addition to downloading the results, you can also download custom metric definitions and import them. For more information, see "Downloading and Importing Custom Metric Definitions" on page 379.

31.3 Configuring Metrics Data Stores for Custom Metrics

Identity Governance allows a Global Administrator or Data Administrator to define data storage locations to reference when creating custom metrics collections. In addition, metrics data stores allow you to easily create multiple metrics collections that use the same metrics data store.

NOTE: Metrics collections can use the same metrics data store, but if the data store is a database, each metrics collection using that data store must specify a different database table.

Identity Governance allows you to configure the following data store types:

- Local Database (Identity Governance databases)
- Vertica
- Kafka
- Oracle
- PostgreSQL
- MS SQL

Before you create a custom data store type, create a database schema that includes a new database and table for the data store you want to create.

31.3.1 Before You Create a Metrics Data Store Using SSL Communication

If you want to create a metrics data store and configure the database to use SSL communication, you must first create and configure the proper global configuration properties for your data store type and for the SSL type -- server authentication or mutual authentication. Use the table below to determine which configuration properties you need to create and the values for each.

Table 31-1 *Global Configuration Properties and Value Types for Data Store and SSL Types*

Data Store Type/SSL Type	Configuration Property	Value Type
Vertica/Server	com.netiq.iac.vertica.ssl.truststore.path	Filename
Vertica/Server	com.netiq.iac.vertica.ssl.truststore.password	Password
Vertica/Mutual	com.netiq.iac.vertica.ssl.truststore.path	Filename
Vertica/Mutual	com.netiq.iac.vertica.ssl.truststore.password	Password
Vertica/Mutual	com.netiq.iac.vertica.ssl.keystore.path	Filename
Vertica/Mutual	com.netiq.iac.vertica.ssl.keystore.password	Password
Oracle/Server	com.netiq.iac.oracle.ssl.truststore.path	Filename
Oracle/Server	com.netiq.iac.oracle.ssl.truststore.type	Type of truststore
Oracle/Server	com.netiq.iac.oracle.ssl.truststore.password	Password
Oracle/Mutual	com.netiq.iac.oracle.ssl.truststore.path	Filename
Oracle/Mutual	com.netiq.iac.oracle.ssl.truststore.type	Type of truststore
Oracle/Mutual	com.netiq.iac.oracle.ssl.truststore.password	Password
Oracle/Mutual	com.netiq.iac.oracle.ssl.keystore.path	Filename

Data Store Type/SSL Type	Configuration Property	Value Type
Oracle/Mutual	com.netiq.iac.oracle.ssl.keystore.type	Type of truststore
Oracle/Mutual	com.netiq.iac.oracle.ssl.keystore.password	Password
PostgreSQL/Server	com.netiq.iac.postgres.ssl.root.cert	Contents of the certificate **NOTE:** Do not use a filename.
PostgreSQL/Mutual	com.netiq.iac.postgres.ssl.root.cert	Contents of the certificate **NOTE:** Do not use a filename.
PostgreSQL/Mutual	com.netiq.iac.postgres.ssl.client.cert	Contents of the certificate **NOTE:** Do not use a filename.
PostgreSQL/Mutual	com.netiq.iac.postgres.ssl.client.key	Contents of the key **NOTE:** Do not use a filename.
MS SQL/Server	com.netiq.iac.mssql.ssl.server.cert	Contents of the certificate **NOTE:** Do not use a filename.
MS SQL/Server	com.netiq.iac.mssql.ssl.password	Password

Use the information from this table to create and configure the required configuration properties for the metrics data store you want to create.

NOTE: The configuration properties required for SSL communication could already exist in your environment. You can select **Configuration** > **Advanced**, then use the search feature to verify whether the configuration property you need is already configured as a global configuration setting.

To create and configure the proper global configuration properties for your data store type and for the SSL type:

1. Log in as a Global Administrator.
2. Select **Configuration** > **Advanced**.
3. Next to **Global Configuration Settings**, click the plus sign (+).
4. Type the name of the configuration property you want to create, then click **Add**.
5. Type the value for the configuration property you want to create, then click **Create**.
6. Perform Step 3 through Step 5 for each property you need to create.

31.3.2 Creating a Metrics Data Store

To create a metrics data store:

1. Log in as a Global or Data Administrator.
2. Select **Configuration** > **Analytics and Role Mining Settings**.
3. Next to **Metrics Data Stores**, click +.

4 Provide the requested Metrics Data Store Details.

5 Provide the configuration information for the selected data store type.

NOTE: If you select Kafka as the data store type, you must click **Import Kafka Configuration**, and then browse to select a JSON file that contains configuration information. You can click the "?" icon to view sample code you can copy and paste into a text editor to modify and create a JSON properties file.

---

6 Click **Test Connection** to verify your settings.

7 Click **Save**.

31.4 Creating Custom Metrics

In addition to default metrics, Identity Governance provides the ability to query your operations database for additional statistics that could help you to better monitor the health of your governance system. The product also displays an asterisk (*) in front of the names of the custom metrics to distinguish them from default metrics. You can click the metric name to view the details of the metric.

To create a custom metric:

1 Log in as a Global or Data Administrator.

2 Select **Configuration** > **Analytics and Role Mining Settings**.

3 Next to **Metrics Collection**, select the **+** icon and select **New.**

4 Specify a name for the new metric.

5 Optionally, select an existing category or create a custom category by selecting **Add Custom**.

6 Type a short description for the metric.

7 (Optional) Select **Allow use in governance widgets** to enable the custom metric results to be displayed as a custom widget on the Governance Widgets page.

8 Click **Storage**, select a data store to publish the custom metric results, and then provide additional location information as required. For a Kafka data store, you must specify a topic. All other data store types are databases, which require a table name. The metrics will collect into the table you specify. For example, for large volume analytics you could define a metrics data store for your Vertica or Kafka database, select that data store for your metric, and then specify a table name or a topic name to store the metrics.

NOTE: If you select a metrics data store that is a Local Database type, Identity Governance collects your metric to a table in the Identity Governance ARA database. In this case you do not have to specify a table name.

If you do not specify a table name, Identity Governance creates a table with `ex_randomGUID` naming convention. However, it is recommended that you provide a meaningful table name.

---

9 (Conditional) If you select to store the metric in Vertica, specify the schema name in **Table** before the table name and separate these with a comma.

10 Click **SQL Statement** and enter a SQL select statement. For example, to calculate how many role policies are active enter `select count(id) as active from role_policy where state = 'ACTIVE'`.

NOTE: Identity Governance automatically checks for statement errors and potential SQL injections to prevent invalid or malicious code. However, ensure that you have defined your query correctly, since you cannot edit saved custom metrics. If needed, you will have to delete the custom metric, and then create a new one to change your definition.

11 Specify an alias and type for each column selected in the SQL statement.

11a Click **Metric Columns**.

11b Click **Add Column** and specify an alias and type for each column selected in the SQL statement. When specifying an alias:

- Do *not* use SQL reserved keywords as an alias for a custom metric column. Using a reserved keyword as a column name will cause an error. If, for example, you use `"end"` as an alias name in your custom metric definition when Identity Governance is connected to a PostgreSQL database, the PostgreSQL client will display the following error message:

  ```
  Fact validation failed: Unable to create table. Verify there are no reserved SQL keywords used as column aliases. ERROR: syntax error at or near "end" Position: 150.
  ```

  SQL reserved keywords vary based on the database. Refer to your database documentation for a list of database-specific reserved SQL keywords.

- For timeline, bar chart, and donut widgets, specify type as `Long`. In addition, for timeline specify `String`. For example, `select ds.name application, count(ds.name) as appcount from cert_policy_violation cpv left join data_source ds on ds.unique_id = cpv.unique_application_id and ds.data_source_type='APPLICATION' and ds.deleted=false group by ds.name.`

- Ensure that the alias in **Metric Columns** and the SQL query match. For example, add metric column `active` with a type of `Long` for the SQL statement example in Step 10 on page 377.

11c Repeat the above step to add more columns.

11d Address any metric column section warnings that appear.

NOTE: Creating a metric with a warning might not work correctly.

12 Select **Save**.

To create a custom metric from an Insight Query:

1 Log in as a Global or Data Administrator.

2 Select **Configuration** > **Analytics and Role Mining Settings**.

3 Next to **Metrics Collection**, select the **+** icon and select **New from Insight Query**. For information about creating insight queries, see Section 12.5, “Analyzing Data with Insight Queries,” on page 134.

4 Select the Insight Query to use, and then select **Add**.

5 Specify a name for the custom metric and adjust any other settings, including those populated based on the Insight Query and storage settings for metrics.

6 Select **Save**.

After creating custom metrics, you can collect them on demand by selecting one or more custom metrics and then selecting **Actions > Collect metrics**. In addition, you can also select **Actions > Delete Custom** to delete custom metrics.

31.5 Downloading and Importing Custom Metric Definitions

In addition to creating a new custom metric using SQL statements or by using an Insight query, Identity Governance provides you the ability to download custom metric definitions so that you can edit and import them.

For more information about exporting and importing procedures and recommended order of import, see Chapter 33, “Exporting and Importing,” on page 387.

32 Monitoring Your Governance and Administration System

Identity Governance provides out-of-the-box widgets and dashboards to monitor key aspects of your identity governance and administration system. Authorized users can:

- View out-of-the-box governance widgets and dashboards
- Create new widgets and dashboards
- Personalize dashboards

Use the following information to create and manage the Identity Governance widgets and dashboards accessible from the **Overview** menu.

In addition to the Governance Overview dashboard, authorized users may view the Workflow dashboard. Click the Home icon on the top right corner of the main navigation bar and select **Workflow Dashboard** to view the dashboard. Click the Home icon on the Workflow dashboard to navigate back to Identity Governance. For information about the Workflow dashboard, see “Exploring your Dashboard” in the *Workflow Administration Guide*.

32.1 Understanding the Governance Widgets and Dashboards

The Governance Overview dashboard provides an overview of real-time adaptive statistics related to the governance system. Global Administrators, Data Administrators, and other authorized users can access the Governance Overview dashboard to monitor:

- Data collection statistics and data summary
- Risk scores
- Policy status and violation trends
- Mapped and unmapped accounts related statistics

- Role effectiveness and number of entitlement assignments via roles versus direct assignments
- Activities statistics and trends

Identity Governance groups the out-of-the-box dashboard widgets by Data, Risk, Policy, Account, Activity, and Role types. You can perform many different actions to customize the dashboard and widgets for your organization. You can:

- Rearrange or hide the default tabs
- Resize and move widgets within each default tab
- Save the new tab order and widget layout as a local user preference
- Save the new tab order and widget layout as the new default setting
- Restore the default view
- Create new widgets and dashboards

You cannot add or remove widgets from the default tabs. Some timeline widgets on the default tabs display a settings icon, and allow you to click the settings icon to view the legend for the widget and specify the values you want the timeline widget to display.

Governance widgets display your governance status and metrics in respective areas. *To view the content on the Governance Overview dashboard, users must have the appropriate access authorization, and administrators must have completed the required tasks.* For example, Auditors have read-only access to the Governance Risk Score widget whereas Global Administrators and Data Administrators can edit the risk score configuration and calculate risk scores.

32.2 Creating New Governance Widgets

Identity Governance uses widgets to display content in the dashboard. Authorized users can create widgets that allow the Identity Governance dashboard to display custom metrics.

NOTE: Before creating a new widget, you must create a custom metric and enable its results to be displayed as a widget.

To create a new widget:

1. Log in as a Global or Data administrator.
2. Select **Overview > Governance Widgets**.
3. Click **+**.
4. Provide a name and a description.
5. Select an available metric type.
6. Select a chart type.
7. Provide the requested information for the selected chart type.

   NOTE: Identity Governance uses the values and labels you provide as data types in the widget legend.

   ---

8. Save the widget.

32.3 Downloading Custom Governance Widget Data

In addition to creating new widgets to discover custom metric results, Identity Governance enables authorized users to download the related chart as a PDF file and data as a CSV file.

To download widget data:

1. Log in as Global or Data administrator.
2. Select **Overview > Governance Widgets**.
3. Access the dashboard that includes the custom widget whose data you want to download.
4. Navigate to the custom widget chart.
5. Click the Chart icon to save the chart as PDF.
6. Click the Download icon to download data to a CSV file.

32.4 Creating and Personalizing Governance Dashboards

Identity Governance uses widgets to display content in the dashboard. Authorized users can personalize the out-of-the-box dashboards or create new dashboards that display content from provided widgets, or custom widgets created by your organization.

You can move and resize the widgets in a dashboard to customize the dashboard layout. If the widget is a custom widget, and that widget contains a large number of data types, resizing the widget and moving the placement of the legend may be necessary to display all the data and the complete legend.

To create a dashboard:

1. Log in as a Global or Data administrator.
2. On the Governance Overview page, click the plus sign (+).
3. Type a name and description for the new dashboard.
4. Click the gear icon.
5. Select default or custom widgets you want to add to the dashboard.
6. (Optional) To customize the settings of a custom widget added to your dashboard:
   - **6a** Click the gear icon in the custom widget.
   - **6b** To configure the widget to display a time stamp, click **Show Timestamp**.
   - **6c** To configure the widget to display the chart legend, click **Show Legend**.
   - **6d** (Conditional) If the widget is a bar or timeline chart, select the position in the widget for the legend.
   - **6e** (Conditional) If the widget is a bar or donut chart, select the series and size.
7. Click **Apply**.
8. Click **Save**.

To personalize a dashboard:

1. Log in as a Global or Data administrator.

2 Click the folder icon on the Governance Overview dashboard to perform any of the following actions:

- Add and remove tabs.
- Drag and drop to rearrange dashboard tabs.
- On each tab, click the corner of a widget and drag to resize the widget.
- On each tab, use the Rearrange icon on the upper-right corner of the widget to drag and drop the widgets to other positions on the dashboard.

3 Click **Save**, and specify whether to save the dashboard in your settings, or to save as a default for all users.

TIP: To clear preferences, on the title bar, select ***your name*** **> Clear Preferences**.

To reset to default view:

1 Log in as a Global or Data administrator.

2 On the Overview page, click on the folder icon next to the page title.

3 Click on the restore icon on the settings panel upper-right corner.

4 To retain your local customized view and reset the global default view for all other users, click **Restore configuration and keep my local settings**.

5 To reset your view to the global default view, click **Reset my view to global default**.

NOTE: You can also reset your view and all other users' view to the global default, by clicking on your user name on the upper-right corner of the application title bar, then using respective My Settings menu options.

32.5 Viewing Data Collection Statistics and Summary

Requires collection from data sources and publication to the Identity Governance catalog.

On the Data tab of the Governance Overview dashboard, the Global Administrators, Data Administrators, and Auditors can view data collection statistics such as the number of identity and application sources and collection schedules in the Data Collection widget on the Data tab. They can also select the sources and schedules to configure application sources and collection schedules. For more information, see Chapter 8, "Collecting Applications and Application Data," on page 95 and Chapter 10, "Creating and Monitoring Scheduled Collections," on page 109.

In addition to the collection statistics, administrators can also view the total number of identities, groups, permissions, permission assignments, applications and accounts in the Data Summary widget. The Data Summary widget displays only the number of objects that are visible in the catalog. You can view this data as a bar chart, and authorized users can select a parameter to view the respective catalog details.

NOTE: View the **Data Sources > Activity** page for the actual number of collected or published data objects that include objects that are not visible in the catalog. You can also use the page to compare the collections or publications from two different times.

32.6 Viewing Governance Risk Score

Requires risk level and score configuration and risk calculation.

On the Risk tab of the Governance Overview dashboard, Global Administrators, Data Administrators, and Auditors can view the Governance, User, and Application risk score and the risk score over a period of time. To change the default time range, log in as one of the authorized administrators, select the calendar icon, then select dates. For more information about risk score calculations, see Chapter 22, “Calculating and Customizing Risk,” on page 285.

32.7 Viewing Policies and Controls Status, Violations, and Trends

Requires definitions of Certification, Data, and Separation of Duties (SoD) policies and reviews.

On the Policy tab of the Governance Overview dashboard, administrators such as the Global, Separation of Duties, Review, and Data Administrator can view the respective SoD, Certification, and Data policy violation statistics. They can also For more information, see Section 20.3, “Creating and Editing Separation of Duties Policies,” on page 268, Section 30.2, “Creating and Editing Certification Policies,” on page 365, and “Creating and Editing Data Policies” on page 115.

The Policy Violation widget of the Governance Overview dashboard displays the Violation detection type results collected by the Policy Violation Metrics. It provides a summary of Data, SoD, and Certification policy violations.

The Policy Event widget of the Governance Overview dashboard displays the Event detection type results collected by the Policy Event Metrics. It provides an overview of data policy detections such as number of users without supervisors that were detected by policy events such as publication, collection, or entity curation.

Change the default date range on the trends widgets to view violation and event trends based on the custom date range. On policies widgets, click **View Policies** to view details about the various policies. On the Policy Violation by Type widget, select a violation type, then click the number of violations to view the list of violations.

32.8 Viewing Account Statistics and Other Details

Requires account collection from application data sources and publication to the Identity Governance catalog.

On the Account tab of the Governance Overview dashboard, administrators can view a summary of the account statistics. The administrators can also view the summary details of the account statistics, such as the total number of accounts and unmapped account percentage for the system. To see results, administrators must collect and publish data sources and then collect metrics on-demand or wait for 24 hours, the default metrics collection interval.

To get the results for a specific time range, log in as one of the authorized administrators and change the default time range. To further customize the results based on risk levels, select the gear icon next to the widget title, then click on one or more risk levels to view or hide the related results on the chart.

NOTE: To keep statistics up to date, the administrators must collect metrics after every publication.

32.9 Viewing Entitlement Assignments Statistics to Leverage Roles

To view the entitlement assignment statistics, your system must include business roles.

On the Role tab of the Governance Overview dashboard, Global, Data, and Business Roles Administrators can view the Role Leverage widget to understand how entitlement assignments conform to business policies. The widget includes a graphical overview of the effectiveness of roles for a length of time, entitlements assignments using roles versus entitlements assigned directly, and the ratio of indirect role-based entitlements versus total entitlement assignments in percentage.

To change the default time range, log in as one of the authorized administrators, select the calendar icon, then select dates. To refresh the graphs, collect metrics for business role mining after publishing new business roles. Based on these metrics, you can then lower the risk by using role mining to create more roles. For more information, see "Creating and Defining Business Roles" on page 236.

32.10 Viewing Activity Statistics and Trends

To view activity statistics, your system should have auditing enabled and collected activity and entity usage statistics metrics.

On the Activity Statistics tab of the Governance Overview dashboard, Customer Administrators, and Auditors can view daily, weekly, monthly, or custom date range Identity Governance activities when authorized users have previously enabled auditing and collected activity usage statistics and entity usage statistics metrics.

By default, authorized users can view overall usage, summaries, and top five activities based on the selected date range and last collection. The top five activities are selected based on the total number of activities within the selected date range. The top five activities will change if the selected date range is changed.

Customer Administrators can also add other activity widgets by adding and removing specific activities from the Activity Statistics dashboard selection panel. For example, an administrator can select certification policy violation detection activity. Click the gear icon to view the list of activities and select one or more activities. Each newly added activity generates a timeline and a summary widget.

33 Exporting and Importing

Identity Governance facilitates businesses to become more resilient by enabling authorized users to easily migrate data, such as policies, roles, and settings from one environment to another using export and import options. Authorized administrators can use the export and import capabilities when upgrading Identity Governance, recovering from a disaster, or testing policies and settings in a stage or test environment, then migrating that data into a production environment. The required authorizations, export and import procedures, order of import, and import flow differ based on the functional area and business needs.

IMPORTANT: When you are upgrading your application or migrating your entire system, we recommend that you work with key stakeholders and administrators to formulate a suitable plan. Start with exporting data from all functional areas, copy information if needed from areas that you cannot download, delete schema and logs, then import data, settings, and policies.

For more information about Identity Governance import and export capabilities and procedures, see the following sections:

33.1 Understanding File Formats and Import Flows

Previous versions of Identity Governance supported the export and import of data related to various functional areas in CSV, JSON, XML, or ZIP format. The current release provides an enhanced export and import capability including export and import of data as a ZIP file containing a single SQLite database file. If you need to open the SQLite database file, you will need to use a database browser application.

If necessary, you can edit the exported files, then import them. However, we recommend that if you need to make any changes to the data, you make the changes using the user interface options, then export. If you choose to edit the files manually, proceed with caution. When you import manually edited files, Identity Governance will not import the file if the edits are not done correctly or if the file is not in the expected format.

When you import data, you either directly import a file (basic import flow) or use an enhanced import flow that enables you to upload, then preview and search imported data. In the enhanced import flow, by default Identity Governance automatically refreshes the imported data when the import process detects a change in the system that affects the loaded import file. For example, during technical role import, if Identity Governance detects any change in the system because of an application publication that leads to changes in permissions, or if any technical role is modified,

added, or deleted, then Identity Governance automatically refreshes the imported data. If you want to disable the automatic refresh behavior, change the default value of the `com.netiq.iac.importExport.refreshPrompt` property using the Advanced Global Configuration menu.

Though the enhanced export and import capability supports compressed SQLite file as the export format, you can continue to import CSV, JSON, or ZIP files exported from previous versions of Identity Governance.

33.2 Exporting and Downloading Data

Downloaded data format and procedures vary based on the type of data you have. You can export data from functional areas in any order. Depending on the type of data, you can additionally download references such as references to business or technical roles, or associated applications.

To enable you to continue performing tasks even as the entities are being downloaded, Identity Governance saves the file to a download page from which you can download the saved file at a later time. The download page enables you to search for a file by description or download type (typically, the page where the user initiated the download). You can also use search strings to search for a file. You can delete downloaded files manually or allow them to expire on the date displayed in your Downloads window. You can delete all files individually or in bulk.

To export and download data:

1. Log in to Identity Governance.
2. Navigate to the respective page.
3. Click the download link or select the appropriate action. For more information, see Section 33.6, “Exporting and Importing Quick Reference,” on page 393.
4. Type a meaningful filename and select **Download**.
5. Select the download icon on the top title bar to access the saved file and download the file.
6. (Optional) Delete the file from the Download area. If you do not delete the file, the file will be automatically deleted based on your download retention setting.

33.3 Prerequisites for Importing Data

Before importing data, ensure that you have exported the data sources, policies, or configurations that you want to move to another system, and have downloaded the exported files to your local computer. For those areas that you cannot export, take screenshots and record the details in a planning worksheet. Also, be aware of the importance of the order in which you import data.

After exporting, prepare your environment for import, using the following steps, then start importing in the recommended order.

To prepare your system for imports:

1. Stop all Tomcat instances.

2 Delete localhost from the following locations:

- **Linux**: `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- **Windows**: `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`

3 Delete all files and folders from the temp directory in the following locations:

- **Linux**: `/opt/netiq/idm/apps/tomcat/temp`
- **Windows**: `C:\netiq\idm\apps\tomcat\temp`

4 Delete or move out all the log files from the following locations:

- Linux: `/opt/netiq/idm/apps/tomcat/logs`
- Windows: `C:\netiq\idm\apps\tomcat\logs`

5 Have the DBA delete all the ID Gov schemas.

NOTE: You do not have to delete the IGRPT schema.

---

6 Have the DBA create the ID Gov schemas either:

- With the same password as described in Configuring the Oracle Database for Identity Governance in the Identity Governance 4.3.1 Installation and Configuration Guide.

  Or

- Run the `dbtool-create-log.txt` file located in one of the following directory of the primary node:
  - **Linux :** `/opt/netiq/idm/apps/idgov/logs`
  - Windows: `C\netiq\idm\apps\idgov\logs`

7 On the primary node, navigate to the `/opt/netiq/idm/apps/idgov/bin` or C:\netiq\idm\apps\idgov\bin directory and run the following command. Make sure that you are using the same password that you have used for all the ID Gov schemas.

```
/db-init.sh -password password 2>&1 | tee -a recreate-schema.log
```

Once you run the command, you will be able to see the output in your Linux terminal or Windows and it will also be captured in the file.

8 On the primary node, navigate to the /opt/netiq/idm/apps/idgov/logs or C\netiq\idm\apps\idgov\logs directory perform the following steps:

8a Copy the actual command (after Command:) from the `dbtool-rptuser-log.txt`.

8a1 Replace *xxx* for the real password and execute the command

This will create the necessary igrptuser and grant the correct view rights on the views in the IGOPS schema.

8b Copy the actual command (after Command:) from the `config-init-log.txt`.

8b1 Replace *xxx* for the real password and execute the command.

This will import the default global properties back into the IGOPS schema.

9 Start the primary tomcat.

During the start-up of this node, the base data load will occur and default data will be added into the necessary tables.

10 Once Tomcat has fully started login as the Bootstrap user.

11 Extract the Identity and Application Source zip files that were previously exported and start importing based on the recommended order of import.

33.4 Recommended Order of Import

When you are importing, you might choose to import respective functional area settings and definitions or might need to work with a Bootstrap, Global, or Customer administrator to import all settings and definitions. In any case, being aware of your data relationships and planning your imports can save you time and prevent errors. For example, to avoid error conditions and text with strikeouts, you must import identities before importing global authorizations.

The ability to import and export varies according to your authorization. To check who is authorized to export and import, see Section 33.6, “Exporting and Importing Quick Reference,” on page 393.

Note that you might not always need to import all exported files. For example, if you did not add a custom attribute or modify a default attribute, you need not import the respective attribute file.

As a best practice, we recommend that you import data in the following order and adjust your import plan based on your governance needs and environment.

Log in as a Bootstrap administrator:

1. Select **Data Administration > Identity Attributes**, then import identity attributes.
2. Import account, permission, group, business role, application, and permission assignment attributes.
3. Select **Data Source > Identities**, then import identity data sources. For each source, test the connection, then test collection for 10 users. When successful, perform a full collection, then publish.
4. Select **Data Source > Application**, then import application data sources starting with IDM AE Permission collector. For each source, test the connection, then test collection for 10 users. When successful, perform a full collection, then publish.
5. Select **Configuration > Authorization Assignments**, then import the authorization assignments.
6. Select **Configuration > General Settings**, then add the URL to Identity Reporting or import the settings.
7. Select **Fulfillment > Configuration**, and on the Fulfillment Targets tab, edit the Manual fulfiller and set a User or Group. Save your changes.
8. Import any previously exported Fulfillment targets and add the necessary passwords.
9. Select **Fulfillment > Configuration**, and on the Application Setup tab, update the application Sources to utilize the necessary Fulfillment Targets.

After successful collection and publication of application sources, log in as a Global or any other authorized administrator, import in the following order:

1. Select **Policy > Coverage Maps**, then import coverage maps.
2. Select **Policy > Delegation**, then import delegation mappings.
3. Select **Policy > Risk**, then import Risk settings.

4. Select **Catalog > Roles**, then import technical roles. Review and fix any items that have strikethroughs, and activate roles as needed.
5. Select **Policy > Business Roles**, then import business roles. Review and fix any items that have strikethroughs, and publish business roles as needed.
6. Select **Policy > SoDs**, then import SoDs. Review and fix any items that have a red strikethrough. Activate the necessary SoDs.
7. Select **Policy > Inconsistency Resolution**, then import auto-resolution policies.
8. Select **Reviews > Definitions**, then import review definitions. Review and fix any items such as permissions, accounts, and review owners that have red strikethroughs.
9. Select **Policy > Certifications**, then import.
10. Select **Data Administration > Policies and Controls**, then import data policies.
11. Select **Policy > Access Request Policies**, then import request policies and request approval policies. Review and fix any items that have strikethroughs, and activate policies as needed.
12. Select **Catalog > Permissions**, then select a permission and import custom forms.
13. (Conditional) If you had exported schedules, import schedules. If not, recreate them.
14. Import any other items that were exported, such as dashboards and insight queries.
15. Select **Configuration**, then import advanced Settings and logging levels or change them as needed.

33.5 Importing Data

When you import data, Identity Governance uses either the basic import flow (directly importing a file) or the enhanced import flow (uploading, filtering, and refreshing data before importing). In both cases, Identity Governance enables you to select the entities to import, import references, and resolve conflicts. For example, during an import, if Identity Governance detects a technical role with the same name but a different unique ID, then Identity Governance shows the technical role as a conflict. You can either replace the existing technical role with the same name or create a new one.

The enhanced import flow does not yet work for all data related to functional areas. Currently, you can use the enhanced export and import flow to import the following:

- Advanced Settings except environment-specific ones
- Analytics and Role Mining Settings
  - Decision Support
  - Similarity Profile
  - Role Mining
- Audit Settings
- Authorization Assignments
- Categories
- Certification Policy Schedules
- Collection Schedules
- Data Policy Schedules
- Delegation Mappings

- Download Settings
- Fulfillment Context Attributes
- General Settings
- Logging Levels
- Maintenance Schedules
- Risk Policies
- Risk Schedules
- Technical Roles

Your import selections are maintained until the import file is deleted or expires. However, if you import the same file, Identity Governance sets a new expiration date.

When Identity Governance uses the basic import flow, if you import more than the preconfigured threshold for the number of roles or policies that can be displayed on the import page or if the import fix size exceeds the preconfigured threshold, Identity Governance switches to bulk import mode. In bulk mode, instead of selecting whether to create, update, or handle conflicts for specific roles or policies, Identity Governance prompts you to import all new roles and policies and update all existing roles and policies. For conflicts, you can choose to either overwrite existing roles or create new roles.

NOTE: In basic import flow, the default value for roles and policies that can be displayed is 200. However, you can change the default value using the `com.netiq.iac.importExport.maxImportsToDisplay` property. Use the Advanced Global Configuration menu to add the property and specify a new value.

Identity Governance does not switch to the bulk mode when it uses the enhanced import flow because Identity Governance supports paging in the enhanced import flow and can display more than 200 roles or policies. In enhanced import flow, you can continue to selectively create, update, or handle conflicts as needed.

Sometimes reimporting previously deleted roles and policies might fail soon after cleanup. For example, when business roles, SoD policies, technical roles, applications, or review definitions are exported, deleted, and later reimported and the cleanup operation purges the deleted business roles, SoD policies, technical roles, applications, or review definitions before they are reimported, you might get an error in the UI during the reimport process, depending on how soon after the purge the reimport takes place.

The server log would contain an ERROR (SEVERE) message that corresponds to the error message in the UI. The wording of the message will be different depending on the database platform, but in general the message will indicate that an insert or update into the auth_role_mapping table violated the fk_auth_scope_id foreign key constraint. When you see this kind of error, we recommend that you wait at least 10 or 15 minutes and then try to reimport again.

To import:

1. (Conditional) If you are importing more than one file, create a plan for import based on the recommended order of import.
2. Log in to the application as the authorized user.

3 Navigate to the appropriate page and click the import link. For more information, see Section 33.6, “Exporting and Importing Quick Reference,” on page 393 for details on importing policies or settings.

4 (Conditional) If Identity Governance prompts you to open a file (basic import flow), navigate to the local folder on your computer where your downloaded file is located, then click **Open**.

NOTE: Identity Governance does not upload a file that does not match the expected name. For example, if you are importing a business or technical role but select an SoD policy file an error will be displayed.

---

5 (Conditional) If Identity Governance prompts you to load a file:

5a Click **Upload Import**.

5b Navigate to the local folder on your computer where your downloaded file is located, then click **Open**.

5c Click the Import icon next to the file you want to import to start the import process.

5d (Optional) Enter a search string to filter the import items, then take action on all or selected items within the filtered list. Identity Governance persists selections across pages if you have a long list of items, as long as the imported file is not deleted or has not expired.

6 Review data and resolve conflicts.

7 (Optional) If you want to preview and analyze the import data, select **Generate Report**.

8 Select the items for import and then select **Import**.

This automatically generates a CSV report that you can download and review. This import report identifies what was imported and calls out any unresolved references.

TIP: At times, the list of import items can span multiple pages. The **Select All** option in the **Actions** menu enables you to select all the import items. If you selected all items and then decided to select only a few items to import, click **Actions > Select None** to remove selection from multiple pages, then select only the items that you want to import.

33.6 Exporting and Importing Quick Reference

The following tables list the required authorizations, navigation path, and high-level steps to export and import policies, roles, and settings. Note that the order in which you export or import will differ depending on your governance needs and environment.

- Section 33.6.8, “Exporting and Importing Review Definitions Related Data,” on page 401
- Section 33.6.9, “Exporting and Importing Analytics-Related Data,” on page 402
- Section 33.6.10, “Exporting and Importing Logging Levels, Categories and Settings,” on page 403

33.6.1 Exporting and Importing Data Sources and Related Data

Identity Governance enables you to download and import entity attributes, data sources, and catalog entities from one environment to another. However, certain conditions and constraints might apply to import capabilities. When importing catalog entities, if there is a conflict between the imported custom attribute data type and the attribute data type in the target system, you will not be able to import the custom attribute. For example, if you edited a custom attribute data type in your staging environment, exported the attribute, then attempted to import it in your production environment, the import will fail. This is because Identity Governance does not support attribute data type change during import or after collection.

To export and import	Log in as	Navigate to	Click the link or select the action
Attributes as a JSON file	Global, Customer, Business Role, Technical Role, or Data Administrator **NOTE:** Business Role Administrator can export and import only Business Role attributes.	**Data Administration** > ***Attributes*** where attributes are: ◆ Identity ◆ Account ◆ Permission ◆ Group ◆ Business Role ◆ Application ◆ Permission Assignments	**Download Attributes** **Import Attributes**
Identity data sources as JSON files	Global, Customer, or Data Administrator	**Data Sources > Identities** Select an identity source, then select **Test Collection and Troubleshooting** > **Download and Emulation**	**Download Data Source Configuration** **Import an identity source**
Application data sources as JSON files	Global, Customer, or Data Administrator	**Data Sources > Applications** Select an application source, then select **Test Collection and Troubleshooting** > **Download and Emulation**	**Download Data Source Configuration** **Import an application source**
Identities merge rules as a single JSON file	Global, Customer, or Data Administrator	**Data Sources** > **Identities**	**Export merging rules** **Import merging rules**

To export and import	Log in as	Navigate to	Click the link or select the action
Application collector as a JSON file	Global, Customer, or Data Administrator	**Data Sources** > **Application**	Expand the collector view, then click **Export** **Import collector,** but before importing, you must create an application source and save it.
Application definition as a JSON file	Global, Customer, Bootstrap, or Data Administrator	**Data Sources** > **Application Definitions**, select an application definition source, then select **Test Collection and Troubleshooting** > **Download and Emulation**	**Download Data Source Configuration** **Import an application definition source**
Data source templates as JSON files	Global, Customer, or Data Administrator	**Configuration** > ***Templates*** where templates are: ◆ Identity Source Collector Templates ◆ Application Source Collector Templates ◆ Application Definition Source Collector Templates	**Actions** > **Download** **Actions** > **Add new template**
Maintenance schedules as SQLite database files	Global, Customer, and Maintenance Administrator	**Data Administration** > **Maintenance** > **Maintenance Schedules**	**Export Schedules** **Import Schedules**
Data policies as JSON files	Global, Customer, or Data Administrator	**Data Administration** > **Policies and Controls**	**Actions** > **Export Data Policies** **Import Data Policies**
Data policy schedules as SQLite database files	Global, Customer, or Data Administrator	**Data Administration** > **Policies and Controls** > **Schedule**	**Export Schedule** **Import Schedule**
Collection schedules as a SQLite database file	Global, Customer, or Bootstrap Administrator	**Data Sources** > **Schedules**	**Export Schedules** **Import Schedules**

To export and import	Log in as	Navigate to	Click the link or select the action
Catalog entities as a CSV file	Global, Customer, Access Request, Data, Business Role, Auditor, Security Officer, Review, Technical Role, or Separation of Duties Administrator	**Catalog** > ***Entities*** where entities are: ◆ Identities ◆ Accounts ◆ Groups ◆ Applications ◆ Permissions	**Download all as CSV**
Email notification templates as XML files	Global, Customer, or Bootstrap Administrator	**Configuration** > **Notification Emails**	**Download XML** **Import XML**

33.6.2 Exporting and Importing Authorization Assignments and General Settings

To export and import	Log in as	Navigate to	Click the link or select the action
Global authorizations as SQLite database files	Global, Customer, Bootstrap Administrator, or Security Officer	**Configuration** > **Authorization Assignments**	**Export Assignments** **Import Assignments**
General settings as SQLite database files	Global, Customer, or Bootstrap Administrator	**Configuration** > **General Settings**	**Export General Settings** **Import General Settings**

33.6.3 Exporting and Importing Fulfillment-Related Data

To export and import	Log in as	Navigate to	Click the link or select the action
Fulfillment context attributes as SQLite database files	Global, Customer, Bootstrap, or Fulfillment Administrator	**Configuration** > **Fulfillment Context Attributes**	**Export Context Attributes** **Import Context Attributes**
Fulfillment target as a single JSON file	Global, Customer, or Fulfillment Administrator	**Fulfillment** > **Configuration**	Select a fulfillment target, then select **Download Fulfillment Target** **Import a fulfillment target**

To export and import	Log in as	Navigate to	Click the link or select the action
Fulfillment target templates as JSON files	Global, Customer, or Data Administrator	Configuration > Fulfillment Target Templates	Actions > Download Actions > Add new template
Email notification templates as XML files	Global, Customer, or Bootstrap Administrator	Configuration > Notification Emails	Download XML Import XML

33.6.4 Exporting and Importing Risk Policies and Schedules

To export and import	Log in as	Navigate to	Click the link or select the action
Risk policies and schedules as SQLite database files	Global, Customer, Bootstrap, or Data Administrator **NOTE:** Bootstrap Administrator can export only risk policies.	Policy > Risk	Export Risk Policies Import Risk Policies

33.6.5 Exporting and Importing Technical and Business Roles and Related Data

When you import technical roles, Identity Governance detects whether you are importing new or updated roles and whether the updates would create any conflicts or have unresolved references. For unresolved technical roles, where a match for the referenced object is not available in the system, Identity Governance adds an indicator. Importing before the roles are resolved will result in incomplete roles with some missing permissions. If an indicator appears next to a role in the import view, inspect these roles and ensure that they map properly in the target system.

NOTE: After importing technical or business roles, you must activate or publish them before they take effect in the system. Also, Identity Governance must recognize the users that hold the permissions as members of a technical role. For more information, see Section 18.8, “Activating Technical Roles,” on page 222.

When you import technical roles as a JSON or ZIP file that is exported from a previous version of Identity Governance, Identity Governance will utilize the enhanced import process to import the file.

When you import a business role, if that role references a technical role that is deactivated, then Identity Governance displays a warning. You can choose to activate the technical role and import, or continue with the import without activating the role. If you select the latter, Identity Governance ignores the reference to the inactive role but allows you to activate the role later and include it in the policy.

To export and import	Log in as	Navigate to	Click the link or select the action
Technical role definitions as SQLite database files	Global, Customer, Bootstrap, or Technical Role Administrator **NOTE:** A Bootstrap administrator can export only technical role definitions.	**Catalog** > **Roles**	**Actions** > **Download Definitions** **Import Technical Roles**
Lists of Technical roles as CSV files	Global, Customer, Bootstrap, or Technical Role Administrator **NOTE:** A Bootstrap administrator can export only technical role definitions.	**Catalog** > **Roles**	**Actions** > **Download all as CSV**
Business role definitions as a JSON file	Global, Customer, or Business Role Administrator	**Policy** > **Business Roles**	**Actions** > **Download Definitions** **Import Business Roles**
List of Business roles as a CSV file	Global, Customer, or Business Role Administrator	**Policy** > **Business Roles**	**Actions** > **Download all as CSV**
Business role approval policies as a single JSON file	Global, Customer, or Business Role Administrator	**Policy** > **Business Roles** > **Approval Policies**	**Download Definitions** **Import Approval Policies**
List of Business role inconsistencies as a CSV file	Global, Customer, or Business Role Administrator	**Policy** > **Business Roles** > **Manage Inconsistencies**, then click on number of inconsistencies	**Actions** > **Download**
Auto Inconsistency Resolution policies as SQLite database files	Global, or Customer	**Policy** > **Inconsistency Resolution** > **Auto Resolution Policies**	**Import Auto Resolution Policies** **Actions** > **Download**
List of Auto Inconsistency Resolution policy related business role inconsistencies as a CSV file	Global, or Customer	**Policy** > **Inconsistency Resolution** > **Auto Resolutions**, then click on inconsistencies count	**Download**

To export and import	Log in as	Navigate to	Click the link or select the action
Analytics and role mining settings as an SQLite database file for: ◆ Decision support ◆ Similarity Profile Attributes ◆ Role Mining	Global, Customer, Bootstrap, Business Role, Technical Role, or Data Administrator **NOTE:** A Technical Role Administrator can export and import decision support and role mining settings.	**Configuration** > **Analytics and Role Mining Settings**	**Export Analytics Settings** **Import Analytics Settings**
Email notification templates as XML files	Global, Customer, or Bootstrap Administrator	**Configuration** > **Notification Emails**	**Download XML** **Import XML**

33.6.6 Exporting and Importing Separation of Duties Related Data

When you import SoD policies, if that policy references a technical role that is deactivated, Identity Governance displays a warning. You can choose to activate the technical role and import, or continue with the import without activating the role. If you select the latter, Identity Governance ignores the reference to the inactive role but allows you to activate the role later and include it in the policy.

To export and import	Log in as	Navigate to	Click the link or select the action
SoD policies as JSON files	Global, Customer, or Separation of Duties Administrator	**Policy** > **SoD**	**Actions** > **Download Definition** **Import Separation of Duty Policies**
SoD approval policies as JSON files	Global, Customer, or Separation of Duties Administrator	**Policy** > **SoD Approval Policies**	**Actions** > **Download Definition** **Import SoD Approval Policies**
Email notification templates as XML files	Global, Customer, or Bootstrap Administrator	**Configuration** > **Notification Emails**	**Download XML** **Import XML**

33.6.7 Exporting and Importing Access Request Related Data

When you download forms, the JSON file contains both request and approval form data because the request and approval forms need corresponding controls to facilitate data flow. When you import forms, you can preview the forms and compare the previous form with the imported form and revert if required. To use the imported form, you must publish it. Note that, for default forms, you must select an application or permission to preview the imported forms.

When you import new access request policies, if that policy references a technical role that is deactivated, Identity Governance displays a warning. You can choose to activate the technical role and import, or continue with the import without activating the role. If you select the latter, Identity Governance ignores the reference to the inactive role but allows you to activate the role later and include it in the policy.

NOTE: When you download approval policies for access requests, the associated assignments for the policy are also included in the download file.

To export and import	Log in as	Navigate to	Click the link or select the action
Default forms as a single JSON file	Global, Customer, or Access Request Administrator	**Policy** > **Access Request Policy** ◆ **Application Default Forms** ◆ **Permission Default Forms**	**Download Forms** **Import Custom Forms**
Custom forms as a single JSON file for applications and permissions	Global, Customer, Access Request Administrator, or Application Owner	**Catalog** > **Applications** > ***Application Name*** > **Custom Forms** Or **Catalog** > **Permissions** > ***Permission Name*** > **Custom Forms**	**Actions** > **Download Forms** **Import Custom Forms**
Assignments	Global, Customer, or Access Request Administrator	**Policy** > **Access Request Policy** > **Approval Policies** Edit the policy, then select: ◆ **Approval Process** ◆ **Applications** ◆ **Permissions** ◆ **Roles**	**Import Assignments**
Workflows or forms	Global, Customer, or Workflow Administrator	Workflow Administration Console > **Catalog** ◆ **Forms** ◆ **Workflow**	Export and import workflows Export and import forms

To export and import	Log in as	Navigate to	Click the link or select the action
Coverage maps as a JSON file	Global, Customer, Bootstrap, Access Request, or Review Administrator	**Policy** > **Coverage Maps**	**Actions** > **Export Coverage Maps** **Import Coverage Maps**
Delegate mappings as a SQLite database file	Global, Customer, or Data Administrator	**Policy** > **Delegation**	**Download mappings** or **Actions** > **Download mappings** **Import Delegate Mappings**
Access requests as a single JSON file	Global, Customer, or Access Request Administrator	**Policy** > **Access Request Policies**	**Import Access Request Policies**
Access request approval policies as a single JSON file	Global, Customer, or Access Request Administrator	**Policy** > **Access Request Policies** > **Approval Policies**	**Actions** > **Download Definitions** **Import Access Request Approval Policies**
List of access request approval policies as a CSV file	Global, Customer, or Access Request Administrator	**Policy** > **Access Request Policies** > **Approval Policies**	**Actions** > **Download all as CSV**
Email notification templates as XML files	Global, Customer, or Bootstrap Administrator	**Configuration** > **Notification Emails**	**Download XML** **Import XML**

33.6.8 Exporting and Importing Review Definitions Related Data

Remediation settings such as email recipients and review definitions can be resolved when a certification policy is imported or it can be resolved manually after import. So, to avoid umapped errors when you are importing, extract the files, import the review definitions, then import the certification policy.

Importing review definitions may also result in unresolved references when matching criteria is not collected. To avoid these errors, make sure the global import and export (`com.netiq.iac.importExport`) settings have been configured correctly. For more information about changing configuration settings, see Section 4.3, “Changing Advanced Configuration Settings,” on page 45.

NOTE: Identity Governance uses an existing coverage map, and automatically resolves coverage map references. If a coverage map does not exist, Identity Governance creates one.

To export and import	Log in as	Navigate to	Click the link or select the action
Review definitions as JSON files	Global, Customer, or Review Administrator	**Reviews** > **Definitions**	**Download Definitions** **Import Review Definitions**
Reviewers and review item lists as CSV files	Global, Customer, or Review Administrator	**Reviews** > **Reviews** > ***review name***	**Download reviewers**
Delegate mappings as a SQLite database file	Global, Customer, or Data Administrator	**Policy** > **Delegation**	**Download mappings** or **Actions** > **Download mappings** **Import Delegate Mappings**
Coverage maps as a JSON file	Global, Customer, Bootstrap, Access Request, or Review Administrator	**Policy** > **Coverage Maps**	**Actions** > **Export Coverage Maps** **Import Coverage Maps**
Certification policies as a JSON file	Global, Customer, Data, or Review Administrator	**Policy** > **Certification**	**Action** > **Export Policies** **Import Certification Policies**
Certification schedules as SQLite database files	Global, Customer, Data, or Review Administrator	**Policy** > **Certification** > **Schedule**	**Export Schedule** **Import Schedule**
Email notification templates as XML files	Global, Customer, or Bootstrap Administrator	**Configuration** > **Notification emails**	**Download XML** **Import XML**

33.6.9 Exporting and Importing Analytics-Related Data

Identity Governance provides ability to define queries and metrics to analyze your governance system.

To improve download speed of insight queries CSV file, the default value of `com.netiq.iac.ui.insightQuery.download.results.pageSize` configuration property is set to 1000. For more information about changing configuration settings, see Section 4.3, “Changing Advanced Configuration Settings,” on page 45.

To export and import	Log in as	Navigate to	Click the link or select the action
Metric results as a CSV file	Global, Customer, or Data Administrator	**Configuration** > **Analytics and Role Mining Settings**	**Actions** > **Download Metrics**
Custom metric definition as a JSON file	Global, Customer, or Data Administrator	**Configuration** > **Analytics and Role Mining Settings**	**Actions** > **Download Definition** **Import Custom Metrics**

To export and import	Log in as	Navigate to	Click the link or select the action
Insight queries as a single JSON file	Global, Customer, Auditor, Data, or Governance Insights Administrator	**Catalog** > **Governance Insights**	**Actions** > **Download Queries** **Import Insight Queries**
Insight query results as a CSV file	Global, Customer, Auditor, Data, or Governance Insights Administrator	**Catalog** > **Governance Insights** then select the query	**Download results of insight query as a CSV file**
Custom governance widget data as a PDF or a CSV file	Global, Customer, or Data Administrator	**Overview** > **Governance Widgets**	**Download chart as PDF file** **Download data as CSV file**
Audit settings as SQLite database file	Global and Bootstrap Administrator	**Configuration > Audit Enablement**	**Export Audit Settings** **Import Audit Settings**

33.6.10 Exporting and Importing Logging Levels, Categories and Settings

You can directly import categories or use the entity import feature to import entities with category reference.

To export and import	Log in as	Navigate to	Click the link or select the action
Categories as SQLite database files	Global, Customer, or Bootstrap Administrator **NOTE:** Bootstrap Administrator can export only categories.	**Configuration** > **Categories**	**Export Categories** **Import Categories**
Logging Levels as SQLite database files	Global, Bootstrap, and Administrator	**Configuration** > **Logging Levels**	**Export Logging Levels** **Import Logging Levels**
Download settings as SQLite database files	Global, Customer, Bootstrap, or Data Administrator	**Configuration** > **Download Settings**	**Export Download Settings** **Import Download Settings**
Advanced settings (except for environment variables) as SQLite database file	Global and Bootstrap Administrator	**Configuration** > **Advanced**	**Export Advanced Settings** **Import Advanced Settings**