NetIQ® Identity Governance

Administrator Guide

June 2019

Legal Notice

Contents

About this Book and the Library

The *Administrator Guide* provides conceptual information about the NetIQ Identity Governance product. This book also provides step-by-step guidance for administrative tasks.

Intended Audience

This book provides information for a variety of users involved in collecting, reviewing, and updating identities, accounts, and analytics in your environment:

Identity architect

Design a catalog of identities that can merge attributes from multiple sources of identity data, such as applications and LDAP directories. Help with the initial set up and configuration of the catalog, data sources, and identity mapping.

Data administrator

Create identity and application sources in the Identity Governance catalog that correlate with existing sources in the organization. Configure and run governance insight queries. Configure roles and security for Identity Governance. Help business administrators and application owners to create scheduled collections and reviews. Set up manual or automated fulfillment workflows. Perform data maintenance tasks including archiving and data cleanup.

Business administrator

Collect and publish identity and application data for review. Manage business roles and permission assignment based on the roles.

Application owner or supervisor

Review identity and application data to ensure that users have only the access that they need to accomplish their assigned functions.

Auditor

Verify that changes to identities have been fulfilled and that users have only the access that they need.

Other Information in the Library

The library provides the following information resources in addition to this guide:

Release Notes

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

Installation Guide

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

User Guide

The User Guide provides a step-by-step guidance for NetIQ Identity Governance user-oriented tasks. Specifically, it provides instructions for the following Identity Governance users:

- Access requesters
- Access Request approvers
- Reviewers
- Review owners
- Fulfillers

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. For more information, see *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide*.

Technical References

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

Videos

Provide supplemental information about using Identity Governance. For more information, see the NetIQ Youtube site (https://www.youtube.com/user/netiqTV).

1 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.

1.1 Understanding Authorizations in Identity Governance

Identity Governance relies on authorizations to define a fixed set of authorizations and permissions. 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 1.1.1, “Global Authorizations,” on page 11.
- **Runtime authorizations** are those that users assume as needed during an access review and validation cycle. 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 1.1.2, “Runtime Authorizations,” on page 14.

NOTE: When you install Identity Governance, use the bootstrap administrator authorization to collect and publish an initial set of identities. You can then use these identities as authorized users for Identity Governance and assign authorizations to them. 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 “Instructions for Access Requesters and Approvers” in the *NetIQ Identity Governance User Guide*. For more information about the bootstrap administrator, see “Understanding the Bootstrap Administrator for Identity Governance” in the *NetIQ Identity Governance Installation Guide*.

1.1.1 Global Authorizations

After collecting and publishing an initial set of identities, assign the Global Administrator authorization to one of these identities. Then the Global Administrator can assign the rest of the global authorizations. For more information, see Section 1.3, “Assigning Authorizations to Identity Governance Users,” on page 17.

Global Administrator

The Global Administrator is the primary authorization and can:

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

Access Request Administrator

The Access Request Administrator manages defining 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

Auditor

The Auditor has read-only rights to the catalog, reviews, separation of duties policies and violations, business roles, risk, certification policy, fulfillment status, and the **Overview**. However, this authorization can configure and run insights 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 1.1.2, “Runtime Authorizations,” on page 14.

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 business role schema under **Data Administration**
- 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

- 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 in the **Overview**
- Perform data maintenance tasks including archiving and data cleanup

Governance Insights Administrator

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

- Configure and run governance 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

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 or live mode
- Modify a review schedule
- Assign delegates for users
- Assign all the runtime authorizations as part of a review, thereby delegating certain rights pertaining to the review to those authorizations
- View running reviews
- View data summary and system trends in the **Overview**
- View the **Catalog** but cannot modify it

Technical Roles Administrator

The Technical Roles Administrator mines for technical role candidates, creates and manages 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 in the **Overview**
- 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.

1.1.2 Runtime Authorizations

Assign runtime authorizations when you need them. For more information, see Section 1.3, “Assigning Authorizations to Identity Governance Users,” on page 17.

Access Requester

Access Requesters request application access, permissions, and technical role (previously labeled as access profile) assignment. Identity Governance Access Request Administrator and Global Administrator define the Access Request policy that specifies who can request access, what can they request for, 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.

Application Owner

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

- View the catalog
- Perform data editing for assigned applications
- Review data and access within the assigned applications, depending on selections 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 clean-up, or editing, for all assigned applications. This authorization can:

- Modify the configuration of a data source
- Execute collections for the data source
- 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

Business Role Owner

The Business Role Owner can review a business role and potentially approve a business role depending on whether or not 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 14, “Creating and Managing Business Roles,” on page 137.

Business Role Manager

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

- Edit the 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 Administrator 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

For more information about assigning an escalation reviewer in a review definition, see Section 10.9, “Specifying Reviewers,” on page 119.

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 authorization 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 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 campaign. 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 review status in **Overview**
- View **Quick Info** details about a catalog item

- View fulfillment status of a review item
- View 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 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
- Edit review decisions before submitting them

For more information about assigning reviewers, see Section 10.9, “Specifying Reviewers,” on page 119.

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

1.2 Adding Identity Governance Users

Until you collect data for your Identity Governance users, no one can log in to the application without using the bootstrap administrator account. Do not use the bootstrap administrator after you add your Identity Governance users to the Identity Governance attribute catalog and assign global authorizations to the users. For more information about the bootstrap administrator account, see “Understanding the Bootstrap Administrator for Identity Governance” in the *NetIQ Identity Governance Installation Guide*. For more information about mapping attributes, see Section 7.1, “Configuring the Data Source for Post Authentication Matching,” on page 67.

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, global or data administrator account.
2. In the **Data Sources**, select **Identities**.
3. Under **Identity Sources**, select the LDAP authentication server that you 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 3.3, “Creating Identity and Application Sources,” on page 40.

   ---

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 4, “Creating and Monitoring Scheduled Collections,” on page 51.

5 When collection is completed, select the icon for **Publish identities now**.

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

   For more information, see Section 1.3, “Assigning Authorizations to Identity Governance Users,” on page 17.

1.3 Assigning Authorizations to Identity Governance Users

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

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

Authorization	Assignment Method	Assigned By
Technical Role Owner	Technical role definition	Technical Roles Administrator or Global Administrator

1.4 Using Coverage Maps

In review definition and approval policy, administrators can select coverage maps to specify:

- Reviewers of a **User Access** or **Account Review** definition
- Approvers for requested access in the **Request** application

Coverage maps are CSV files with header and criteria cells. 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 via entity-entity relationships

It is important to have an understanding of Identity Governance supported coverage map types, keywords, syntax, and enitity-entity relationships in order to create and load coverage maps.

- Section 1.4.1, “Creating Coverage Map,” on page 18
- Section 1.4.2, “Loading Coverage Map,” on page 22

1.4.1 Creating Coverage Map

To create a coverage map, create a CSV file with header and criteria cells. For greater flexibility use only keywords.

- “Supported Coverage Map Types and Keywords” on page 18
- “Supported Syntax” on page 19
- “Supported Relationships” on page 20
- “User Access Review Coverage Map Examples” on page 20
- “Account Review Coverage Map Examples” on page 21
- “Access Request Coverage Map Example” on page 22

Supported Coverage Map Types and Keywords

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

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

Supported Syntax

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>`

NOTE: 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 that have 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

The system evaluates date types in comparisons using ISO 8601 date and time format. The following are some examples of January 31, 2017:

- 2017-01-31
- 2017-01-31T10:00Z
- 2017-01-31T10:00-05:00

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

Supported Relationships

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

Find below the supported predefined relationships:

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)
`REVIEW` and `REQUEST`	`applicationOwners`	`owner`	`USER`
`REVIEW` and `REQUEST`	`applicationOwners`	`groupOwner`	`GROUP`
`REVIEW` and `REQUEST`	`PERMISSION`	`permissionOwners`	`resolved_spermission_owner` (table)
`REVIEW` and `REQUEST`	`resolved_spermission_owner`	`owner`	`USER`
`REVIEW` only	`ACCOUNT`	`accountHolders`	`saccount_user` (table)
`REVIEW` only	`saccount_user`	`holder`	`USER`
`REVIEW` only	`ACCOUNT`	`accountOwners`	`resolved_saccount_owner` (table)
`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`

NOTE: Any of the relationships that resolve to a table would need another segment to resolve to an `ENTITY`. For example, `APPLICATION.applicationOwners` is incomplete, since 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. Once a review item matches, the example uses the `displayName` attribute from the `User` entity to select a reviewer.

All of 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 both the permission's 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 row is the header 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 that are not members of the Finance department. The fourth row assigns Henry Morgan as reviewer for users that are members of a department.

During coverage map processing, a matching row is searched for in the order they appear in the CSV file. Once a match has been 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 will be 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 uses a simpler format by using only keywords, and the first criteria row uses relationships to assign reviewer. Note that the `ReviewItem` is referenced within the `Reviewer` criteria cells. For users under review that are in the Transportation or Tours department, reviewer is assigned based on the location of the supervisor of the user

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 headers 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.supervisorUniqueId"
```

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

1.4.2 Loading Coverage Map

To load coverage map:

1. Log in to Identity Governance as a Global or Data Administrator.
2. Select **Configuration**.
3. Select **Coverage Maps** to expand the section.
4. To add a new coverage map:
   - **4a** Select **+**.
   - **4b** Select coverage map type: **REVIEW** or **REQUEST**.
   - **4c** Specify coverage map name and description.
   - **4d** Browse for the coverage map CSV file.
   - **4e** Select **Save**.
5. Repeat the above steps to upload additional coverage maps.
6. To preview the map, select the number of segments.
7. To modify a coverage map:
   - **7a** Select the coverage map.
   - **7b** Browse for a different CSV file.
   - **7c** Select **Open** to upload and replace the selected CSV file.
8. To delete a coverage map, select **Delete**.

NOTE: Only coverage maps not in use can be deleted.

---

2 Customizing 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.

2.1 Customizing the 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 has been 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.

You can also customize the product name in email notifications to brand it for your organization instead of the default name of NetIQ Identity Governance. To change the product name, run the Identity Governance Configuration Utility, and specify the product name you prefer on the **Identity Governance Server Details** tab. For more information, see Appendix A, “Running the Identity Governance Configuration Utility,” on page 191.

For information about configuring Identity Governance to send email notifications, see Configuring the Mail Server for Notifications. For information about Review related notifications, see “Setting Up Review Notifications” on page 106.

2.1.1 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 in 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. (Conditional) To customize all email templates in a single file, under **email templates (all languages)**, select **Download**.

   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.

   ---

4. (Conditional) To customize email templates for specific functional areas, such as Bulk Data or Business Role Approval, next to **View functional areas by**:
   - **4a** Select **Email Name**.
   - **4b** Select an email name, such as **Bulk Data Update Performed** from the list of functional areas.

     TIP: Click an email name and then select **Email source preview (en)** to view the template. Specify an email address to **Send notification preview**.

   - **4c** Select **Download** to download the email template for the languages for your locale.
5. 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 appropriately if you change the code strings incorrectly. For descriptions of the email tokens, see “Email Tokens” on page 24.

   ---

6. Save and close the files.
7. To submit the modified files, select the **Upload** icon next to **email templates (all languages)**.
8. Select **Save**.

Email Tokens

When customizing emails be careful in handling the tokens. Some email templates expect only certain processing tokens. Therefore, the product might not be able to replace a token with a value in some situations. In these situations, the template contains blank values when unexpected tokens are present. Notifications sent during review preview mode that enable administrators and review owners to preview notifications, might also 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

Token	Notes
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
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.

2.1.2 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 base64encode website or similar encoders to encode the image.

2. Download 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 file.

2.2 Customizing the Collector Templates for Data Sources

Usually, a collector template 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 for specifying 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 Global or Data administrator.
2. Select **Configuration**.
3. Expand the **Identity Source Collector Templates** or **Application 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** Select **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, complete the following steps:
   - **6a** Select the template that you want to disable.
   - **6b** Select **Disable**.

2.3 Customizing 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. To customize your categories offline and upload them in bulk, you can export a JSON file, edit it, and import it to modify categories and category assignments.

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. (Optional) 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**.
   - **4d** Each entity type with that category assigned now has a tab on the **Category** window. From this window you can remove the category assignment, if needed.
5. Select **Save** and then close the window.
6. To edit categories in bulk, select **Export Categories** and save the JSON file.
7. After you have edited the file, select **Import Categories** to import the file.

2.4 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 "Stopping, Starting, and Restarting Tomcat" in *NetIQ Identity Governance Installation Guide*.
2. Launch the Identity Governance Configuration utility in console mode. For examples, see Appendix A, "Running the Identity Governance Configuration Utility," on page 191.
3. Specify suppress commands for the emails you want to disable as shown in the following examples.

   WARNING: Disabling review notifications will be a global change and will be 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 follow these steps:
     - **3a1** Enter `dc com.netiq.iac.reviews.suppressReviewTerminationEmail`. No value should be returned.
     - **3a2** Enter `sp com.netiq.iac.reviews.suppressReviewTerminationEmail true`.
     - **3a3** Press Up-arrow two times so that the dc command is active.
     - **3a4** Press Enter. You should see `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 follow these steps:

3b1 Enter `dc com.netiq.iac.reviews.fulfillment.suppressLosingPermissionEmail`. No value should be returned.

3b2 Enter `sp com.netiq.iac.reviews.fulfillment.suppressLosingPermissionEmail true`.

3b3 Press Up-arrow two times so that the dc command is active.

3b4 Press Enter. You should see `com.netiq.iac.reviews.fulfillment.suppressLosingPermissionEmail = true`.

4 Exit the console mode.

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

6 Start Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" in *NetIQ Identity Governance Installation Guide*.

2.5 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.

Extending the schema is adding attributes to the default schema provided. You can view the default schema for Identity Governance in the console. You login as an global administrator or data administrator to view the schema. The schema is listed under the **Data Administration** menu.

- Section 2.5.1, "Adding or Editing Attributes to Extend the Schema," on page 28
- Section 2.5.2, "Adding Attributes to a Collector," on page 30
- Section 2.5.3, "Viewing Available Attributes in Business Roles," on page 31

2.5.1 Adding or Editing Attributes to Extend the Schema

Identity Governance provides a simple way to extend the schema for the different entities. You 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 on 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**

NOTE: You cannot extend the schema for groups. Identity Governance does not allow it.

---

3 Select the plus sign **+** to add a new attribute or select an existing attribute to edit the properties.

4 Add or edit the attribute by configuring the following:

NOTE: Some values might not be editable, depending on the Attribute Behavior settings.

Attribute name and Key

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

Type

Select the type of attribute you want to create. The types are **String**, **Boolean**, **Double**, **Long**, **Date**, and **Locale**.

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 this is not enabled, and the value is longer than the maximum size, it will cause an error and the record will not be 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 the Identity Governance Console.

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.

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
- Available in typeahead searches

IMPORTANT: For all attributes that you have configured for authentication matching rules, ensure that you enable the following list and search options for these attributes:

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

For more information, see “Security Settings” on page 193.

5 Select **Save**.

2.5.2 Adding Attributes to a Collector

If a collector you are using does not contain the schema you need, you can simply extend the schema of the collector by adding additional attributes. You must have already created and configured the collector before performing the following steps. For more information, see Chapter 3, “Creating and Managing Data Sources,” on page 33.

1 Log in to Identity Governance as a Global Administrator.

2 Select **Data Sources** > **Identities** > ***Your Identity Source***.

3 Select **Collect Identity** > **Collect Identity Attributes** > **Add attribute**.

4 Add the attribute by configuring the following:

Attribute name and Key

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

Type

Select the type of attribute you want to create. The types are **String**, **Boolean**, **Double**, **Long**, **Date**, and **Locale**.

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 this is not enabled, and the value is longer than the maximum size, it will cause an error and the record will not be collected.

Attribute Behavior

Select the behavior of the attribute. The attribute can be required, allowed to change, allowed to have multiple valued, 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 the Identity Governance Console.

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.

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

5 Select **Save**.

2.5.3 Viewing Available Attributes in Business Roles

When you create a business role, you define a membership expression that search for all users that meet a certain criteria to be added to the business role. For more information, see Section 14.3, “Defining Business Roles,” on page 141.

The **Membership expression** lists all of the available attributes you can match on under the **Title** field. This list matches the list displays 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, Global, Data or Business Role administrator have rights to administer business role schema. For more information, see Section 2.5.1, “Adding or Editing Attributes to Extend the Schema,” on page 28.

---

3 Creating and Managing Data Sources

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 1.2, “Adding Identity Governance Users,” on page 16.

3.1 Understanding Collector Configuration

When you create an identity or application source, you will also create the **collectors** that you want to use for gathering specific identity, account, or permission data from that source. A collector is based on a collector template that is populated, when possible, with common data mappings for the selected data source type. Each collector has one or more views that allow you to specify which data you will collect from your identity or application source, and describe how that data will be linked together in the Identity Governance catalog.

When you configure the collector, you designate the incoming attributes that you want to map to the attributes in the Identity Governance catalog. Then you can map the permissions to the accounts. You can map a static value to any attribute in a collector configuration. This has the effect of assigning the same specified value for the selected attribute to all collected objects. The **multivalue** field allows you to collect multiple values for an attribute. If you collect multiple values for the attribute, you can statically map only a single value.

3.1.1 Understanding the Common Elements in a Collector

Every collector has the following configurable 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
- JDBC, such as Oracle or PostgreSQL
- Resource Access Control Facility (RACF)
- Salesforce.com
- SAP HR
- SAP User Management
- ServiceNow
- SharePoint

NOTE: Template name ending in **with changes** can be enabled for incremental change events processing.

The CSV collector support TSV file. You enter the word `tab`, in uppercase, lowercase, or any combination in the **Column Delimiter** field.

To see all the data source types, select **Collector Template** when you create the data source. To collect data from a JDBC or 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 *NetIQ Identity Governance Installation Guide*.

You can also customize an existing template or create your own. For more information, see Section 2.2, "Customizing the Collector Templates for Data Sources," on page 26.

Service Parameters

These are the configurable parameters that allow the collector to connect and, if required, authenticate to the target data source. These typically include file locations, server host and port specifications, or service URLs.This section includes a **Test connection** button to verify the settings.

Select **Test connection** to verify the settings.

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.

3.1.2 Understanding Collector Templates for Identity Sources

Identity sources provide core identity information to Identity Governance. When using multiple identity sources you can:

- Specify the order of priority between different sources
- Specify how identities from different sources will be matched and merged
- Designate which source will be used for different identity attributes

Identity collectors populate the Identity Governance system with users. When using an LDAP-based One SSO Provider (OSP) system, such as eDirectory or Active Directory, ensure that the proper data source is providing the LDAP Distinguished Name attribute to the identities. This is the attribute that Identity Governance uses for single sign-on authentication.

Collector templates for an identity source can have the following elements:

Collect Identity

To ensure that you can create a unique identity from the data that you collect, you 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 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

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.

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.

Collect Group to User Membership

This view is used to collect 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

This view is used to collect 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.

3.1.3 Understanding Collector Templates for Application Sources

An application source might contain account and permission collectors. 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 to the application accounts as needed.

Depending on the type of data that you want to collect, the 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.

Collect Permission

Permissions can describe any of the following:

- Actions that you can take within an application, such as running reports
- Items that you possess, such as an identity badge
- Things that you can access, such as a building

A permission in Identity Governance is similar to an entitlement in Identity Manager.

NOTE: If you use **Permission-Account** or **User Mapping** to join permissions to accounts or users, you must disable the optional **Permission and Holders Mapping** collections. Failure to do so could result in duplicate permission assignments in the catalog.

Permission and Holders Mapping

(Optional) These views exist to allow you to specify how a permission will be joined to either an Identity Governance identity or to an application account. In most application sources, such as Active Directory, the permissions (groups) are joined to Active Directory users (accounts). In this situation, you will use an Active Directory account and an Active Directory permission collector and join the permissions to the account using the distinguishedName attribute of the account. However, if your identities also came from the same Active Directory source, the account collector is not needed and the group permissions could be joined directly to the identities using the distinguishedName. The collector configuration page presents all available permission join attribute options. Due to differences in the holder/permission relationship management in different application sources, Identity Governance provides two optional views:

- **Permission to Holder Mapping** where the relationship is best expressed by starting with the permission object and following the relationships to the holders of that permission. For example, the "member" attribute on an eDirectory permission group.

  When Mapping permissions to holders in any application where it exists, you must use **Account ID from Source** not **User ID from Source** if you want the permission to be linked to the user (which is the usual expectation).

- **Holder to Permissions Mapping** where the relationship is best expressed by starting with the user account and following the relationships to the permissions held by that user account. For example, the "groupMembership" attribute on an eDirectory user.

In some applications, the relationship can exist bidirectionally between the holder and permission. In this situation, use only one of the above views.

Collect Provisioning Applications

Applies only to Identity Manager data sources

Collect Connected Accounts

Applies only to Identity Manager data sources

Collect Permissions hierarchy

(Optional) When an application source organizes permissions in parent-child relationships, you can collect the relationship between the permissions. When gathering nested permissions, specify one of the following methods:

- **Child to parent** where the collected permissions include an attribute that points to child permissions
- **Parent to child** where the collected permissions include an attribute that points to a parent permission, such as eDirectory user

3.1.4 Understanding the Variations for Data 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.

This section explains how to use the collector templates for the following application sources:

- "Collecting from Active Directory with Azure Active Directory" on page 37
- "Collecting from a CSV File" on page 38
- "Collecting from Google Apps" on page 38
- "Collecting from Identity Sources with Change Events" on page 38

Collecting from Active Directory with Azure Active Directory

When your environment uses both Active Directory and Azure AD, some user identities might be unique to one of the applications while other identities 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 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`.

If you are using the Active Directory Azure collector, complete the following steps:

1. Enable the Azure Active Directory Graph API for your site and grant the following permissions to an account to access the API:
   - `Directory.Read.All`
   - `User.Read`
2. Generate an OAuth2 client and secret for API access.
3. Check 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.

Collecting from a CSV File

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.

If you use a CSV file as an identity source, you might 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 support TSV file. You enter the word `tab`, in uppercase, lowercase, or any combination in the **Column Delimiter** field.

Collecting from Google Apps

Google Apps manage 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.

Collecting from Identity Sources with Change Events

Identity sources with change events provide incremental change events for user and group data from certain identity sources to incrementally update the identity catalog. To periodically pull change events and incrementally make changes to your identity catalog the following conditions must be met:

- An identity source is configured as an identity event source, 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 and Application Sources” on page 40 and “Migrating an Identity Collector to a Change Event Identity Collector” on page 48.
- 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*.

Once event collection is enabled, Identity Governance uses the global configuration parameters: `com.netiq.iac.rtc.event.polling.interval` and `com.netiq.iac.rtc.max.polling.timeout` settings to determine the identity context change event polling frequency and time limit for batch event collection. Typically, events are collected in batches of up to one hundred events. However, if the identity source’s **Batch Size Limit** as configured in the **Service Parameters** is less than one hundred, then that batch size is the upper limit for event collection also.

IMPORTANT: The identity source with change event collectors are 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 change.

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

NOTE: For a more efficient event processing, change events are not generated 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.

3.2 Transforming Data During Collection

Because each application may have its own format for the data that you plan to collect, you might need to transform the data during the Identity Governance collection process. For example, the application might store dates as a string (`20151202`) which 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.

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';
}
```

3.3 Creating Identity and Application 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. 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. For more information, see “Migrating an Identity Collector to a Change Event Identity Collector” on page 48.

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 collect the information from that source. Identity Governance provides collector templates to facilitate this configuration, or you can import a JSON file to add identity or application sources.

NOTE

- If you are using the Identity Manager Identity collector, it must always be first in the list of collectors, or user authorizations fail. For more information, see “User Authorizations Fail if the Primary Identity Source is not Identity Manager”.
- When collecting identities using the publish and merge setting, matching attributes become mandatory attributes to have Identity Governance 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.
- 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`.
- To collect from a CSV file, specify the full path to the file.
- You must export data sources from the current version of Identity Governance to be able to correctly import them.
- You can use the Identity Governance Custom Collector SDK to create collectors. For more information, see the *Release Notes for Identity Governance 3.0.1*.
- 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.

To create a data source:

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

5 Select + to create a data source collector from a template.

or

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

IMPORTANT: You must export a data source from the current version of Identity Governance to import an updated version. 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.

---

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 "Collecting from Identity Sources with Change Events" on page 38. For more information, see "Understanding Change Event Collection Status" on page 42 and "Supported Attribute Syntaxes for eDirectory and Identity Manager Change Events Collection" on page 42.

NOTE: Only one event collector is allowed and any 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 in Understanding Collector Configuration:

- Section 3.1.1, "Understanding the Common Elements in a Collector," on page 34
- Section 3.1.2, "Understanding Collector Templates for Identity Sources," on page 35
- Section 3.1.3, "Understanding Collector Templates for Application Sources," on page 35
- Section 3.1.4, "Understanding the Variations for Data Sources," on page 37

8 Save your settings.

9 (Optional) If you want to preview all or part of the data, select **Test Collection and Troubleshooting**. For more information, see "Testing Collections" on page 46.

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.

To populate the catalog:

1 Select **Collect Now** for each data source on the Identities and Applications pages.

You need to collect and publish the data for Identity Governance to add the data to the catalog.

2 (Optional) To merge the collected data from an identity source, specify the rules for publishing and merging.

For more information, see Section 6.1.2, "Setting the Merge Rules for Publication," on page 64.

3 Select **Publish Now** on the **Identities** page and next to each application data source on the **Applications** page.

NOTE: When you publish any identity source, Identity Governance publishes all identity sources. For more information, see Section 6.1, "Publishing Identity Sources," on page 63.

---

4 When you see that publication has completed, go to **Catalog** to view the collected information.

3.3.1 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 “Collecting from Identity Sources with Change Events” on page 38.
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.

3.3.2 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`

3.4 Managing Identity and Application Sources

Identity Governance offers several ways to help you manage your data sources.

IMPORTANT: If your Identity Governance database environment runs Oracle, you must turn on the SQL Tuning Advisor to optimize queries in the Oracle database.

3.4.1 Exporting and Importing Collectors

The ability to export 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 go through several iterations of trial and error. When you have configured a collector that achieves the results you want, you should export it and save it with your other backup files. You can also use exported 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 export and import collector templates under **Configuration** in Identity Governance. For more information, see “Customizing the Collector Templates for Data Sources” on page 26.

To export and import collectors:

1. Select a data source, and then select **Test Collection and Troubleshooting**.
2. Select **Download and Emulation**, and then select **Download Data Source Configuration**.
3. Select a location for the file, and then select **OK**.

4 If you make changes and want to import a collector, under **Data Sources**, select **Identities** or **Applications**, and then select **Import an identity source** or **Import an application source**.

5 Select the file to import.

3.4.2 Creating and Editing Data Policies

Data policies can help you prove to auditors and internal risk partners that the data collected and published into the Identity Governance catalog is complete and accurate. Having data policies in place can promote confidence in your data collection processes and help you show others that your processes and configuration comply with a set of standards, reducing the need for further proof unless your process or configuration changes.

When you have defined data policies in place, you can compare collection and publication details from the same data source at two different collection or publication times. Identity Governance uses the defined data policies to produce the comparison details. For more information, see "Comparing Collections and Publications" on page 46.

Identity Governance provides separate tabs for data collection policies and data publication policies. Each set of policies contains separate tabs for identity and application data sources.

1 Log in as a Global or Data Administrator.

2 Under **Data Administration**, select **Data Policy**.

3 Navigate to the appropriate tab and select **+** to create a new policy.

4 Select the desired elements for the policy and specify criteria.

5 Save your settings.

6 Under **Data Administration**, select **Data Policy**.

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

8 (Optional) When editing a policy, select the trashcan icon to delete the policy.

9 (Optional) Select **Estimate impact** to show estimated violations for the policy.

3.4.3 Calculating and Remediating Data Policy Violations

After creating data policies, you can calculate violations on demand and resolve violations to reduce risk. Data 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, you can recalculate the number of data policy violations. For more information about micro certification and fulfillment, see Section 10.3, "Understanding Micro Certification," on page 109 and "Instructions for Fulfillers" in the *NetIQ Identity Governance User Guide*.

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 Data Policy page and edit the remediation setup.

To calculate data policy violations:

1 Log in as a Global or Data Administrator.

2 Under **Data Administration**, select **Data Policy**.

3 Select **Publication Data Policies** tab.

4 Select **Identity** or **Application** tab.

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

To remediate data policy violations:

1 Log in as a Global or Data Administrator.

2 Under **Data Administration**, select **Data Policy**.

3 Select **Publication Data Policies** tab.

4 Select **Identity** or **Application** tab.

5 Select **Set Remediation**.

6 Select **Remediation Type**.

6a If you selected **Email Notification**, select **Email source** and enter or search and select user or group as recipient of the email.

6b If you selected **Change Request**, select violation types, and provide instructions for fulfilling the change requests generated for selected violation types.

6c 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 selection of only relevant review definitions.
- **Review Name**: Specify a name for the micro certification.
- **Start Message**: Specify 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.

7 Select **Run Remediation on new violations when calculated** check box to automatically run remediation after saving your remediation setup.

8 **Click** Save.

9 To run remediation, select **Actions > Run Remediation**.

3.4.4 Exporting and Importing Data Policies

Once you have created your data policies based on your business requirements, you can easily export the collection and publication data policies and publication data policy 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.

To export or import data policies:

1 Log in as a Global or Data Administrator.

2 Under **Data Administration**, select **Data Policy**.

3 Select **Collection Data Policies** or **Publication Data Policies**.

4 In the **Identity** or **Application** tab, select the policy or policies you want to export.

5 Select **Export Data Policies** or **Actions > Export Data Policies**. A zipped file containing publication data policies and review definitions files in JSON format will be downloaded to your default download location.

6 Extract the files if you want to import them later.

7 To import data policies, click **Import Data Policies** on the Data Comparison Policies page.

8 Navigate to the folder where your data policies file is located, and click **Open**.

9 Identity Governance detects whether you are importing new or updated policies and whether the updates would create any conflicts or have unresolved references.

10 Select how to continue based on what information is displayed. For example, under **Updates**, you can compare the imported values with current values for each entity by selecting the respective policy before selecting policies to import.

11 Select the policies you want to import, and then click **Import**.

3.4.5 Comparing Collections and Publications

When you need to show that you have complete and accurate data, you can compare collection and publication details from the same data source at two different collection or publication times. Identity Governance uses the defined data policies to produce the comparison details. For more information, see Section 3.4.2, “Creating and Editing Data Policies,” on page 44.

To compare collections and publications from the same source:

1 Under **Data Sources**, select **Activity**.

2 (Optional) Select the calendar icon to focus the list on a specific time period.

3 Click on the advanced filter icon and select a data source name in the search to focus the list on specific data sources.

4 (Optional) Change the number of rows per page to show a longer list.

5 Select two listed collections or publications using the check boxes.

6 Under **Action**, select **Compare**.

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

8 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.

9 (Optional) To quickly view or open the applicable data policies, complete the following:

9a Select **Refine comparison options**.

9b Select or clear listed policies to change your comparison results.

9c Select **Edit Policies** to open the **Data Administration** > **Data Policy** page. For more information see, “Creating and Editing Data Policies” on page 44.

10 (Optional) Select **Overview** to see Data Policy Status details. For more information, see Section 19.2, “Monitoring Your Identity Governance System,” on page 188.

3.4.6 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 Identity Governance until you delete them.

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

- All records
- Some records
- Raw data
- Transformed data

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 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 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. Select a configured data source.
2. Select **Test Collection and Troubleshooting**.
3. Under **Test Collection**, select the collectors, and then select **Run Test Collection**.
4. Select the specific entities to collect and type the number of records to collect or leave **All** to collect all records.
5. Select the option for the type of collection to run.
6. After the test collection shows **Complete**, select **Action** to view, download, or delete test collection results.

3.4.7 Creating Emulation Packages

You can more easily troubleshoot collection configuration outside your production environment by creating emulation packages for data 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 Identity Governance until you delete them.

To create an emulation package:

1. Select a configured data source.
2. Select **Test Collection and Troubleshooting**.
3. Under **Download and Emulation**, select **Create emulation package**.
4. When the emulation status shows **Complete**, select **Action** to view, download, or delete the emulation package.

3.4.8 Migrating an Identity Collector to a Change Event Identity Collector

If you have upgraded from a previous version of Identity Governance or if you want to migrate an existing identity collector to one that accepts change events, use the Identity Source Migration utility to update your Active Directory, eDirectory, or Identity Manager data collector to accept change events. The identity collector you are migrating must publish using the **Publish without merging** or the **Do not publish** setting.

NOTE: Identity Governance 3.0.1 and later support change event identity collectors.

---

1. Upgrade to Identity Governance 3.5.1 or later and make sure that Identity Governance is up and running.
2. Verify that the `idgov/bin/rtc-migration.sh` (Linux) or `c:\netiq\idm\apps\idgov\bin\rtc-migration.bat` (Windows) file references the jar file `idgov/lib/ig-migration.jar` (Linux) or `c:\netiq\idm\apps\idgov\lib\ig-migration.jar` (Windows).
3. Run the command-line utility from the server where Identity Governance is installed.
   - **Linux:** Default location of `/opt/netiq/idm/apps/idgov/bin/rtc-migration.sh`, then enter `./rtc-migration.sh`
   - **Windows:** Default location of `c:\netiq\idm\apps\idgov\bin\rtc-migration.bat`, then enter `rtc-migration.bat` from a command line.
4. Provide the information needed to connect and authenticate to Identity Governance and the authentication server. When the utility successfully connects, it displays a numbered list of discovered identity sources.
5. Enter the number displayed next to the identity source to migrate.
6. After the utility runs checks to determine migration suitability, either confirm to proceed with the migration, if the checks succeeded, or review messages for failed checks and either address the problem areas, select a different source, or quit the utility.
7. (Conditional) If you confirm to proceed with migration, enter a local file name for the utility to back up the current collector configuration.
8. After the utility applies updates and exits with a success message, review the following updates to the collector configuration when viewed in Identity Governance:
   - The template (just under the name of the collector) has been changed to the **with changes** template corresponding to the one prior to the update.
   - After the **Collector name** is a new **Enable Change Event Collection** option, which is unchecked. To enable event processing, select this option, and then collect and publish the identity source.
   - The **Service Parameters** remain unchanged.
   - Under **Collect Identity** (the user view):
     - The **Base Dn** parameter is no longer required, but the value has not been changed. Omitting a value here will cause the entire LDAP tree to be collected.
     - (Conditional) For Active Directory identity change event source, a new parameter, **LDAP Search Filter for Identity Object Changes**, has been added, with the value `(objectClass=user)`. This parameter identifies events in Active Directory DirSync or AD Connect that should be delivered 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, a new parameter, **AD Object Categories for Changes**, has been added with the value `user`. You can modify this value if needed by adding other object category names in a comma-separated list.
- **User ID from Source** has been set to `OBJ_ID`. Do not change.
- The **Object GUID** parameter is now required. Its value is set to `objectGUID`. Do not change.
- **LDAP Distinguished Name** has been set to `OBJ_ID`. You can remove this value if you do not need to collect the `dn` separately from the `userId`. Do not assign any other value.

- Under **Collect Group** (the group view):
  - The **Base Dn** parameter is no longer required, but the value has not been changed. Omitting a value here will cause the entire LDAP tree to be collected.
  - A new parameter, **LDAP Search Filter for Identity Object Changes**, has been added with the value `(objectClass=group)`. This parameter identifies events in Active Directory DirSync or AD Connect that should be delivered in this view to Identity Governance. Only modify this value if you have other object classes in the local AD that correspond to groups and only by adding other `objectClass` terms to an LDAP expression.
  - A new parameter **AD Object Categories for Changes** has been added with the value `group`. You can modify if needed by adding other object category names in a comma-separated list.
  - **Group ID from Source** has been set to `OBJ_ID`. Do not change.
  - A new parameter, **Object GUID**, has been added with value `objectGUID`. Do not change.

4 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 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.

4.1 Creating a Scheduled Collection

You can schedule collections to run on at regular intervals. For example, collect data from Workforce and SAP identity sources every week. You 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.

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.
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, do not schedule collections with fewer than 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 4.3, “Understanding the Cron Expression for a Custom Interval of Collection,” on page 52.

6 (Conditional) 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.

4.2 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. For example, add and remove 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.

4.3 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`.

5 Integrating Collected Data with Identity Manager

This section provides guidance for using the **NetIQ Identity Manager Driver for NetIQ Identity Governance** (Identity Governance driver). For more information about installing and configuring the driver, see the *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide*.

Identity Governance can collect data from identity and application sources that are not connected to Identity Manager. With the Identity Governance driver, these user identities and application data can become resources in the Identity Vault for Identity Manager users. This gives 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 as needed for the customer's use-case.

5.1 Understanding Synchronization and Reflection

The Identity Governance driver helps synchronize changes to identities and applications in Identity Governance with matching user and resource objects in Identity Manager. The driver provides Global Configuration Values (GCVs) that allow you to delete or disable user objects or delete resource objects in the Identity Vault. Alternatively, you can remove the association between the user object and the identity in Identity Governance.

5.1.1 Reflecting Application Permissions in Identity Manager

For each application source in Identity Governance, you can **reflect** the collected permissions and assignments as resources in Identity Manager, with the exception of Identity Manager applications or child applications. With this setting enabled for an application, the Identity Governance driver can create resources in Identity Manager that match the permissions and permission assignments in Identity Governance. Identity Manager users can then request access to these resources even when the application is not a connected system in Identity Manager.

If an application source is also a connected system in Identity Manager and the driver uses entitlements, then you do not need reflection for that application source. However, if the driver does not use entitlements, the you might want to enable reflection for the application source.

When you reflect an application's permissions, the Identity Governance driver creates a new container in the Identity Vault for the permissions and creates a new Resource Category for grouping the permission resources. The driver specifies the same name for the Resource Category that Identity Governance has for the application. For example, if an application source in Identity Governance is named "SAP Permissions," then the driver creates a Resource Category named "SAP Permissions" in Identity Manager.

If you stop reflecting an application's permissions, the application is no longer linked to the resource containers in the Identity Vault. Identity Manager uses Global Configuration Values (GCVs) to determine the course of action after you disable reflection. By default, a GCV instructs Identity Manager to delete the resource containers and the resource category in the Identity Vault. However, you can modify the GCV to keep the containers and category, which allows you to reestablish reflection. For more information about de-linking the application from the Identity Vault, see Section 5.1.2, "Synchronizing Data Changes between Identity Governance and Identity Manager," on page 56.

When integrating application data with Identity Manager, the Identity Governance driver serves as the proxy for the application sources. The driver needs both a system account and a workflow in the User Application to create resources. For more information about configuring reflection, see Section 5.3, "Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager," on page 57.

5.1.2 Synchronizing Data Changes between Identity Governance and Identity Manager

When you stop reflecting an application's permissions or you delete an application from Identity Governance, you can synchronize those changes with Identity Manager. For example, you replace ABC Money, a financial application, with its competitor DEF Accounting. You stop collecting data from ABC Money, and then delete the application from Identity Governance. When you publish the latest snapshot of collected data to Identity Manager, the Identity Governance driver uses the Publisher Resource Object Unlink GCV to communicate that the ABC Money application no longer exists in Identity Governance. Identity Manager responds according to the GCV's setting.

After you have turned off reflection for an application, it is necessary to collect and publish both the application and the Identity Manager application in order to update Identity Governance with the changes made to Identity Manager when you turned off reflection. It is also necessary to review, and possibly modify, fulfillment settings for the application.

You can also synchronize changes to user identities. For example, in the latest collection of identities from the SAP application, Identity Governance notes that the identity for Joe Smith has been deleted. This generates an event in Identity Governance to delete the Joe Smith identity. The driver uses the setting for the Publisher User Object Deletion GCV to determine how to process deletions.

The Identity Governance driver creates user objects only for the identities that you add to Identity Governance after you enable synchronization. If you have identities in Identity Governance already, you can migrate those identities to the Identity Vault.

For more information, see the following sections:

- Section 5.5, "Migrating User Objects to the Identity Vault," on page 59
- Section 5.4.1, "Synchronizing New User Objects," on page 58

5.2 Ensuring Best Performance for Identity Matching

Review the following recommendations to ensure the best performance among the Identity Governance driver, Identity Governance, and Identity Manager components:

- Before enabling reflection for an application, perform the following actions:
  - Configure the driver to allow User Add operations on the Publisher channel (synchronization)
  - Migrate identities that do not exist in Identity Manager from Identity Governance to the Identity Vault

    For more information, see Section 5.5, “Migrating User Objects to the Identity Vault,” on page 59.

  If you enable reflection first, the process might generate a large number of synchronization events and assignment operations.
- Tune the Identity Vault to index the attributes that the Identity Governance driver uses for matching a large number identities. For example, you should index the attributes in an identity management solution with more than 100,000 users. The driver runs policies to match attributes in the following order:
  1. `workforceID`
  2. Internet Email Address
  3. Given Name + Surname
- Review the migration queries to reduce the amount of data that the driver transfers through the Remote Loader and the Identity Manager engine.
- Order your identity sources in Identity Governance such that the source collecting from Identity Manager is the first source to collect data. If you are using the Identity Manager Identities Collector, it must always be first in the list of collectors or user authorizations fail.

  For more information, see Chapter 4, “Creating and Monitoring Scheduled Collections,” on page 51 and Section 6.1.2, “Setting the Merge Rules for Publication,” on page 64.

5.3 Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager

Identity Governance can collect account and permission data from application sources that do not have role and resource objects in Identity Manager. The Identity Governance driver serves as the proxy for the application sources. For more information, see Section 5.1.1, “Reflecting Application Permissions in Identity Manager,” on page 55.

NOTE: The driver needs both a system account and a workflow in the User Application to create resources. For more information, see “Installing and Configuring the Identity Governance Driver” in the NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide.

---

1. Log in to Identity Governance as a Global Administrator.
2. Add the Identity Manager information to Identity Governance.
   - **2a** Select **Configuration**, then expand the **Identity Manager system connection information** section.
   - **2b** Provide the Identity Manager URL. For example: `http://myserver:8180/IDMProv`.

2c Add the administrator user name and password for your Identity Manager system. For example, `admin` or `cn=uadmin,ou=sa,o=data`.

2d Select **Test Connection**. Ensure that you have a valid connection before proceeding.

3 Under **Catalog**, select **Applications**.

4 Select an application that you want to integrate with Identity Manager.

5 Select the icon for **Edit application**.

6 Under **Identity Manager Synchronization**, select **Reflect permissions and assignments as resources in Identity Manager**.

7 Specify the provisioning workflow that you want Identity Manager to use.

8 For **Identity Manager Resource Owner**, specify the user account in Identity Manager that can grant permissions for the application. For example, the application owner.

In Identity Governance, the name for this user is the concatenation of the account `GivenName` and `Surname` attributes. For more information about this account, see "Creating an Identity Manager Provisioning Service Account for the Driver" in the NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide.

9 For each application, repeat Step 4 through Step 8.

5.4 Synchronizing Changes in Identity Governance Data with Objects in the Identity Vault

You can synchronize new and modified identities and application permissions in Identity Governance with user and resource objects in Identity Manager. The Identity Governance driver includes policies that tell Identity Manager how to respond to changes that occur to application and identity data in Identity Governance. You configure these policies in the Global Configuration Values.

- Section 5.4.1, "Synchronizing New User Objects," on page 58
- Section 5.4.2, "Synchronizing Resource Objects," on page 59

5.4.1 Synchronizing New User Objects

The Identity Governance driver synchronizes only the identities that are created in Identity Governance after you enable synchronization with Identity Manager. If you already have identities in Identity Governance when you enable synchronization, you need to migrate the existing user objects. For more information, see Section 5.5, "Migrating User Objects to the Identity Vault," on page 59.

The following GCVs allow you to configure how the Identity Governance driver and Identity Manager synchronize user objects.

Publisher User Object Placement

Specifies the container in the Identity Vault that stores the users created by the driver. When attempting to match Identity Governance identities with Identity Manager identities, the Identity Governance driver looks first in this sub-tree to determine whether an identity from Identity Governance already exists in Identity Manager. The driver recognizes a matched identity by its

`Distinguished Name` value in Identity Manager. When the driver creates new users in the Identity Vault, this policy writes the GUID of the Identity Governance user object to a value of the `DirXML-Accounts` attribute on the user object.

The default value is `\data\users\arusers`. Specify a different folder than the one that contains identities imported from connected systems. When you use separate folders for identities from systems connected to Identity Manager and identities from Identity Governance, you can efficiently remove users collected from Identity Governance.

Publisher User Object Deletion

Provides options for Identity Manager when responding to an identity deleted from Identity Governance. When the Identity Governance driver communicates the delete event through the driver, you can configure Identity Manager to perform one of the following actions:

- **Remove Association**: Removes the `DirXML` association for the identity between Identity Manager and Identity Governance. The user object remains in the Identity Vault.
- **Disable Users, Remove Association**: (Default setting) Breaks the relationship for the identity between Identity Manager and Identity Governance. Identity Manager disables the user object. This is the only time the driver can set or reset the Login Disabled flag for a user object in Identity Manager.
- **Delete Users**: Deletes the user object from the Identity Vault.

For more information about configuring GCVs in a driver, see "When and How to Use Global Configuration Values" in the *NetIQ Identity Manager Driver Administration Guide*.

5.4.2 Synchronizing Resource Objects

The **Publisher Resource Object Unlink** GCV specifies how Identity Manager responds when you remove an application source from Identity Governance. This policy has the following options:

- **Delete Unlinked Resources**: Deletes the application and its associated permissions and permission resources form Identity Manager.
- **Keep Unlinked Resources**: (Default setting) Flags the application resources in Identity Manager to indicate that your organization is no longer interested in the application.

This policy also applies when you deselect **Reflect permissions and assignments as resources in Identity Manager** for the application in Identity Governance. For more information about reflecting permissions, see the following sections:

- Section 5.1.1, "Reflecting Application Permissions in Identity Manager," on page 55
- Section 5.3, "Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager," on page 57

5.5 Migrating User Objects to the Identity Vault

The Identity Governance driver has an optional Publisher channel functionality that enables the driver to capture identities added to Identity Governance then synchronize them with the Identity Vault. To ensure that synchronization does not create duplicate identities, the driver adds only the identities

that do not have a value for the `Distinguished Name` attribute. It is recommended that you configure synchronization in the driver for matching identities between Identity Governance and Identity Manager.

However, you might have previously configured the driver to prevent identity synchronization and now need to change that decision. For example, you enabled synchronization after you collected a set of identities. Since the Publisher channel is event driven, the driver publishes only the identities added to Identity Governance after you start synchronization. The only way to publish pre-existing identities to the Identity Vault is to **migrate** them using the Subscriber channel.

NOTE

- You cannot migrate identities if you have not configured synchronization. For more information about synchronizing identities, see Section 5.4.1, “Synchronizing New User Objects,” on page 58.
- Before starting user migration to the Identity Vault, enable **Adds and Migrate Allowed** in the driver configuration then restart the driver.

For more information, see the following sections:

- Section 5.5.1, “Targeting Identities that Do Not Exist in Identity Manager,” on page 60
- Section 5.5.2, “Adding Application Permissions after Migrating Identities,” on page 60

5.5.1 Targeting Identities that Do Not Exist in Identity Manager

To support migration, the Identity Governance driver provides a full set of migration queries. The migration queries allow for wildcards for any of the supported schema attributes. In general, you should migrate only the identities that do not exist in the Identity Vault. For example, you might already have used the Identity Manager Identity Collector to collect identities from the Identity Vault. You would not want to migrate these identities since they already have user objects in the Identity Vault. The Identity Governance driver recognizes these synchronized identities by the value of their `Distinguished Name` attribute. To avoid duplicating identities, you can add the `DirXML-Accounts` attribute to the migration query. The `DirXML-Accounts` attribute has the following values:

- **false**: When you set the value to `false`, the query targets only the identities in Identity Governance that do not have the `Distinguished Name` attribute value. Use this setting to identify the user objects that you want to create in the Identity Vault.
- **true**: When you set the value to `true`, the query targets only the identities in Identity Governance with the `Distinguished Name` attribute value. Use this setting to find identities that have already been collected from Identity Manager.

To target all of the Identity Governance identities, regardless whether they already exist in the Identity Vault, do not use the `DirXML-Accounts` attribute in the migration query.

5.5.2 Adding Application Permissions after Migrating Identities

When you migrate identities to Identity Manager, the Identity Governance driver does not include any permission assignments associated with those identities. To add the permission assignments, you must enable reflection for the target application. Then the driver uses the Publisher channel to

synchronize the permission and assignments. Each time you modify the application or change the published data for the application, the driver reflects the changes to Identity Manager. For more information, see the following sections:

- Section 5.2, “Ensuring Best Performance for Identity Matching,” on page 57
- Section 5.1.1, “Reflecting Application Permissions in Identity Manager,” on page 55

6 Publishing the Collected Data

Publication makes the most recently collected data, and the relations among that data, available in the Identity Governance 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.

6.1 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.

6.1.1 Understanding Publication Behavior

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 options:

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.

You must 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 6.1.2, “Setting the Merge Rules for Publication,” on page 64.

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.

6.1.2 Setting the Merge Rules for Publication

You might want to customize the rules for unifying the information collected from multiple identity sources for the same identity. Merging 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 don't select priorities using merging rules, Identity Governance uses the first collected value.

IMPORTANT: When collecting identities using the publish and merge setting, matching attributes become mandatory attributes to have Identity Governance 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.

---

1. Log in to Identity Governance as a Data Administrator.
2. Select **Data Sources > Identities**.
3. (Optional) Arrange the order of the identity sources to set their priority for merging the published attributes.
4. (Optional) 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 (go by order)** option instructs Identity Governance to use the first identity source as the attribute authority.
5. Select the **Save** icon.
6. (Optional) Publish your pending changes.
7. (Optional) Verify the changes that you published to the catalog.

6.1.3 Publishing the Identity Sources

If you have a scheduled collection, the scheduled run 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.

1. Log in to Identity Governance as a Data Administrator.
2. Select **Data Sources > Identities**.
3. Select the **Publish identities now** icon.

6.2 Publishing Application Sources

You can publish an application source independently from other application sources. However, before publishing an application source, you must publish your identity sources.

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

   For more information, see Section 6.1.3, “Publishing the Identity Sources,” on page 64.
3. Select **Data Sources > Applications**.
4. For each application source that you want to publish, select **Publish**.

TIP: You may 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.

---

7 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 a Data Administrator, Global Administrator, or bootstrap 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 CSV file as a data source, the file must use UTF-8 encoding.

7.1 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 “Auth Matching Rules” on page 193.

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 Global Administrator or 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 1.3, “Assigning Authorizations to Identity Governance Users,” on page 17.
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 1.3, “Assigning Authorizations to Identity Governance Users,” on page 17.

7.2 Understanding Identity, Application, and Permission Management

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

7.2.1 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, and identity source information. Identity source information shows the collector mappings, curated, and effective values for the identity attributes.

To view or edit identity details:

1 Navigate to **Catalog > Users** 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 user.

5 Modify the available attribute values, and then select **Save**.

7.2.2 Managing Application Information

Application information includes the application's photo, name and description, the identities of the application's owner and administrators as well 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, `MoneyHoney Financials`.
3. Select the **Edit** icon.
4. Modify the application settings, such as:

   Risk

   Specifies the importance 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

7.2.3 Reviewing Application Fulfillment Settings

Identity Governance allows you to specify a fulfillment method 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 methods, see Section 9.2, “Configuring Fulfillment,” on page 88.

7.2.4 Managing Permission Information

Permission information includes the permission’s photo, name and description, identity of the permission’s owners and 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 policies.

When you save changes, Identity Governance displays an icon beside 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 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

7.3 Editing Attribute Values on 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. To view the attributes of a specific item in the catalog, select **Catalog**, the type of data you want to view, then the object you want to view.

To edit attribute values, select 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 change a value, Identity Governance shows an icon next to the value to indicate the change. You can later reset the value to its original setting. You can also associate tags, or metadata, so you can more easily identify the information when you create and perform a review.

NOTE

- You can edit only the attributes that are marked as editable.
- 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.
- If you edit any permission records to set the `excludeFromCatalog` attribute to `true`, the only way to ever see these records in the catalog again is to manually change the `spermission` table value back to `false`, or if bulk editing was used to set it to `true`, copy the Bulk Data Update CSV file that made the original edits and change the edited value to `UNDO_CURATION`.

For more information, see the following sections:

- Section 7.3.1, “Editing Data,” on page 71
- Section 7.3.2, “Editing Attribute Values in Bulk,” on page 71

7.3.1 Editing Data

When you edit the data, you override the originally collected content. Any attribute that you edit will be persisted through subsequent collection and publication, even if the original value for the attribute changes. To replace the edited value with the currently collected value, reset the collected value.

IMPORTANT: Identity Governance evaluates only collected attribute values for the authentication matching rules, not edited values. For more information, see “Auth Matching Rules” on page 193.

7.3.2 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 comma-separated value (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 (|).

IMPORTANT: Identity Governance evaluates only collected attribute values for the authentication matching rules, not edited values. For more information, see “Auth Matching Rules” on page 193.

Before you follow this procedure, make sure you have configured the bulk database folder in the Identity Governance Configuration Utility. For more information, see Section A.6, “Bulk Data Update Settings,” on page 195.

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. Select **Bulk data update** in the upper right.
3. Select **+**.
4. Specify all the mandatory fields.
5. Select **+** next to **Attributes to update** and select the attributes.
6. (Optional) Select **+** next to **Decision context attributes** and select the attributes Identity Governance will use to match the updated information with the correct item.
7. Save your settings.
8. Select the **Export file** icon to generate the template.

9 Get the template from the appropriate location on the Identity Governance server. The template location is specified through the Identity Governance Configuration Utility. For more information, see Section A.6, “Bulk Data Update Settings,” on page 195.

10 Add the update information to the template, and then copy the updated template to the appropriate location on the Identity Governance server. Identity Governance automatically detects updated files and applies the updated information to your data.

NOTE: You can specify multiple users as permission owners. When performing bulk edits of permission owners, the ID name has changed from `uniqueUserId` to `uniqueOwnerId` and `uniqueOwnerId` requires a new flag, `#true`, with each permission owner ID.

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.

7.4 Searching for Items in the Catalog

Identity Governance gives you 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 give flexibility in searching for entities in your system, including searching across entity relationships.

7.4.1 Searching 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.

You must have one of the following authorizations to have access to Insight Queries:

- Global Administrator
- Auditor
- Data Administrator
- Governance Insights Administrator

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 186.

To access Insight Queries:

1 Log in using the Global, Data, or Data Query administrator or the Auditor authorization.

2 Select **Catalog** > **Governance Insights**.

3. Select the **+** icon to create a query or select a query you have previously created.
4. Complete the form with the desired criteria. The criteria includes a set of attribute conditions or sub-expressions and filters that can be used to filter the result set based on specific attribute values.
5. (Optional) Add a cross-reference filter or add expression criteria to the search criteria. Cross-reference filters are relationships between the selected entity type being searched and other entities in the system. They do not widen the data search, but limit the query based on the specified filter. For example, if you are searching for identities and want to only find all identities that are members of business roles, then add **Member of Business Role** as a cross-reference filter. If you only want to find users who are in violation of an Separation of Duty policy, then add **Violating SoD** cross-reference filter.
6. 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.
7. Select the **Run** icon to see query results. As you change the query options, select the **Run** icon to update the results.
8. Select the **Save** icon to save the query.
9. (Optional) Select **Download as CSV** to save the results.

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 these as a column:

- User: Geo Location
- Access Request Item: Change Item Comment
- Change Item Action: Item Comment

7.4.2 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 type-ahead search by selecting **Configuration > General Settings > Typeahead Delay**.

The attributes that appear in the refinement list are fixed for Technical Roles, however, they can be configured 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 when you want the attribute displayed in review items. For more information, see Chapter 11, “Running a Review Instance,” on page 123.

   Display in business role selection criteria

   Select this option when you want the attribute displayed when creating a business role membership expression. The membership expression contains the search criteria for membership in a business role. For more information, see Chapter 14, “Creating and Managing Business Roles,” on page 137.
4. Select **Save**, then publish the changes to the catalog.

7.4.3 Managing Filters

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.

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.

1. After using the expression builder to add a filter to a search, name the filter and select **Save**.
2. The next time you select the filter icon, a menu allows you to select from several options.
3. Select **Manage saved filters**.
4. Here you can see all your saved filters, edit them, or delete them.
5. Select **Save** or **Close**.

7.5 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.

After you have published application data, you can group permissions that have common or frequents associations to create technical roles. When you have created technical roles, Identity Governance detects users with permissions that match the technical roles you have defined and lists the technical roles a user has in the user catalog. When you have defined technical roles, you can create user access review definitions for technical roles reviews.

7.5.1 Understanding Technical Role States

There are several states in the life cycle of a technical role after they are created manually or mined. From beginning to end, the technical role goes through the following states:

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; however, the role is excluded from the detection process. This state corresponds to the internal state called REJECTED.
INVALID	Invalid and excluded from detection process due to a detected error. Detection errors are usually the result of a deleted permission that is included in the technical role.

7.5.2 Understanding Technical Role Mining

Identity Governance uses advanced analytics to mine business data and identify role candidates. This process of discovering and analyzing business data to logically group permissions to simplify the review process or allow grouping related permissions under one technical role candidate is called

Technical Role Mining or Role Discovery. Global or Technical Role administrators can use role mining to create technical roles with common permissions. Identity Governance uses two approaches to technical role mining to identify technical role candidates.

- **Automatic Suggestions** enables administrators to direct the mining calculations by either saving the defaults, or by specifying minimum number of permissions that specified number of users should have in common, coverage percentage, maximum number of role suggestions, and other role mining options and saving the options.
- **Visual Role Mining** enables administrators to select role candidates from a visual representation of the distribution of users based on permissions. Administrators can click in the user access map and drag to select an area in the map, and then view technical role candidates.

NOTE: Technical role candidate can also be generated when using mining to create business roles. For more information about business roles, see Chapter 14, “Creating and Managing Business Roles,” on page 137

NOTE: Mined business or technical roles are created in a candidate state. Role candidates can be edited and saved, but must be promoted before they can be approved or published as a role.

7.5.3 Creating Technical Roles

To create technical roles you must have either the Global Administrator or the Technical Roles Administrator authorization. You can create technical either manually or by using role mining analytics. Additionally, Business Role Administrator can generate technical roles when creating business role candidate.

When using role mining analytics, permissions are automatically grouped together and presented as role candidates. You must promote role candidates as roles, before they can be activated.

When creating technical roles manually, an understanding of what permissions you want to assign to the technical role is helpful. However, you can create the technical role without adding any permissions to it in order to delegate responsibility for assigning the permissions in a technical role to the Technical Role Owner. The designated owner can then log in to Identity Governance and add the appropriate permissions to the technical role. You cannot activate a technical role until you have added permissions to the technical role.

To create a technical role:

1. Log in as a Global or Technical Roles Administrator.
2. Under **Catalog,** select **Roles**.
3. Select the **Mining** tab.

If	Then
You want to direct role mining calculations and create more than one technical roles	◆ Select **Automatic Suggestions**. ◆ Save default options, or specify options, and save. ◆ Select one or more items from the list and **Create Roles**. **NOTE:** Suggestions are sorted by number of users times the number of permissions. For example, if there are five users who match the role mining options and who hold four permissions in common, they will be listed first, followed by a suggestion with four users who hold four permissions in common.
You want to use user access map to create a role candidate	◆ Select **Visual Role Mining**. ◆ Click in the map and drag to select an area. ◆ Click **View Candidate**. ◆ (Optional) Click **more** to add description, risk, cost, or category. ◆ (Optional) Click **+** to add permissions, or click **Remove** next to a permission to remove permissions. ◆ Estimate impact. ◆ Click **Create candidate**.

4 On the **Roles** page, click the mined role.

5 (Optional) Edit the role name, description, risk, cost, or category.

6 Estimate impact by viewing list of associated users and analyzing SoD violations if SoD policies had been previously defined.

7 (Optional) Add or remove permissions based on the estimated impact and save the changes.

8 Select **Yes** to promote the role candidate.

NOTE: If a role candidate is not promoted, it cannot be activated and published as a role.

9 Alternately, on the **Roles** page, select **+** to create a role manually.

10 Provide the required information.

11 (Optional) Select **+** next to **Permissions** and select the permissions to include in the role, and then select **Add**.

12 (Conditional) If permissions have been added to the technical role, estimate impact and edit role if needed.

13 Save your settings.

NOTE: When you add a permission 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 filters that you have defined. For more information about filters, see Section 7.4.3, “Managing Filters,” on page 74.

7.5.4 Activating Technical Roles

After you have added permissions to a technical role definition, you can see an estimate of the number of users holding the permissions of the technical role, and you can activate the definition. If you do not activate the definition, 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.

To activate a technical role:

1. Under **Catalog**, select **Roles** as a Global or Technical Roles Administrator.
2. Select the role from the list, then select **Edit**.
3. In the role definition, select **Active**.

Activating and deactivating a technical role both start a detection process. Identity Governance detects users in the catalog that contain the permissions when you activate a technical role. When you deactivate a technical role, Identity Governance removes the detected technical roles in the catalog. Similarly, if you change the permissions in an active technical role definition, Identity Governance goes through the detection process and updates the catalog. However, if a technical role was authorized for a business role, deactivation does not remove the technical role authorization or its contained permissions' authorizations. Also, it does not change any current or pending auto-grant or auto-revoke request. For more information, see Section 14.11, "Automated Access Provisioning and Deprovisioning," on page 151.

You can quickly search for a role by name or description. 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.

7.5.5 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.

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 14.11, "Automated Access Provisioning and Deprovisioning," on page 151.

To edit or delete a technical role:

1. Under **Catalog**, select **Roles** as a Global or Technical Roles Administrator.
2. 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, selected permissions, and any Separation of Duties policies that reference the technical role.

3 Select **Edit** at the end of the details panel to edit the technical role.

4 (Conditional) Select **Delete** to delete the technical role.

You must edit the technical role to delete the technical role.

7.5.6 Downloading and Importing Technical Roles

You can download technical roles as a JSON file and import them later into another environment.

To download or import technical roles:

1 Under **Catalog**, select **Roles** as a Global or Technical Roles Administrator.

2 Select a role or all the roles on the **Roles** tab.

3 Select **Actions > Download**.

3a (Optional) Include references to technical role owners and download associated applications and assigned categories.

3b Select **Download**.

4 If you make changes, or want to want to import previously downloaded technical roles into another environment, select **Import Technical Roles** on the **Roles** tab.

5 Navigate to the technical roles JSON file, select the file to import, and click **Open**.

6 Identity Governance detects whether you are importing new or updated roles and whether the updates would create any conflicts or have unresolved references.

NOTE: Technical roles that cannot be resolved because a match for a referenced object cannot be found in the system will have an indicator. Importing before the roles are resolved will result in incomplete roles with some missing permissions. If an indicator is shown next to a role in the import view, inspect these roles and make sure they map properly in the target system.

---

7 Select how to continue based on what information is displayed.

NOTE: After importing, you must activate the role for Identity Governance to recognize the users that hold the permissions as members of a technical role. For more information, see “Activating Technical Roles” on page 78.

---

8 Database Maintenance

Identity Governance database maintenance features allow data and global administrators to archive data in the database and to clean up old and unused data in the database. Use these features to maintain your database.

8.1 Understanding Database Maintenance

The operations database (by default, `igops`) 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 database increases with each new collection, publication, review, and other operations. This can have an adverse impact on the performance of some database queries, because they are having to filter through more and more irrelevant historical data. Identity Governance includes the **Database Maintenance feature**, which provides capabilities for data administrators and global administrators to archive older data in a separate archive database, and then allows historical data to be cleaned up from the operations database.

The Database Maintenance feature provides the following:

- Shows 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 disable running archive
- Shows the latest complete archive details
- Allows you to start the database maintenance process, with optional database cleanup

When doing database cleanup, Identity Governance searches the operations database for purgeable items that are older than the number of retention days you specify. 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 may be needed for current operations. For more information about how the utility decides which items can be purged, see Section 8.3, “Identifying Purgeable Data,” on page 82. If archiving is enabled, data will always be archived to the archive database before it is purged from the operations database. Database cleanup will not be performed if an archive fails to complete. You can disable archiving to bypass this restriction, but it is not recommended.

When starting database maintenance, Identity Governance does not start archiving or cleanup until all current operations (collections, publications, scheduled processes, starting reviews, and so forth) have been completed or idled cleanly. Furthermore, it prevents starting any new operations while archiving and cleanup are in progress. Normal Identity Governance operations are automatically resumed when maintenance tasks are completed or canceled. This is done to ensure that Identity Governance cannot update the operations database while an archive or cleanup is in progress. In this way Identity Governance guarantees 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. Disabling archive can result in the loss of historical operational data.

An administrator has the ability to cancel archive and cleanup tasks while they are running. Usually, both archive and cleanup tasks are run automatically one after the other, and when they are completed, normal Identity Governance operations are automatically resumed. 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.

8.2 Archiving the Operations Database and Purging Data

To use the Database Maintenance features in Identity Governance, you must be a Data Administrator or Global Administrator.

1. Select **Data Administration** > **Maintenance.**
2. (Optional) Select one of the summaries to view details for changes since last archive or items ready to be purged.
3. Select **Start Maintenance**.
4. (Optional) To purge data after the archive process completes, select **Do cleanup after archive** check box.
5. (Optional) Select whether to pause after any of the phases.

   IMPORTANT: Pausing after a phase means that the system will NOT automatically transition to the next phase or exit maintenance mode until a user manually starts the next phase or exits maintenance mode, even if the archive fails or is canceled.
6. Select the number of days to retain data before making it available to purge.
7. (Optional) Select **Advanced Cleanup Configuration** check box to specify retention days per entity type.

8.3 Identifying Purgeable Data

During the cleanup phase of database maintenance, Identity Governance removes the following types of data from the operations database (types are listed alphabetically).

NOTE: The conditions listed for each type of data to be purged *can change* if scenarios come up where it is determined that the conditions need to be amended.

Access request

Can be purged only when the request is completed, 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

Analytical facts

Can be purged only when retention time is specified and facts are older than the specified retention time.

Business role

Can be purged if:

- 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

Bulk data update definition

Can be purged if it has been deleted.

Category

Can be purged if the category has been deleted.

Certification policy

Can be purged if policy has been deleted.

Collection

Can be purged if:

- Is not currently running, that is it must be in a canceled, failed, completed, or terminated state
- Its data is not part of any snapshot (snapshots containing a collection's data must be purged first)

Data policy

Can be purged if has been deleted.

Data source

Can be purged if:

- Is not scheduled for collection
- Is not currently being collected or published
- Has been deleted
- Is not part of a snapshot (snapshots containing data from data source must be purged first)

Additionally, when data source is an application it can be purged if the application:

- Is not a parent to 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 policy

Request approval policy

Can be purged if:

- Policy has been deleted
- There are no requests associated with the policy (requests associated with the policy must be purged first)

Request policy

Can be purged if:

- Policy has been deleted
- There are no requests associated with the policy (requests associated with the policy must be purged first)

Review definition

Can be purged if:

- Has been 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:

- Is not running, that is has been canceled, experienced an error, or has completed certification
- Is not referenced by a change request item action that is still pending, that is its not in a final verified or error state

---

NOTE: Materialized views, if any, are also purged when review instances are purged.

Risk score status

Can be purged if:

- Is in the error, canceled, or completed state
- If in completed state, there must be another completed risk score status of the same entity type that has a later start time

Separation of Duties case

Can be purged if:

- Case is closed
- There are no change request items that 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:

- Has been deleted
- Is not referenced in a Separation of Duties case (Separation of Duties cases should be purged first)
- There are no access requests that had potential SoD violations for the policy (such access requests must be purged first)

Snapshot

Can be purged if:

- Is not the current snapshot of the Identity Governance catalog
- Is not a precursor to another snapshot
- Is not referenced by a review instance
- There are no Separation of Duties violations for users or accounts in the snapshot
- There are no technical roles that reference permissions in the snapshot

Technical role

Can be purged if:

- Has been deleted from the Identity Governance catalog
- Is not referenced by a review instance
- Is not referenced by a Separation of Duties policy
- Is not referenced by a Review Definition
- Is not referenced by a business role

Unregistered facts

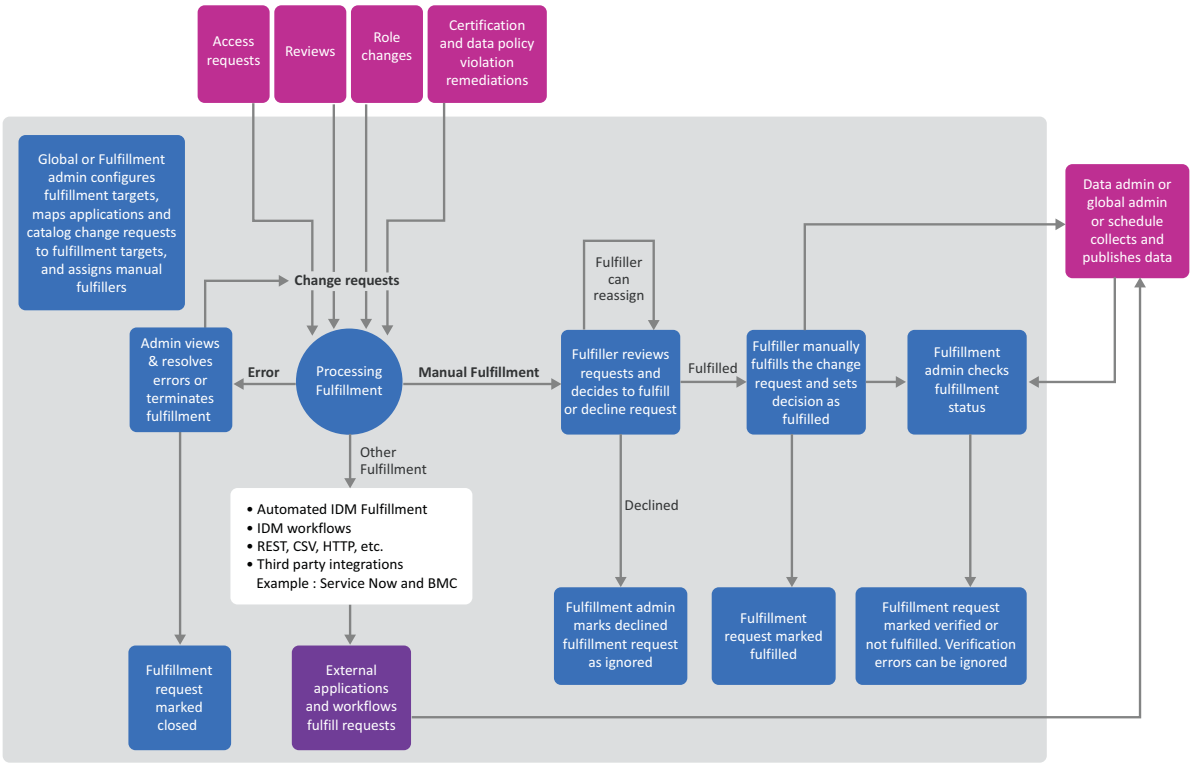
Can be purged when fact tables are available in schema even after custom facts are unregistered from fact catalog.

9 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. Identity Governance users with global, fulfillment, or bootstrap administrator authorization assignments can configure fulfillment options.

9.1 Understanding the Fulfillment Process

Figure 9-1 *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.

9.2 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 fulfillment targets:

- Active Directory LDAP
- BMC Remedy Incident
- CSV
- eDirectory LDAP
- Generic HTTP

- Identity Manager Dxcmd Fulfillment for Active Directory
- REST Service
- ServiceNow Generic
- ServiceNow Incident
- ServiceNow Request
- SOAP Service

To configure fulfillment methods:

1. Log in to Identity Governance as a user with global, fulfillment, or bootstrap administrator authorization assignment.
2. Select **Fulfillment > Configuration**.
3. (Conditional) Select a fulfillment target.

   or

   If you want to add a fulfillment target, select **+** and complete the required fields in the template. When adding fulfillment targets, you must configure service parameters to connect Identity Governance to your fulfillment service, and then configure mappings to create an appropriate fulfillment request. 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. An Identity Governance administrator must enable these attributes in **Configuration** > **Context Fulfillment Attributes**.

   NOTE: You can download the fulfillment target templates, edit them, and upload them to Identity Governance instead of configuring the service parameters and mappings in the application. For more information, see Section 9.3, “Customizing Fulfillment Target Templates,” on page 99.

   ---
4. Make any additional updates for the selected fulfillment target, such as fulfillment response mapping and specifying change request types, and select **Save**.
5. Select **Fulfillment > Configuration** and select the **Application setup** tab.
6. (Optional) If you want to use the same fulfillment method for multiple applications, you can select and configure them using the **Fulfillment Target** selector at the top of the page.
7. For each application, select the fulfillment method in the **Fulfillment Target** column. The **Change Request Type** column updates to show whether the fulfillment target handles all change request types or some types for this application.
8. (Optional) Select **customize** to change the default configuration for any fulfillment method you want to customize for a given application. Identity Governance adds an icon to each application row showing that you have customized the fulfillment configuration and providing an easy way to restore default values.
9. Select the **Catalog update setup** tab and select the fulfillment method for each type of catalog update request initiator you have in place.
10. Select **Save Fulfillment Configuration** using the icon at the top of the tab when you have made changes.

9.2.1 Configuring Multiple Fulfillment Targets for an Application

You can configure each application 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.

1. Log in to Identity Governance as a user with global, fulfillment, or bootstrap administrator authorization assignment.
2. Select **Fulfillment > Configuration** and select the **Application setup** tab.
3. Select the green plus sign (+) next to the fulfillment target where you want to specify multiple targets.
4. Select the target you want to process change requests in each row for the application. You can use the same fulfillment target and customize each row to process different 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 display in red text.
5. After making changes, select the save icon at the top of the tab to save your settings.

9.2.2 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 user with global, fulfillment, or bootstrap administrator authorization assignment.
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:
   - Paste a script in the text field

- Select **Advanced Edit** to open a script editor
- Select **Browse** to upload a script file

5 Save the fulfillment target.

9.2.3 Configuring Identity Manager and Manual Fulfillment Methods

For Identity Manager automated, Identity Manager workflow, and manual fulfillment methods, Identity Governance evaluates and fulfills the change items without the need for extensive configuration. When specifying one of the default methods of fulfillment, observe the following considerations:

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 9.5.3, “Automatically Fulfilling the Changeset,” on page 101.

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 workflow needs to have inputs for the following fields:

- `String: changesetId`
- `String: appId`

To connect to the external provisioning system, specify the workflow settings in the Identity Governance Configuration Utility. For more information, see “External Provisioning System” on page 196.

For more information about the workflow process, see Section 9.5.2, “Using Workflows to Fulfill the Changeset,” on page 101.

Manual

Specify an individual or group of individuals to serve as the fulfiller. For more information about manual fulfillment, see Section 9.5.1, “Manually Fulfilling the Changeset,” on page 100.

To have Identity Governance email reminders to the fulfillers, ensure that you configure email notifications. For more information about configuring notifications, see “Notification System” on page 197. For more information about customizing emails, see Section 2.1, “Customizing the Email Notification Templates,” on page 23.

9.2.4 Configuring Service Desk Fulfillment

Identity Governance includes connectors to 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.

The Identity Governance Fulfillment target configuration allows you to customize your incidents for these various systems. When you create a service desk 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.

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:

- `REMOVE_ACCOUNT_PERMISSION`
- `ADD_USER_TO_ACCOUNT`
- `REMOVE_PERMISSION_ASSIGNMENT`
- `REMOVE_ACCOUNT_ASSIGNMENT`
- `REMOVE_ACCOUNT`
- `ADD_PERMISSION_TO_USER`
- `ADD_APPLICATION_TO_USER`
- `ADD_TECH_ROLE_TO_USER`
- `MODIFY_PERMISSION_ASSIGNMENT`
- `MODIFY_ACCOUNT_ASSIGNMENT`
- `MODIFY_ACCOUNT`
- `REMOVE_APPLICATION_FROM_USER`

fulfillmentInstructions (optional)

Instructions the reviewer provided for the fulfiller

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"
}
```

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. For more information, see Section 2.2, “Customizing the Collector Templates for Data Sources,” on page 26.

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 method.

BMC Remedy Incident Management Integration

The Identity Governance fulfillment connector for BMC Remedy 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`.

The connector uses a pre-configured template that maps the Identity Governance change item data and application-specific static values into various attributes in the SOAP XML payload. The WSDL from your incident 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 Micro Focus technical support representative for details.

IMPORTANT: The Remedy application requires several fields to create an incident. The template identifies fields that *must* be properly configured to ensure the ability to create incidents.

Use the following table to understand the Identity Governance mappings to the Remedy incident fields. Quotation marks surround static values. You can modify the static values provided in the template to conform with the options available in the target service desk application.

BMC Remedy Incident Field	Identity Governance Mapping
`Service_Type`	"User Service Request" (required)
`Reported_Source`	"Direct Input" (required)
`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`	

ServiceNow Incident Management Integration

The Identity Governance fulfillment connector for ServiceNow Incident Management uses the Incident SOAP service `insert` method for creating incidents in the Incident Management application. For example, `https://your-service-url/incident.do?WSDL`.

The connector uses a pre-configured template that maps the Identity Governance change item data and application-specific static values into various attributes in the SOAP XML payload. The WSDL from your incident 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 Micro Focus technical support representative for details.

Use the following table to understand the Identity Governance mappings to the Incident Management incident fields. Quotation marks surround static values. You can modify the static values provided in the template to conform with the options available in the target service desk application.

ServiceNow Incident Field	Identity Governance Mapping
`cmdb_ci`	appName
`assignment_group`	
`category`	"request"
`subcategory`	
`description`	reason, appName, userName, account (ecmascript transformation provided)
`contact_type`	"automated"
`short_description`	
`correlation_id`	changeItemId
correlation_display	“Access review or request fulfillment item”
`caller_id`	requesterName
`opened_by`	requesterName
`severity`	"2"
`urgency`	"2"
`impact`	"2"

ServiceNow Service Catalog Request Management Integration

The Identity Governance fulfillment connector for ServiceNow Service Catalog Request Management uses the Service Catalog Request SOAP service `insert` method for creating requests in the Service Catalog application. For example, `https://your-service-url/sc_request.do?WSDL`.

The connector uses a pre-configured template that maps 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 Micro Focus technical support representative for details.

Use the following table to understand the Identity Governance mappings to the Service Catalog Request Management incident fields. Quotation marks surround static values. You can modify the static values provided in the template to conform with the options available in the target service desk application.

ServiceNow Incident Field	Identity Governance Mapping
`fulfillment type`	"request"
`cmdb_ci`	appName
`assignment_group`	
`description`	reason, appName, userName, account, fulfillmentInstructions (ecmascript transformation provided)
`contact_type`	"automated"
`request_state`	“requested”
`short_description`	
`correlation_id`	changeItemId
correlation_display	“Access review or request fulfillment item”
`requested_for`	userName
`opened_by`	requesterName
`priority`	"2"
`urgency`	"2"
`impact`	"2"

9.2.5 Viewing Fulfillment Status

The fulfillment status list allows you to view specific status categories, such as fulfillment items that have been fulfilled and fulfillment items that have ended in error or timeout conditions. The fulfillment status area also provides a way to retry, or resubmit, fulfillment items that did not succeed.

1. Log in to Identity Governance as a Global or Fulfillment administrator.
2. Select **Fulfillment > Status**.
3. Select all 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.

9.2.6 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**.
	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.

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
	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.
	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.

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
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.	Global Administrator or Fulfillment Administrator selects **Retry** or **Terminate** for the item on the Fulfillment Requests page.

9.3 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 Fulfillment 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**.

9.4 Specifying Additional Fulfillment Context Attributes

By default, the system sends basic information on how to perform fulfillment after a review or a request. Optionally one may specify additional attributes which also should be included when sending instructions to an external fulfillment target.

NOTE: Manual fulfillment target attributes are not based on 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**.

9.5 Fulfilling the Changeset for a Review Instance

An application owner can configure the application source to require manual or automated fulfillment. After a review 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 9.5.1, “Manually Fulfilling the Changeset,” on page 100
- Section 9.5.2, “Using Workflows to Fulfill the Changeset,” on page 101
- Section 9.5.3, “Automatically Fulfilling the Changeset,” on page 101
- Section 9.5.4, “Using Service Desk Fulfillment,” on page 102

Data administrators can configure the fulfillment method for an application, including configuring multiple fulfillment targets for an application based on change request types. For more information, see Section 9.2, “Configuring Fulfillment,” on page 88.

9.5.1 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, global or fulfillment administrators 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 assignment (user access review or SoD case), fulfilled by removing the permission assignment to 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 119. For more information about specific change request types, and fulfillment status, see “Configuring Fulfillment” on page 88.

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 2.1, “Customizing the Email Notification Templates,” on page 23.

For more information about performing fulfillment tasks, see “Instructions for Fulfillers” in the *NetIQ Identity Governance User Guide*.

9.5.2 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.

9.5.3 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.

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.

9.5.4 Using Service Desk Fulfillment

You can 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**. For more information, see “Configuring Service Desk Fulfillment” on page 91.

9.6 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.

9.7 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 “Viewing Fulfillment Status” in the *NetIQ Identity Governance User Guide*.

10 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 by accessing the **Configuration** menu; you can begin creating reviews. This is where a set of reviewers examine who has access to what in their environment. Administrators can create review definitions for the following types of objects:

- Access permissions, accounts, or technical roles of a set of users
- Unmapped accounts
- Accounts, which includes both mapped and unmapped accounts, and optionally, the 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

Only users with the Review Administrator or Global Administrator authorization can create and modify review definitions.

10.1 Viewing the Catalog

Before creating or editing review definitions, reviewing the data in the catalog will be helpful in determining who needs to be included in the reviews and whether reviews are needed for certain items. Some examples of the information a Review Administrator or Global Administrator can look for are:

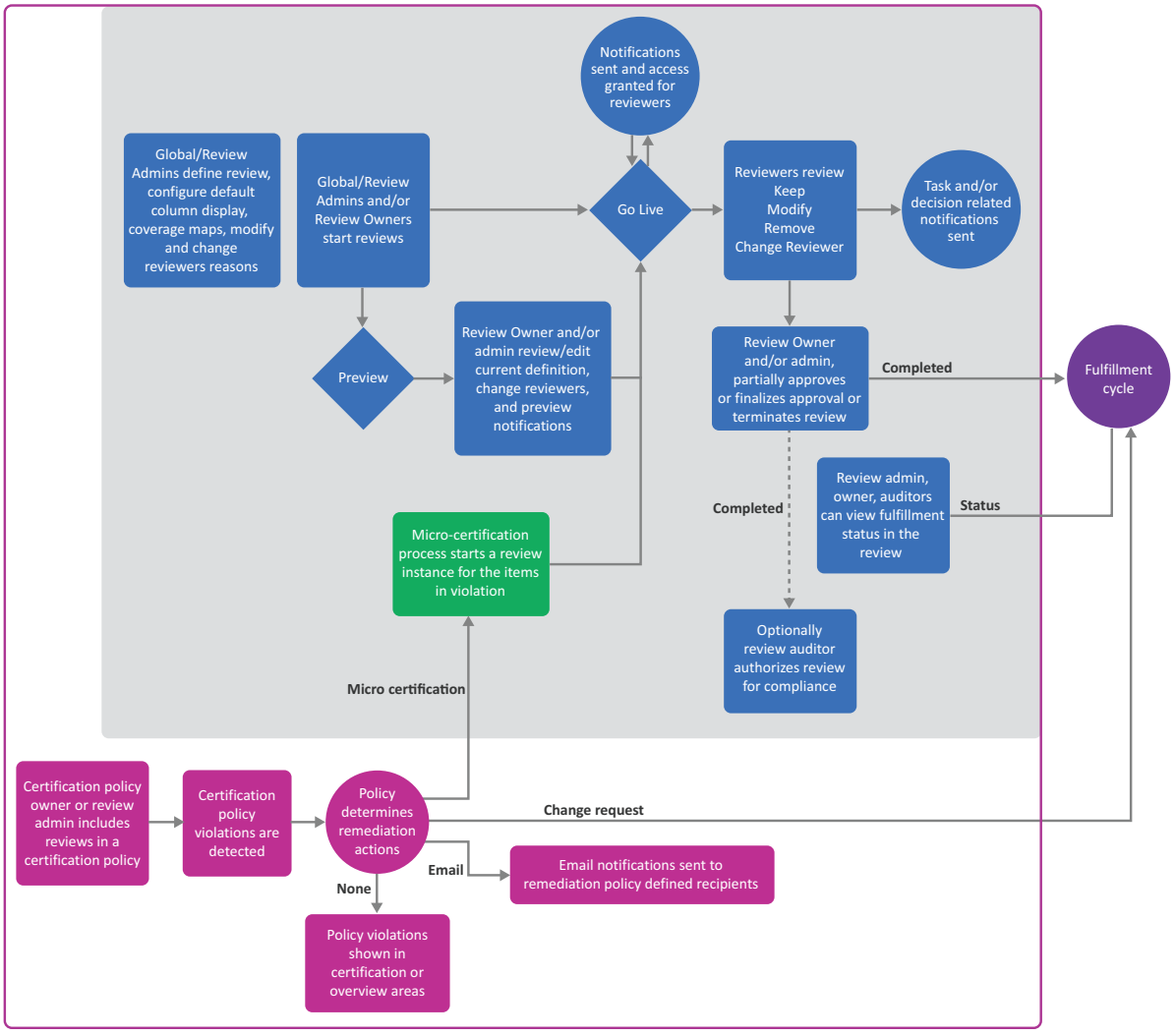
- Attributes of the user that may not be available in **Quick Info** to help determine whether the person should be included in a review or not
- The last review date of an account

NOTE: This date reflects the date when an account was last reviewed as part of an **Account Review**. Review of an user's access to an account as part of an **User Access Review** does not impact this date.

- Risk levels of users or permissions
- Association with an application
- Group or 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

10.2 Understanding the Review Process

Figure 10-1 *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.

- Review owners start, preview, monitor, complete, and terminate reviews.
- Reviewers, such as supervisors and application owners, act on review items.
- Fulfillers manage change requests.
- Auditors accept or reject completed reviews.
- Review, or data administrator create certification policies to check for violations and set remediation action which triggers remediations including micro certifications (focused reviews)

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.

For multistage reviews, if at any stage in the review an exception occurs, Identity Governance moves the items to the exception queue at the start of the review. The exception queue is handled by the escalation reviewer, if any, or if not, the review owner.

10.2.1 Creating a Review Definition

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 defines all parameters for that particular review process. Review Administrators or Global Administrators create review definitions that focus on specific types of access or access to specific systems. Review definitions 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 17, “Creating and Managing Certification Policies,” on page 175. Once a review definition is referenced in an active certification policy, it cannot be deleted. For detailed procedures about creating review definitions, see Section 10.5, “Creating a Review Definition,” on page 110.

10.2.2 Previewing a Review

Administrators can start a review run, or **review instance**, in preview mode or in live mode. In preview mode, administrators can:

- Preview review definition version, assigned reviewers, review items, and notification emails
- 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 property and reviewer changes made in preview mode will only be applicable to the current review instance. Only changes made in the **Reviews > Definitions** itself, will reflect in future review run instances.

10.2.3 Reviewing Items

When a review run, or **review instance**, is live, the server generates **review items** based on the criteria. Assigned reviewers 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 multistage review, reviewers must act on review items in the order that the stages are defined in the review definition.

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 made remain in each reviewer's list until someone submits actions for them.

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.

For multistage reviews, if at any stage in the review an exception occurs, Identity Governance moves the items to the escalation reviewer, if any, or if not, the review owner exception queue at the start of the review.

10.2.4 Setting Up 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 course of a review. You can click an email name to view who will receive the email, why they will receive it, and when they will receive it. You can either accept the defaults or customize it. You can also view the name of the email source, preview the email, and email the notification to specified email address. In addition, you can remove a default notification and add new notifications by selecting an email template provided by

Identity Governance. For information about customizing the templates, see Section 2.1, “Customizing the Email Notification Templates,” on page 23. 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 27.

10.2.5 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 becomes the default escalation reviewer.

NOTE: If a review definition specifies a group as the reviewers and a member of the group is the person being reviewed, Identity Governance sends the review item to the escalation reviewer instead of to the members of group. To prevent this, enable **Allow self review in all stages**, and Identity Governance then sends the review to the members of the group instead of to the escalation reviewer.

10.2.6 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.

- 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.

10.2.7 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 (when all multi-stage reviewers of a review item have submitted their decisions, the review item has a final decision made)
- 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

10.2.8 Fulfilling Changes and Audit Acceptance

The **fulfillment** process begins when a review run completes or when a review owner approves review items individually. For more information about fulfillment, see Section 9.5, “Fulfilling the Changeset for a Review Instance,” on page 100.

The Review Auditor, if specified, accepts or rejects the review run after the review owner approves it. Although a **review audit** is a legal stamp, accepting a review has no impact on the fulfillment of the requested changes.

10.2.9 Creating Certification Policies and Remediating Violations

A 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 10.3, “Understanding Micro Certification,” on page 109 and Chapter 17, “Creating and Managing Certification Policies,” on page 175.

10.3 Understanding Micro Certification

Micro certifications are focused reviews which involve a smaller number of review items. For example, a micro certification review could involve review items that violated a certification policy or a data policy. Micro certifications are event driven and 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, except unmapped account review type support micro certification. Multiple micro certification reviews can run in parallel with on demand or scheduled reviews that use the same review definition.

A Global, Review, or Data 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 “Customizing Review Display” on page 118.

NOTE: For information about setting up micro certification as a remediation for policy violations, see Section 3.4.3, “Calculating and Remediating Data Policy Violations,” on page 44 and Section 17.5.3, “Remediating Certification Policy Violations,” on page 179.

10.4 Selecting a Review Type

Identity Governance enables administrators to create six types of review definitions. Each review type can be defined by selecting different types of objects. Use the following table to select the review type based on the object or objects you want to review, and then create review definition using the procedures in “Creating a Review Definition” on page 110.

	User Access Review	Unmapped Accounts	Account Review	Business Role Membership Review	User Profile Review	Direct Reports Review
Identities	Y	N	Y	N	Y	Y
Permissions	Y	N	Y Permissions are grouped by accounts in this type of review. Use **User Access Review** if you want to review individual permissions.	N	N	N
Unmapped Accounts	N	Y	Y	N	N	N

	User Access Review	Unmapped Accounts	Account Review	Business Role Membership Review	User Profile Review	Direct Reports Review
Mapped Accounts	Y You can only review an user's access to an account in this type of review. Use **Account Review** for reviewing account in totality.	N	Y	N	N	N
Applications	Y	Y	Y	N	N	N
Technical Roles	Y	N	N	N	N	N
Business Roles	N	N	N	Y	N	N
Attributes	N	N	N	N	Y	N
Supervisor and Direct Reports	N	N	N	N	Y You can review and change supervisors; however, use **Direct Reports Review** to review and change direct reports as well as supervisors.	Y

10.5 Creating a Review Definition

The review definition 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.

- Section 10.5.1, "Expanding and Restricting Review Items," on page 117
- Section 10.5.2, "Scheduling a Review," on page 117

1. Log in as a Review Administrator.
2. Select **Definitions**.
3. Select **+** to create a new review definition.

4 Select the review type based on the object or objects you want to review. For more information, see “Selecting a Review Type” on page 109.

5 Name and describe the review.

6 (Optional) For **Review Instructions**, provide information that explains to reviewers what they need to do. For example, `please review these items or reassign to someone else if necessary`.

7 Specify review items using steps listed below as the options for specifying review items will differ based on the review type. After specifying review items based on review type, skip to Step 14 on page 115.

If you select	Go to
User Access Review	Step 8 on page 111
Unmapped Accounts	Step 9 on page 112
Account Review	Step 10 on page 113
Business Role Membership Review	Step 11 on page 113
User Profile Review	Step 12 on page 113
Direct Reports Review	Step 13 on page 114

8 (Conditional) For **User Access Review items**, specify the permissions, authorizations, accounts, applications, users, or a combination of these that you want to review for user access reviews.

Use the following options:

All permissions

Specifies that you want to review the selected users regardless of assigned permissions.

Select permissions

Indicates that you want to specify the permissions criteria for reviewing users.

All roles

Specifies that you want to review the selected users only if their permissions are included in a role in Identity Governance.

Select roles

Indicates that you want to specify the roles criteria for reviewing users.

All applications

Specifies that you want to review the selected users for any application. When you select this option, you then select whether to review the users based on permissions or accounts.

Select applications

Indicates that you want to specify the application criteria for reviewing users.

All users

Specifies that you want to review every user in the catalog.

Select users

Specifies that you want to enter the criteria for users to review. You can specify specific user names, browse for users, as well as define criteria such as users in a particular group.

Group

Applies only when you select **Select users**.

Specifies the names of the user groups that you want to include in the review.

Managed by

Applies only when you select **Select users**.

Indicates that you want to review all users who directly report to the specified manager.

Reporting up to

Applies only when you select **Select users**.

Indicates that you want to review all users within the reporting structure of the specified manager. For example, you might want to review a large department that includes several managers with direct reports. To do so, specify the individual to whom the managers report.

User Risk

Applies only when you select **Select users**.

Indicates that you want to review all users with a greater than, less than, or equal to your risk threshold. For example, you might want to review only users with greater than or equal to 50% risk.

Additional Criteria from the catalog

Applies only when you select **Select users**.

In the attribute definition editor of the catalog, you can specify whether an attribute can be used as review criteria. For example, Title, Department, and Job Code. Identity Governance adds these items to the select criteria menu.

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. You will have to either 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 71.

NOTE: When you narrow the review items by specifying criteria rather than selecting all users, permissions, or other types of review items, you have the following options for selecting them:

- Start typing the name and select the item you want
- Select the magnifying glass icon to browse the items
- Select **+** to add selection criteria

---

9 (Conditional) For **Unmapped Account Review items**, specify the accounts and applications you want to review.

Use the following options:

All unmapped accounts

Specifies that you want to review all unmapped accounts from all applications.

Select unmapped accounts

Specifies that you want to enter the criteria for unmapped accounts to review. You can specify specific account names as well as define criteria such as last login, last unmapped account review, or number of logins.

All applications

Specifies that you want to review all applications for unmapped accounts. When you select this option, you have an additional option to specify all or selected unmapped accounts.

Select applications

Specifies that you want to enter the application criteria for reviewing unmapped accounts.

10 (Conditional) For Account Review items, specify the accounts, identities, and applications you want to review and optionally add permission filter.

Use the following options:

Accounts

Specifies the combination of mapped and unmapped accounts to review. Selection criteria includes account attributes such as account custodian, account category, last account review date, and so forth.

Identities

Specifies that you want to review accounts regardless of users or custodians assigned to the accounts or that you want to review accounts who have specified users or account custodians.

Applications

Specifies that you want to review accounts for all applications or select applications.

Permissions

Specifies that you want to review accounts that hold select permissions or all permissions.

NOTE: *Specifying identities or applications first* will enable Identity Governance to determine if users mapped to accounts or custodians of accounts will be reviewed. In addition, selecting specific users instead of all users will enable you to indicate whether the users to be reviewed are users mapped to an account, custodians of an account, or either mapped users or account custodians. For more information, see Section 10.5.1, “Expanding and Restricting Review Items,” on page 117.

---

11 (Conditional) For **Business Role Membership Review**, specify the business roles you want to review.

Use the following options:

All business roles

Specifies that you want to review all business roles.

Select business roles

Specifies that you want to enter the criteria for business roles to review. You can specify specific business role names as well as define criteria such as owners or risk.

12 (Conditional) For **User Profile Review**, specify attributes you want to review for all users or selected users.

Use the following options:

All users

Specifies that you want to review attributes for every user in the catalog.

Select users

Specifies that you want to enter the criteria for users whose attributes you to review. You can specify specific user names, browse for users, as well as define criteria such as users in a particular group.

Group

Applies only when you select **Select users**.

Specifies the names of the user groups that you want to include in the review.

User Risk

Applies only when you select **Select users**.

Indicates that you want to review all users with a greater than, less than, or equal to your risk threshold. For example, you might want to review only users with greater than or equal to 50% risk.

Additional Criteria from the catalog

Applies only when you select **Select users**.

In the attribute definition editor of the catalog, you can specify whether an attribute can be used as review criteria. For example, Title, Department, and Job Code. Identity Governance adds these items to the select criteria menu.

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. You will have to either 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 71.

NOTE: When you narrow the review items by specifying criteria rather than selecting all users, permissions, or other types of review items, you have the following options for selecting them:

- Start typing the name and select the item you want
- Select the magnifying glass icon to browse the items
- Select **+** to add selection criteria

Attributes

Specifies which attributes of the user you want to review. For example, Email, Employee Status, and Department.

NOTE: Attributes must have been selected to be **Allow to be reviewed** under **Listable Options** in **Data Administration > Identity Attributes** page to be available here as an option.

---

13 (Conditional) For **Direct Reports Review** specify direct reports or supervisors whose reporting relationship you want to review.

All users

Specifies that you want to review all direct reports or all supervisors in the catalog.

Select users

Specifies that you want to enter the criteria for users whose reporting relationship you want to review. You can specify specific user names, browse for users, as well as define criteria such as users in a particular group.

Group

Applies only when you select **Select users**.

Specifies the names of the user groups that you want to include in the review.

User Risk

Applies only when you select **Select users**.

Indicates that you want to review all users with a greater than, less than, or equal to your risk threshold. For example, you might want to review only users with greater than or equal to 50% risk.

Additional Criteria from the catalog

Applies only when you select **Select users**.

In the attribute definition editor of the catalog, you can specify whether an attribute can be used as review criteria. For example, Title, Department, and Job Code. Identity Governance adds these items to the select criteria menu.

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. You will have to either 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 71.

NOTE: When you narrow the review items by specifying criteria rather than selecting all users, permissions, or other types of review items, you have the following options for selecting them:

- Start typing the name and select the item you want
- Select the magnifying glass icon to browse the items
- Select **+** to add selection criteria

---

14 (Optional) Further expand or restrict **User Access Review items** and **Account Review items** by selecting additional options. For more information, see "Expanding and Restricting Review Items" on page 117.

15 (Optional) Select **Estimate Impact** to view the number of users, permissions, roles, accounts, and review items affected by the review.

NOTE: Identity Governance calculates the *approximate* number of review targets. Business role authorizations is 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.

16 (Optional) For **Review Options**, select any additional options that apply to this review. For example, you can require comments for certain actions and allow review owners to override decisions.

17 (Optional) Specify the reviewers you want to participate in the review.

For more information about types of reviewers, see Section 10.9, "Specifying Reviewers," on page 119.

18 (Optional) To create a serial, multistage review, select **Add Reviewer**.

This allows you to specify multiple individuals who review the identity's permissions in the order listed in the definition. For more information, see Section 10.9, "Specifying Reviewers," on page 119.

19 (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 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 "Improving Performance in Large Scale Reviews" on page 121.

---

20 (Optional) For **Escalation**, specify the following options:

20a Specify the **Escalation Reviewer** by entering user names or by using the search and selecting identities, groups, or business roles. If you do not specify a value, Identity Governance escalates tasks to the Review Owner.

20b For **Escalation timeout**, specify the amount of time allowed for the Reviewers to complete their tasks. You must use whole numbers for the value.

21 (Optional) For **Duration**, set or change any of the following options:

21a For **Review period**, specify the length of time allowed for the review run.

21b For **Expiration policy**, specify what happens when a review expires without being completed.

21c For **Partial approval policy**, specify whether partial approvals are allowed and if so, whether or not partial approvals will occur automatically.

21d For **Validity period**, specify the length of time that the reviewed data will be valid. For example, if you intend to run the review twice a year, specify `6 months`.

22 (Optional) For **Notifications**, customize and add recipients or remove default review notifications. Click **Email source preview** to preview email HTML source and specify a recipient and **Send** the rendered version of the email. Click **Add notification** and specify options to add more notifications based on different criteria.

NOTE: You can specify only one recipient in the **To** field and multiple recipients in the **CC** field. The read-only **Review terminated notice** goes to reviewers, review owners, escalation reviewers, and auditors when a review ends. You cannot change the recipients.

---

23 (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 "Scheduling a Review" on page 117.

24 (Optional) For **Default Reviewer Display Preferences**, specify the default grouping and default sort for the reviewer display. Specify default reviewer columns by using display columns previously customized for each review type using the **Configuration > Review Display Customization** menu, or set default columns for the current review definition.

NOTE: If needed, the reviewer can change the default grouping for the current 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.

---

25 Save the review.

10.5.1 Expanding and Restricting Review Items

After specifying review items using different selections of users, permissions, accounts, and roles, administrators can further expand or restrict items being reviewed in an User Access Review and an Account Review by selecting additional options. The additional options are based on your initial criteria for review items. The following table provides a few examples of available options and special conditions if any.

When...	If you want to...	Select
Creating user access review definition	Enable reviewers to make decisions on accounts that grant specified permissions for the selected set of users	**Additionally review accounts for the selected users and permissions**
Creating account review definition	Enable reviewers to review both users mapped to the accounts and users who are account custodians when reviewing mapped accounts	**Selected users are either mapped users or account custodians** **NOTE:** This option will be available when you *initially specify select users* and then specify accounts.
Account Review	Restrict review items to only users mapped to the accounts or to users who are account custodians when reviewing mapped accounts or to include account custodians as review items when reviewing unmapped accounts	**Selected users are mapped users to the accounts** or **Selected users are account custodians of the accounts** **NOTE:** These options will be available when you *initially specify users or applications* and then specify accounts.
User Access Review and Account Review	Restrict review items to items that were not authorized by a business role	**Review only items that have not been authorized by a business role**

NOTE: In order 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 *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.

10.5.2 Scheduling a Review

Identity Governance calculates schedule based on specified start time, time interval, and time zone. Time interval can be daily, weekly, monthly, or yearly. For all schedules the time period end date is adjusted automatically based on Java `add` calendar method. For monthly and yearly schedules, the next review always starts in a month or a year regardless of the number of days in a month or year. The following table provides a few examples of a monthly schedule.

Start time	Next monthly scheduled start time
Tue Jan 01 00:00:00 EST 2019	Fri Feb 01 00:00:00 EST 2019
Wed Jan 30 00:00:00 EST 2019	Thu Feb 28 00:00:00 EST 2019
Sun Mar 31 00:00:00 EDT 2019	Tue Apr 30 00:00:00 EDT 2019

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.

10.6 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.

10.7 Customizing Review Display

Identity Governance customizes display based on user authorization and the context of your action. In addition it also enables you to customize review display by:

- Dragging and dropping attributes that can be displayed as columns by review type in the **Configuration > Review Display Customization** area
- Selecting default grouping, sort, and reviewer columns in the **Review Definition > + > Default Reviewer Display Preferences** section

  NOTE: Only attributes selected in **Review Display Customization** will appear as a column in **Default Reviewer Display Preferences**.

- Dragging and dropping column options in the review definition and review items list areas by clicking the gear icon and viewing additional columns available for display

To select user attributes that can be displayed:

1. Log in to Identity Governance as a Global or Review Administrator.
2. Select **Configuration** > **Review Display Customization**.
3. For each review type, drag-and-drop columns to add, rearrange, or remove a column from reviewer display.
4. Click **Save**.

NOTE: To show attribute in expanded details, 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 > User**, and then select **Display in Quick Info views** under **Listable Options**.

10.8 Configuring Reasons for Review Actions

Identity Governance allows you to configure reasons for review actions for analytical and reporting purposes. Global or Review Administrator 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 an **User Access Review** or selects **Modify with instructions** in an **Account Review**.

1. Log in to Identity Governance as a Global or Review Administrator.
2. Select **Configuration** and **Change Reviewer Reasons** or **Modify Review Item Reasons**.
3. To add a new reason, click **+** and specify a reason. For example, you can add 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.

10.9 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 of the following options:

User Access	Unmapped Accounts	Accounts	Business Role Membership	User Profile	Direct Reports
Supervisor of the individual being reviewed	Owner of the application being reviewed	Supervisor of the individual being reviewed	Supervisor of the individual being reviewed	Supervisor of the individual being reviewed	Supervisor whose direct reports are to be reviewed
Owners of the applications being reviewed	Selected users or groups	Owner of the application being reviewed	Business role owner	Holder of the permission being reviewed, called self review	Supervisor's supervisor whose downline reports are to be reviewed
Owners of the permissions being reviewed (not available for roles reviews)	Account custodian	Owner of the account being reviewed	Selected users or groups	Selected users or groups	Selected users or groups

User Access	Unmapped Accounts	Accounts	Business Role Membership	User Profile	Direct Reports
Holder of the permission being reviewed, called self review	Business role	Selected users or groups	Business role	Business role	Business role
Selected users or groups		Account custodian			
Coverage map		Coverage map			
Business role		Business role			

For more information about owners of applications and permissions, see Section 7.2, “Understanding Identity, Application, and Permission Management,” on page 68. For more information about coverage maps, see “Using Coverage Maps” on page 18.

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 own 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 of the reviewers share 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.

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 Exceptions stage with these review items in that stage.

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 an users, groups, and business roles as Escalation Reviewers. If you do not specify an Escalation Reviewer, the owner of the review must perform these tasks. 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 review authorizations, see Section 1.1.2, “Runtime Authorizations,” on page 14.

10.10 Downloading and Importing Review Definitions

You can download review definitions as JSON files and import them later into another environment.

To download or import review definitions:

1. Log in to Identity Governance as a Review or Global Administrator.
2. Under **Reviews**, select **Definitions**.
3. Select a definition or all the definitions.
4. Select **Download**.
   - **4a** (Optional) Download included business roles, technical roles, and associated applications.
   - **4b** Select **Save**.
5. If you make changes, or want to import previously downloaded review definitions into another environment, select **Import Review Definitions**.

   NOTE: Review definitions import may 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 configuration settings, see Appendix A, “Running the Identity Governance Configuration Utility,” on page 191.

   ---
6. Navigate to the review definitions JSON file, select the file to import, and click **Open**.
7. Identity Governance detects whether you are importing new or updated roles and whether the updates would create any conflicts or have unresolved references.
8. Select how to continue based on what information is displayed.

10.11 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 these options should be used with caution.

Disabling review statistics calculations

Use the global configuration 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 or 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 global configuration setting `ap GLOBAL iac.review.display.materializedViews.enabled` 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 `ap GLOBAL iac.materializedViews.oracleTableSpace` *`Tablespace`* (example, ap 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 materialized view is not initially enabled using the global configuration utility, **Cache review item names** check box will not be displayed. For small scale reviews, caching of review item names is *not* recommended. For more information about the configuration utility, see Appendix A, “Running the Identity Governance Configuration Utility,” on page 191.

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**. In addition, you can **Enable** or **Disable** the caching of review item names for that review instance.

11 Running a Review Instance

When you start a review in live mode (on demand) or when view is started by defined schedule or when a event triggers micro certification, Identity Governance initiates a running review instance and notifies any person or role specified in the **Notifications** settings of the review definition. A review instance will always be associated with the version of the review definition used to start it. 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 "Managing a Review in Live Mode" in the *NetIQ Identity Governance User Guide*.

11.1 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 1.1.2, "Runtime Authorizations," on page 14. For automated fulfillment configurations, Identity Governance sends fulfillment changes to configured systems. For more information about automated fulfillment, see Section 9.2, "Configuring Fulfillment," on page 88.

For more information about completing review tasks, see "Instructions for Review Owners" and "Instructions for Reviewers" in the *NetIQ Identity Governance User Guide*.

11.2 Verifying and Approving a Review Instance

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**.

For more information, see "Approving and Completing the Review" in the *NetIQ Identity Governance User Guide*.

12 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.

12.1 Understanding Separation of Duties

When any one 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 company. By creating policies to keep any one person from having too much responsibility, the SoD Administrator enables Identity Governance to identify users with access to company assets that should be reviewed. Having these SoD policies puts access control rules over your business systems to give you the ability to show auditors the automated protection that Identity Governance provides.

When you have active SoD policies, Identity Governance provides the ability to check for violations and warns of violations when executing actions such as performing reviews, defining roles, requesting access, approving access, or examining manual fulfillment requests.

Based on your SoD policies, Identity Governance not only enables you to identify SoD violations in your current data, it also enables you to detect SoD violation that *might* occur in the future if a set of access requests are fulfilled. When *potential* SoD violations are detected, the violations are listed on the **Access Request > Approvals > SoD Violations** page if approvals are required. 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, potentials violations do not require approvals then Identity Governance will directly send the requests to fulfillment.

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. For more information about reviews, see Section 10.2, “Understanding the Review Process,” on page 104 For more information about SoD violations, SoD cases and potential SoD violations, see Chapter 13, “Managing Separation of Duties Violations,” on page 131.

12.2 Creating and Editing Separation of Duties Policies

After you have published data, you can create separation of duties (SoD) policies that Identity Governance uses to alert you of possible violations. When you have active SoD policy definitions, Identity Governance lists violations and creates cases for you to review and approve or send to fulfillment for correction. Users with the Separation of Duties Administrator or Global Administrator authorization can create and modify SoD policies.

1. Under **Policy**, select **SoD**.
2. Select **+** to create a separation of duties policy.
3. (Optional) Select **Active** to have Identity Governance discover violations of the policy and create SoD violations and cases.
4. Provide the required information. For more information about defining SoD conditions, see "Defining Separation of Duties Conditions" on page 128.

   NOTE: Policy names must be unique. When Identity Governance checks for uniqueness, case is not considered. Therefore, Identity Governance considers SoD1 and SOD1 to be equivalent.
5. (Optional) Specify potential SoD violation approval policy for the current policy by overriding global policy. For more information, see "Overriding Global Potential SoD Violation Approval Policy" on page 127.
6. (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. For more information, see Section 12.3.3, "Deciding what Occurs when the Separation of Duties Policy is Violated," on page 127.
7. (Optional) Click **Estimate Violations** to see an estimate of the number of violations of this policy. You must add SoD conditions to make this button active.
8. Save your settings.

After a policy has been created and activated, some of the permissions or authorizations listed in the policy's conditions might be deleted. When this happens, the policy is marked as invalid, and all of the policy's currently open SoD cases 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.

12.3 Understanding the Separation of Duties Policy Options

When you create an SoD policy, you must define what conditions make up the policy, what happens when the policy is violated, and how to solve the violation. Use the following information to create the SoD policies that work best in your environment.

- Section 12.3.1, "Providing Resolution Instructions for the Separation of Duties Policies," on page 127
- Section 12.3.2, "Overriding Global Potential SoD Violation Approval Policy," on page 127
- Section 12.3.3, "Deciding what Occurs when the Separation of Duties Policy is Violated," on page 127
- Section 12.3.4, "Defining Separation of Duties Conditions," on page 128

12.3.1 Providing Resolution Instructions for the Separation of Duties Policies

When you create the SoD policy, you can add resolution instructions in the **Resolve** field. You can embed HTML links in these instructions to point to additional information or instructions for a user to follow when reviewing a 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.

12.3.2 Overriding Global Potential SoD Violation Approval Policy

The global potential SoD violation approval policy determines if approval is required for potential SoD violations and if required, whether self approval is allowed. Only users with Global Administrator or Access Request Administrator authorization can set global potential SoD violation approval policy. However, SoD Administrator and policy owners specify potential SoD violation approval polices for each SoD policy and override the global policy by selecting the **Override global potential SoD violation approval settings**.

NOTE: The override only applies to potential violations that are detected for that SoD policy. For more information, see “Understanding Potential SoD Violations” on page 134 and “Setting Global Potential SoD Violation Approval Policy” on page 172.

12.3.3 Deciding what Occurs when the Separation of Duties Policy is Violated

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 32768 days.

You add these compensating controls when you create the SoD policy in the **Compensating Controls** field.

12.3.4 Defining Separation of Duties Conditions

An SoD policy specifies what combinations of permissions and roles are illegal for a user to hold by defining one or more conditions. Each condition specifies some combination of permissions and roles that are illegal. Most of the time, a single condition suffices, but there are scenarios where you must define multiple conditions to cover more complicated combinations.

Identity Governance tests a user's permissions and roles against a condition to see if the user has the combination of permissions and roles specified in the condition. If the user's permissions and roles match the condition, the user violates that condition. If a user's permissions and roles violate **every** condition in the SoD policy, the user is in violation of the 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. Identity Governance uses the same procedure for unmapped accounts as it does for users. It tests if the account has the combination of permissions specified in the condition. If the account's permissions match the condition, the account violates that condition. If an account's permissions violate **every** condition in the SoD policy, the account is in violation of the policy.

Many simple policies require only a single condition to specify illegal permission and role combinations. More complex combinations require multiple conditions, but it is probably very rare that you need more than two conditions.

A condition consists of two parts:

- A list of one or more permissions and roles that Identity Governance tests against a user's permissions and roles. The list can consist of all permissions, all roles, or a mixture of permissions and roles.
- 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 of the listed permissions and roles. This the most commonly used type of condition. You can specify most illegal combinations of permissions and roles using a single condition.

  User has one or more of the following

  A user violates this condition if the user has any of the specified permissions and roles. The condition must always be used in conjunction with one or more of the other conditions. Identity Governance does not allow an SoD policy with a single condition of this type.

  NOTE: Identity Governance does not allow a SoD policy that would make it illegal for a user or account to possess a single permission or role all by itself. For example, a policy with a single **User has all of the following** condition that lists a single permission or role, or a policy that has a single **User has one or more of the following** condition.

  To enforce this restriction, Identity Governance tests each permission or role specified in a policy's conditions. For each listed permission and role, it simulates a dummy user that possesses exactly that one permission or role and determines if the dummy user would violate all of the conditions of the policy. If it does, the policy is invalid and Identity Governance does not allow the SoD policy to be saved in that state.

  User has more than one of the following

  A user violates this condition if the user has two or more of the specified permissions and roles. 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.

12.4 Downloading and Importing Separation of Duties Policies

You can download SoD policies in JSON format as a backup to edit offline. You can also import SoD policies by uploading a JSON file.

1. Under **Policy**, select **SoD**.
2. Select one or more policies from the list, and click **Actions** > **Download**.
3. Select options you want to download with each policy, and then click **Download**.
4. To import policies, click **Import Separation of Duties Policies** on the **Policy > SoD** page.
5. Navigate to the file, select the file to import, and click **Open**.
6. Identity Governance detects whether you are importing new or updated policies and whether the updates would create any conflicts.
7. Select how to continue based on what information is displayed.

13 Managing Separation of Duties Violations

Identity Governance provides the ability for 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 violations are found. SoD administrators and policy owners 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 9.5, “Fulfilling the Changeset for a Review Instance,” on page 100.

13.1 Understanding SoD Violation versus SoD 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 SoD violation detection. For example, publishing identities and accounts, creating, changing, or deleting roles all trigger 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.

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.

13.2 Listing SoD Violations or SoD Cases

There are multiple places where actual SoD violations may be listed and the associated SoD case managed. Which you use depends on what your needs are.

SoD violations for a particular user or account

1. Under **Catalog**, select **Users** or **Account**.

2. Select the user or account you want to see.
3. Select the **Separation of Duties Policy Violations** tab. Identity Governance only displays this tab for a user or account if there are active violations.

NOTE: This tab shows only the SoD violations whose associated SoD case is currently open.

SoD violations for a particular SoD policy

1. Under **Policy**, select **SoD**.

   Ensure that you display the **# Users** and **# Unmapped Accounts** columns.
2. Select the count in the **# Users** column to see the list of users violating the policy.
3. Select the count in the **# Unmapped Accounts** column to see the list of unmapped accounts violating the policy.

NOTE: This tab shows only the SoD violations whose associated SoD case is currently open.

SoD violations for a particular SoD case

1. Under **Policy**, select **Violations**.
2. Filter on SoD case state list by selecting any of the state icons, for example **Total**, **Not Reviewed**, **Approved**. You can also perform advanced searches. For more information, see Section 7.4.3, “Managing Filters,” on page 74.

13.3 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

  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.

13.4 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 an SoD violation is first detected, an SoD case is created, and it is put into this state. It 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 whether to request that certain permissions be removed in order to resolve it.
Approved	SoD case has been looked at by a user and was approved. Approval means the user determined that the SoD violation could continue for a certain period of time – the control period. There may be one or more compensating controls that were specified. Compensating controls are basically the conditions under which the approval was granted, that is it is expected that the compensating controls will be in effect during the approval period.
Approval Expired	SoD case was approved at one time, but the control period has expired.
Resolving	SoD case has been looked at by a user, and the user 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.
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.

13.5 Approving and Resolving an SoD Violation

Approving an SoD violation records that the violation has been recognized and approval has been given to allow the violation to continue for some time period. A comment is always required when approving a violation. You must also specify a time period (days) that the violation is allowed to continue. If the SoD policy has defined compensating controls, you can select one or more controls. This allows you to state what controls you want to be enforced while the violation is allowed to continue.

Resolving an SoD violation allows you to specify what permissions or roles you want removed from the user or account. Upon selecting permissions or roles to remove, changesets are generated which then show up in fulfillment. You can visit the fulfillment pages to perform the usual types of fulfillment actions. For more information, see Section 9.5, “Fulfilling the Changeset for a Review Instance,” on page 100.

IMPORTANT: The closing of an SoD case is not the same thing 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.

13.6 Closing an SoD Case

Identity Governance automatically closes an SoD case on any of the following conditions:

- It 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.

13.7 Understanding Potential SoD Violations

Identity Governance not only enables you to identify SoD violations in your current data, it also enables you to detect SoD violation that *might* occur in the future if a set of access requests are fulfilled. When potential SoD violations are detected, Identity Governance determines if approval is required for the potential SoD violation before processing the request. The SoD policy or the global potential SoD violation approval policy determine if approval of potential SoD violations is required and whether self-approval is allowed. If approval is required, Identity Governance creates a potential SoD violation approval task that is assigned to SoD policy owners and SoD administrators to handle. SoD policy owners and SoD administrators can see a list of the potential SoD violations they need to approve or deny via **Access Request > Approvals > SoD Approvals** page.

NOTE: Only users with Global Administrator or Access Request Administrator authorization can set global potential SoD violation approval policy. For more information, see “Setting Global Potential SoD Violation Approval Policy” on page 172.

13.8 Approving or Resolving Potential SoD Violations

Access requests can contribute to one or more potential SoD violations. If approval is required for potential SoD violations (as specified in the SoD policy or via 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 SoD policy owners or SoD administrators.

All request items that contribute to the potential SoD violation must either be approved or denied to clear the potential violation. Denying request items may 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 would still exist after approving or denying all of the contributing request items, the potential SoD violation is considered **preapproved**, Identity Governance will prompt the SoD policy owner or SoD administrator 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 happens to occur, 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.
- (Optional) **Compensating Control**. If compensating controls were specified in the SoD policy, the selection here indicates which compensating controls applies to the preapproval.

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 had been 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 request status, see “Requesting Access and Viewing Timeline” in the *NetIQ Identity Governance User Guide*.

14 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 each role's membership policy.

14.1 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.

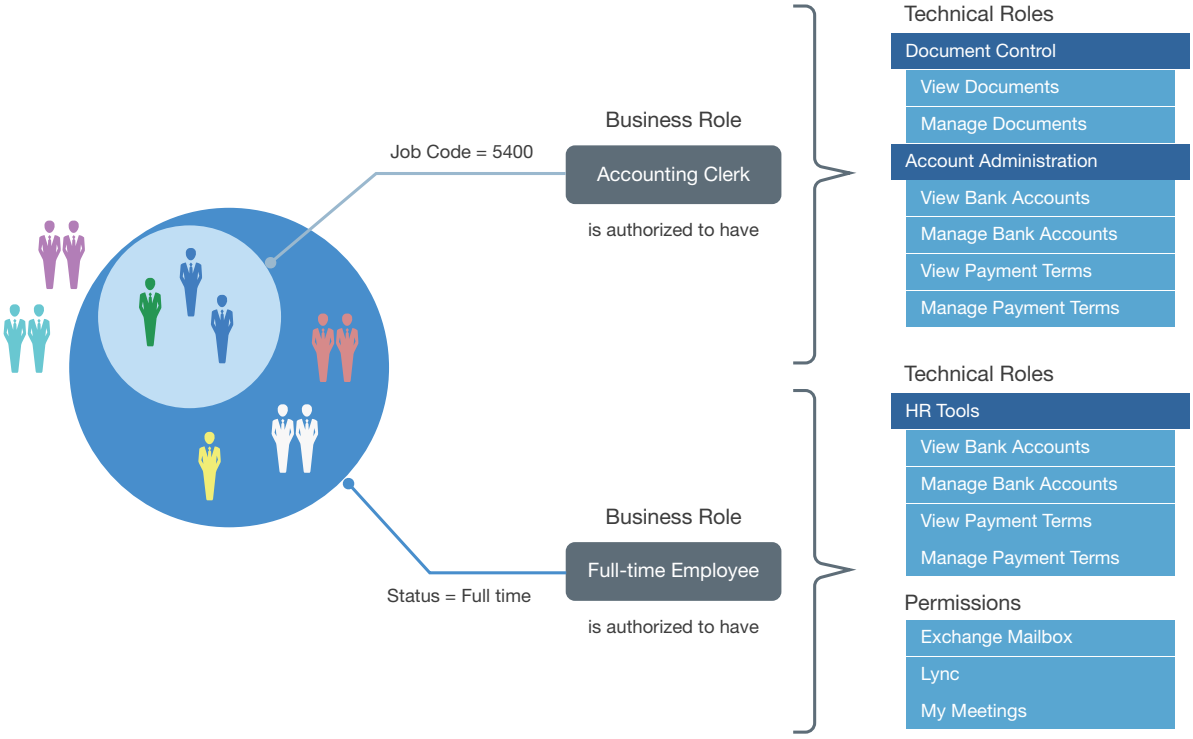
Business roles organize people by their business function and user based attributes to solve questions of what users should have access to because of who they are or what they need or might have an option to request without additional approval. Business roles authorize **resources** (permissions, technical 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 14-1 contains an example of how the different types of roles overlap. The company's 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 as they have been pre-approved by the policy. This saves you time, effort, and error and enables controlled access through business roles. To understand how your entitlement

assignments confirm to your business polices, you can view the **Role Leverage** widget on the **Overview** page. For more information, see “Viewing Entitlement Assignments Statistics to Leverage Roles” on page 189.

Figure 14-1 *Detailed Example of the Overlap between Business Roles and Technical Roles*

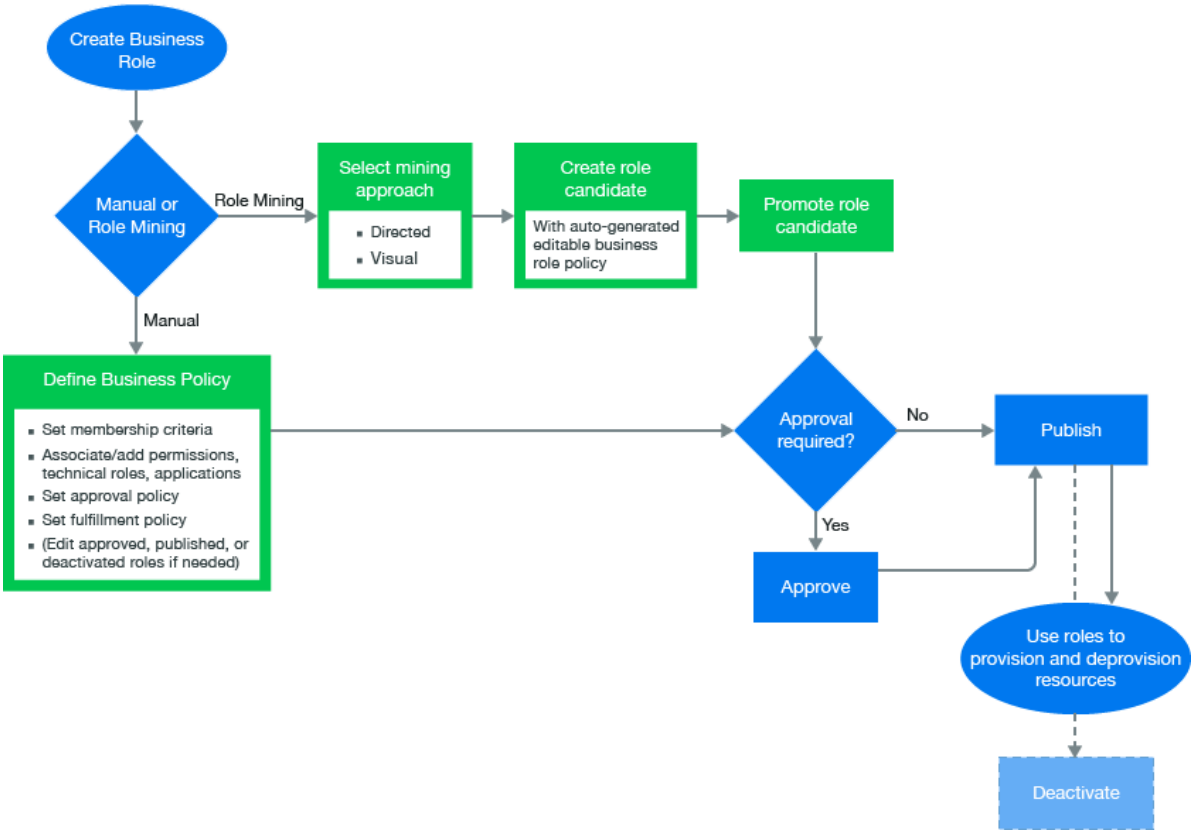


NOTE: This chapter primarily discusses business role policy concepts and procedures. For information about technical roles, see “Managing Technical Roles” on page 75

14.2 Understanding Business Roles

The workflow shows the business role process in Identity Governance.

Figure 14-2 *Business Role Workflow*



The primary purpose of business roles is to 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 each business role's authorization policy. A business role authorizes resources and generates requests, but does not assign resources.

- Section 14.2.1, "Understanding Business Role Access Authorizations," on page 139
- Section 14.2.2, "Understanding Business Role Mining," on page 140
- Section 14.2.3, "Understanding Business Role States," on page 140

14.2.1 Understanding Business Role Access Authorizations

The Business Role or Global administrator creates, modifies, and defines business roles and manages business role policies. The Business Role or Global administrator can delegate administrative actions by specifying a Role Owner or a Role Manager for each business role. The Role Owners can view and approve business roles but cannot edit business roles. The Role Managers can edit business role membership and resource authorizations, submit business role for approval, promote role candidates, publish roles, and deactivate roles. If the administrator did not specify Role Owners in the business role definition, then Identity Governance automatically assigns the Business Role or Global administrator who created the role as the Role Owner. For more information about access authorizations, see Section 1.1, "Understanding Authorizations in Identity Governance," on page 11.

14.2.2 Understanding Business Role Mining

Identity Governance uses advanced analytics to mine business data and identify role candidates. This process of discovering and analyzing business data in order to group multiple users and access rights under one business role candidate is called **Business Role Mining** or **Role Discovery**. The Global or Business Role 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 as well as technical roles with common permissions. Identity Governance uses two approaches to business role mining to identify business role candidates.

- **Directed Role Mining** enables administrators to direct the mining based on user attributes they specify. If administrators are not sure which attribute to select, they can search for recommended attributes, and select an attribute from the recommended bar graph which displays the strength of attributes that have data. Additionally, directed role mining also enables them to specify minimum membership and coverage percentage to identify role candidates. For example, when an administrator selects “Department” as the attribute to group candidates by, the mining results displays the list of items consisting of department name with the associated users, permissions, roles, and application as role candidates.
- **Visual Role Mining** enables administrators to select role candidates from a visual representation of the user attributes. The attribute circle’s width displays the strength of the recommendation, and the width and darkness of the lines indicate the affinity of the attribute to other user attributes. Administrations can customize the mining results by modifying the default maximum number of results, minimum potential members, and number of automatic recommendations.

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 183.

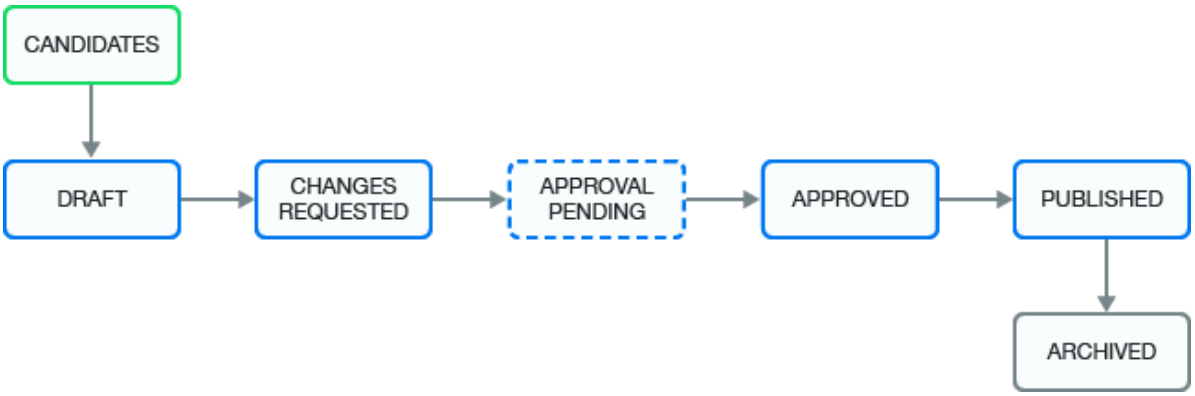
After previewing users and their associated permissions, technical roles, and applications, administrators can select one or more items from the list to create either role candidates for each selected item in the list or a single candidate for all of them. Additionally, Identity Governance could group common permissions under a technical role, and generate 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 approve or publish the candidate as a role. Administrators can also select multiple role candidates and submit them for approval, publish them, or delete them using the **Actions** options.

14.2.3 Understanding Business Role States

After you create or Identity Governance mines a business role, it contains many states during its life cycle. From beginning to end, the business role goes through the states in Figure 14-3 on page 141. For detailed description of the states see the following table.

Figure 14-3 *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 (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	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. Identity Governance never displays archived business roles in the application.

14.3 Defining Business Roles

In order to use business roles, you must create a business role and define a membership policy and an authorization policy for the business role based on your business needs.You can create a business role either manually or use role mining analytics.

To define a business role:

1 Log in to Identity Governance as a Business Role or Global Administrator.

2 Under **Policy**, select **Business Roles**.

3 Select the **Mining** tab if you want the system to recommend role candidates, and based on your selection auto-create membership expression and authorize associated permissions, technical roles, and applications.

NOTE: If you are confident about your data and want to define membership expression manually, select **+** on the **Business Roles** page to create a new business role and then proceed to Step 12.

If	Then
You are not sure about where to start	◆ Select **Visual Role Mining**. ◆ (Optionally) Click the gear icon to modify the maximum number of results to display for recommended attributes, and the required minimum number of members for each role candidate. ◆ Click an attribute node (circle) to select a role candidate. **WARNING:** You might not see any recommendations if the **Settings > Minimum potential members** is set too high or when the role mining settings in **Configuration > Analytics and Role Mining Settings** does not meet the required conditions. For more information see, "Configuring Analytics and Role Mining Settings" on page 183.
You want to direct the mining by specifying user attribute	◆ Select **Directed Role Mining**. ◆ Specify the user attributes by entering the user attribute names or by searching and selecting the attributes based on the strength of the recommendation. ◆ Specify a minimum number of times the attribute value must occur across users, or the percentage of all users who must have the attribute value. ◆ Specify additional coverage criteria. **NOTE:** Identity Governance uses the permission, technical role, and application coverage fields to determine which authorizations are auto-populated in the business role candidate. For example, if permission coverage is at 50% then 50% of the members must hold a 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. ◆ Save the specified values to trigger the user catalog analysis. ◆ (Optional) Click the gear icon to adjust the settings, and save the settings to refresh the candidate suggestions.

4. Select one or more items from the **Directed Role Mining > Mining Results** list or **Visual Role Mining > Role Candidates** list.
5. Click **Create Candidates**.
6. **Create separate candidates for each criteria** or **Create a single business role candidate**. If the latter, specify a name for the business role.
7. (Optional) Select **Create associated technical for common permissions** to generate the technical roles with users who have the same permissions.
8. (Optional) Select **Group permissions added to technical roles by application** to create application-specific technical roles.
9. In the **Role** tab, click the newly generated inactive role to view the role description.
10. Click **Edit**.

NOTE: Identity Governance creates the role candidate in a pending state and administrators must promote it before anyone can approve the role candidate or publish it as a role. Ensure that the membership criteria and authorizations are as you want them to be before publishing.

---

11. Select **Yes** to promote the role candidate.
12. Specify the following information to create the business role:

Name and Description

Modify the auto-generated name to a unique name and edit the description for the business role.

Grace period

Specify a grace period. 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

Specify the importance of the business role in terms of limited access and security.

For example, you might want to review access to business roles with a **high** risk more often than business roles with a **mild** risk.

Included Membership

Optionally, specify roles whose membership criteria, users, and groups you want to include in the new business role. When combining the included roles, Identity Governance only includes published roles membership and eliminates duplicates. For example, you can include role A and role B in the membership of role C. Then, role C becomes the union of role A and role B along with any membership criteria specified for role C.

NOTE: Excluded members of the including role take precedence over inclusion of included business role members. For example, when role C includes A, and A has a member User1, and role C excludes User1 then Identity Governance also excludes the user.

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 Identity Governance's 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 on. To optimize specific SELECT statements that might not be performing as expected, contact your database administrator.

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 Sales group and exclude Contractors group. Then, Identity Governance excludes a user who belongs to both of those groups because exclusion takes precedence over inclusion.

---

13 Select the **Authorizations** tab, then define the following:

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 not. Specify whether Identity Governance should or should not 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.

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 (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.

Technical Role

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 not. Specify whether Identity Governance should or should not 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.

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 only applies 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 specify 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 which those permissions might contain.

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.

NOTE: Applications must have an account collector to allow you to specify automatic grant or revoke.

For more information about authorizing permissions, technical roles, and applications, see Section 14.5, “Adding Authorizations to a Business Role,” on page 146.

14 Select the **Owners and Administration** tab to assign the following:

- Role owner
- Role manager
- Fulfiller
- Categories
- Approval Policy

Identity Governance makes default assignments for the owner, and fulfiller, and assigns a default approval policy to the business role if you do not make selections on this tab.

15 (Optional) On the **Membership** tab, select **View Membership** to view list of business role members.

NOTE: During migration or upgrades, you must always run publication to refresh list of business role members. For more information about publishing data sources, see Chapter 6, “Publishing the Collected Data,” on page 63.

---

16 Under **What-if Scenarios**, select **Estimate Publish Impact** and **Analyze SoD Violations** to respectively view types of changes and SoD violations information.

17 (Conditional) Resolve SoD violations or edit business role definition to resolve any issues. For more information about SoD violations, see “Approving and Resolving an SoD Violation” on page 134.

18 Select **Save** to save your modifications to the mined business role definition.

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 pertaining to the business role.

After you have created the business role and assigned owners and administrators, the business role is ready for approval or it is ready to be published 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 14.6, “Adding a Business Role Approval Policy,” on page 147.

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 14.7, “Publishing or Deactivating Business Roles,” on page 148.

14.4 Authorizing User Access Through Business Roles

Membership policy determines which users are members of a business role. 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 a user becomes a member of a role (matching a membership expression, explicitly included, and so forth), they are authorized to have the resources specified in the business role for as long as they are a member 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.

14.5 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. That means that the business role authorizes all business role users and groups for all of the permissions included in each technical role. For more information, see Section 7.5, “Managing Technical Roles,” on page 75.

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

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), the authorization policy can authorize the user for permission that the Identity Manager role contains.

Authorized Technical Roles

The authorization policy can authorize a user in the business role for technical roles included in the authorization policy. If an authorized technical roles 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).

Authorized Applications

The authorization policy can authorize a user in the business role to have accounts in the applications included in the authorization policy.

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 they are 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 only applies 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 request only for the top-level role and then Identity Manager rules apply for all children authorizations. For more information, see Section 14.11, “Automated Access Provisioning and Deprovisioning,” on page 151.

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 authorization period for business roles to change specific role authorization, as you handle it more efficiently using periodic business role membership reviews.

14.6 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.

Micro Focus recommends 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 does 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 requires approval by the business owner (recommended) and another one that does not require approval. A global administrator 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 a business role. 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 Business Role or Global Administrator.
2. Under **Policy**, select **Business Roles**.
3. Select 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.

14.7 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 in 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, three things can occur to the role status:

1. If there is an approved draft, Identity Governance archives the active version and the approved draft replaces it.

2. 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.
3. If there is no draft, Identity Governance moves the published business role to the approval state.

To Publish or Deactivate a business role:

1 Log in to Identity Governance as a Business Role or Global Administrator.

2 Under **Policy**, select **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**.

14.8 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 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 Business Role or Global Administrator.

2 Under **Policy**, select **Business Roles**.

3 Select **Analysis** tab.

4 Select an **Analyze** option and configure related parameters. For example, when selecting similarity analysis, you can modify the default similarity threshold. If you specify 60%, then the results display business roles that have 60% of similarity for 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 list of members in **Mandatory authorization**.

7 (Optional) Select **Download as CSV** to download the results as a `.csv` file for further analysis.

14.9 Editing Business Roles

Identity Governance allows you to edit business roles. If you edit a business role that has been approved, it is changed to a draft when you save your edits and then it must be re-approved. To edit a published business role, a new draft copy is made for editing so that the published role continues to be used in governance processes until the new draft is approved and published. You can also download business roles as JSON files using the bulk action menu. After editing, you can import the roles on the page that lists all business roles.

Editing a business role:

1 Log in to Identity Governance as a Business Role or Global Administrator.

2 Under **Policy**, select **Business Roles**.

3 Select the business role you want to edit, then select **Edit**.

4 (Optional) If the business role is published, on the top of the page, select **Edit**.

NOTE: It is recommended that you think through business role definitions and add all members and authorizations 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 revokes if auto-grants and auto-revoke settings are enabled.

Identity Governance creates a draft of the business role for you to edit in the **Draft** tab.

5 Make the appropriate changes to the business role.

You can change the name, description, grace period, risk level, memberships, authorizations, owners, and administrators of the business role.

6 Select **Save** to save the draft.

7 (Conditional) Select **Compare with published** to compare the draft version with the published version of the business role to ensure that the changes are correct.

8 If the business role approval policy requires approval, when the draft is ready for approval select **Submit for approval**. If the business role approval policy does not require approval, the draft is automatically approved whenever you save your edits.

9 After you approve a draft, select **Publish** to publish it.

When deleting a business role that has been published, Identity Governance archives the business role for reporting and auditing purposes.

14.10 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. Under **Policy**, select **Business Roles**.
3. Select the **Pending Your Approval** tab.
4. Select on 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.

14.11 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, it determines if the auto requests including compensating requests should be issued. Requests are then sent to the fulfillment system where the fulfillment system handles them according to the rules specified in your system fulfillment configuration.

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.

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.

14.11.1 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 the 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

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

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:

- 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 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
- 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 the user is a member of, the business role is deleted, or the business role is deactivated.

  NOTE: When evaluating whether an auto-revoke request should be issued, 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 as opposed to being deleted, business role authorizations stemming from that technical role are not lost.

- 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 14.11.2, “Automatic Provisioning Requests,” on page 154. For specific conditions that could result in Identity Governance issuing auto-revoke requests, see Section 14.11.3, “Automatic Deprovisioning Requests,” on page 154.

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 14.11.4, “Managing Compensating Requests,” on page 155.

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. Identity Governance does *not* automatically check for such assignment inconsistencies during normal business role detection as there would be additional overhead to do so, thus slowing down the business role detection process. Instead, Identity Governance enables administrators to manually check for such inconsistencies and fix them. For more information, see Section 14.11.5, “Managing Auto Request Inconsistencies,” on page 157.

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 14.11.6, “Monitoring Business Role Detections,” on page 158.

14.11.2 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.

14.11.3 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 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 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-revoke request from a business role detection for the user + 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.

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 triggers business role detection on BR1.
4. Identity Governance detects that Permission X is no longer authorized for BR1, which means that all members which had authorizations for permission X from BR1 lose that authorization. User A is one of those members that loses the authorization.
5. The loss of the 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.

14.11.4 Managing Compensating Requests

Identity Governance examines both the current state of 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.

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 Business Role or Global Administrator.

2. Select **Policy > Business Roles > Manage Auto 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 they are no longer a member of BR1. Identity Governance's real time identity collection detects this change and user A loses its 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 that it 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 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 it a member of BR1. Identity Governance's real time identity collection 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 they are 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 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.

14.11.5 Managing Auto Request Inconsistencies

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. Resource assignment changes are not examined by Identity Governance when determining if it should issue an auto-grant or an auto-revoke requests as 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 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.

Auto-grant request inconsistencies occur when there are permissions or applications which business roles authorize and normally would auto-grant to users, but which the users either do not currently hold or would not hold in the future (due to a pending revoke request for the same resource). Here is one scenario where such an 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 which contains permission X removes permission X from user A without Identity Governance issuing any request to do so 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 which contains permission X and updates its catalog to reflect that User A no longer has permission X. After the publication, Identity Governance triggers the business role detection. But, 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 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 when Identity Governance finds a permission or an application which are currently held or will be held in the future (due to a pending grant request for the same resource) but the resource is not authorized by any business role the user is currently a member of and the resource was auto-revoked by a business role the user was previously a member of. Here is one scenario where such an 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 it to lose its membership in BR1. Identity Governance's real time collection process 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 which 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.

Identity Governance does *not* automatically check for such assignment inconsistencies during normal business role detection as there would be additional overhead to do so, thus slowing down the business role detection process. Instead, Identity Governance allows an administrator to find these 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 does 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.

To find and optionally resolve inconsistencies:

1. Log in to Identity Governance as a Business Role or Global Administrator.
2. Select **Policy > Business Roles > Manage Auto Requests**.
3. Select the policy type and click **Detect Inconsistencies**.
4. (Conditional) For 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 a member of. It only looks for business role memberships the user lost within the last *N* days. Identity Governance ignores business role memberships that were lost before *N* days.
5. (Optional) In the pop-up window search bar, specify a user name, a permission, or a business role name to search for related inconsistencies.
6. (Optional) Submit grant or revoke requests for some or all inconsistencies to resolve them.

14.11.6 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 counts of memberships, authorizations, and auto-requests. You might enable collection of more detailed information on the exact memberships, authorizations, and auto-requests that were generated during a detection by setting the following configuration properties in the Identity Governance configuration utility.

IMPORTANT: If you enable collection of detailed information, business role detections slow down and consume more space in the database in order to store the detailed information. Generally, you should enable collection of detailed information only if you are troubleshooting some 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 Business Role or Global Administrator.
2. Select **Policy > Business Roles > Business Role Detections**.
3. (Optional) Specify business role name in the search bar to search for the detection status and details such as detection end time, number of auto-revokes generated for a business role, and so forth.
4. (Optional) Select the number of business role 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.

14.12 Downloading and Importing Business Roles and Approval Policies

You can download business roles and approval policies as JSON files and import them later into another environment.

To download or import business roles:

1. Log in to Identity Governance as a Business Role or Global Administrator.
2. Under **Policy**, select **Business Roles**.
3. Select a role or all the roles on the **Roles** tab.
4. Select **Actions > Download**.
   - **4a** (Optional) Include references to business role owners, managers, and fulfillers; and download included business roles, associated applications, technical roles, and assigned categories and approval policies.
   - **4b** Select **Download**.
5. If you make changes, or want to import previously downloaded business roles into another environment, select **Import Business Roles** on the **Roles** tab.
6. Navigate to the business roles JSON file, select the file to import, then click **Open**.
7. Identity Governance detects whether you are importing new or updated roles and whether the updates would create any conflicts or have unresolved references.
8. Select how to continue based on what information the application user interface displays. For example, under **Updates**, you can compare the imported values with current values for each role by selecting the respective role before selecting the roles to import.
9. Select the roles you want to import, and then click **Import**.

NOTE: Identity Governance does *not* automatically publish imported business roles. You must publish them in order for them to take effect in the system. For more information, see “Publishing or Deactivating Business Roles” on page 148.

To download or import business role approval policies:

1. Log in to Identity Governance as a Business Role or Global Administrator.
2. Under **Policy**, select **Business Roles**.
3. Select a policy or all the policies on the **Approval Policies** tab.
4. Select **Actions > Download**.
   - **4a** (Optional) Include references to approval policy approver.
   - **4b** Select **Download**.
5. If you make changes, or want to want to import previously downloaded approval policies into another environment, select **Import Approval Policies** on the **Approval Policies** tab.
6. Navigate to the approval policy JSON file, select the file to import, then click **Open**.
7. Identity Governance detects whether you are importing new or updated policies and whether the updates would create any conflicts or have unresolved references.
8. Select how to continue based on what information the application user interface displays. For example, under **Updates**, you can compare the imported values with current values for each entity by selecting the respective policy before selecting the policies to import.
9. Select the policies you want to import, then click **Import**.

15 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 10, “Creating and Modifying Review Definitions,” on page 103.

15.1 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:

- Global Administrator
- Data Administrator
- Auditor (read only)

See the following sections for more details about how Identity Governance helps you manage risk in your environment:

15.1.1 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.

15.1.2 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.

15.1.3 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

Application Risk Factors	Risk Factor Type
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

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

15.1.4 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. The calculations use the following variables:

- **RFV:** raw risk factor value
- **LL:** lower boundary
- **UL:** upper boundary
- **URL:** upper risk level value from risk level configuration
- **FW:** factor weight as a percentage
- **RRFV:** ranged risk factor value
- **FRS:** factor risk score
- **RS:** overall entity risk score

Risk based factor score

FRS = RFV * FW/100

Count based factor score

RRFV = (RFV - LL) >0 ? ((RFV -UL) >=0 ? URL: ((RFV * URL / (UL - LL)) : 0

FRS = RRFV * FW/100

Overall entity risk score

RS = SUM FRS[0-N]

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.

15.1.5 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 **Overview** page
- 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.

15.2 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 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.

15.3 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 7.3, “Editing Attribute Values on Objects in the Catalog,” on page 70.

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 175.

To configure risk scoring:

1. Log in as a Global or Data Administrator.
2. Under **Policy**, select **Risk**.
3. Expand a risk score section 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 163.

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 **Overview** page 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.

15.4 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 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.

15.5 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 **Overview**.

1 Log in as a Global or Data Administrator.

2 (Conditional) On **Overview**, view the Governance risk score for your organization if you have configured Identity Governance to calculate the Governance risk score.

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.

15.6 Exporting and Importing Risk Policies

Once you have configured your risk levels, scores, and schedule, you can also export all the configured polices as a JSON file, edit it if required, and import it into another Identity Governance environment.

To export and import risk policies:

1. Log in as Global or Data Administrator.
2. Under **Policy**, select **Risk**.
3. Configure risk levels, scores, and schedule and save each policy.
4. Select **Export Risk Policies**.
5. (Conditional) When you set calculated risk scores for users in the system, export schema definition of user risk attribute if needed.
6. To import risk policies, select **Import Risk Policies**.
7. Identity Governance detects whether you are importing new or updated policies and whether the updates would create any conflicts or have unresolved references.
8. Select how to continue based on what information is displayed. For example, under **Updates**, compare the imported values with current values for each entity by selecting the respective policy.
9. Select the policies you want to import, and then click **Import**.

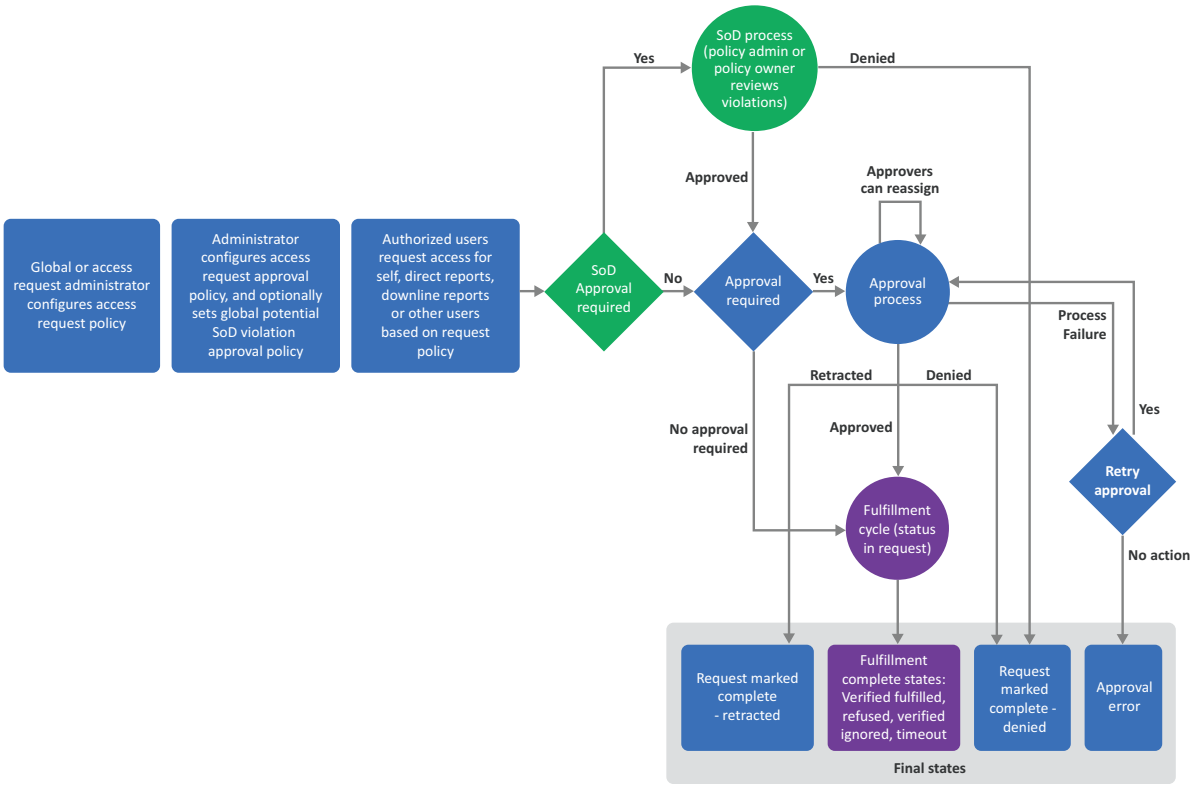
16 Administering Access Request

The Access Request Administrator or Global Administrator must configure policies that govern who can request access and who can approve access requests in your environment. Request policies define which applications, permissions and technical roles access can be requested in the Access Request interface. Request approval policies define the approvals needed when users request access.

For more information about using the Access Request interface, see “Instructions for Access Requesters and Approvers” in the *NetIQ Identity Governance User Guide*.

16.1 Understanding Access Request

Figure 16-1 *Access Request Process*



The Access Request interface allows users to monitor and request access for items that are available in their organization. The Identity Governance Access Request interface allows users to:

- Review their current access or the access for other users
- Review access that is recommended for them based on business role policies
- Browse application access that is available to request
- Browse technical roles to request a group of permissions in a single step
- Retract access request
- Retry failed request after fixing the cause of the error
- Compare access of multiple users
- Approve requests
- Approve or resolve potential SoD violations
- Review a list of access requests, status of each request, and a timeline of all related events including fulfillment

Administrators can configure the Access Request interface to provide access that is pre-approved or can be automatically routed for approval. For example, you 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.

16.2 Configuring Access Request

Setting up Identity Governance for Access Request requires configuring several items:

- (Optional) Business roles
- (Optional) Technical roles
- Request policies
- (Optional) Request approval policies.
- Request policies assigned to resources and roles

As indicated above, you need not configure all the items. Create business roles if you want to show recommended access to users and do not already have any business roles in your system. For more information, see Chapter 14, "Creating and Managing Business Roles," on page 137. Create technical roles to group permissions if you want to enable users to request access to many permissions in a single step. For more information, see Section 7.5, "Managing Technical Roles," on page 75. Create a request approval policy if you need access requests to require approval. Otherwise, the default approval policy will be in effect. The default approval policy does not require approval. For more information about request and request approval policies, see the following sections:

- Section 16.2.1, "Creating Request Policies," on page 171
- Section 16.2.2, "Creating Request Approval Policies," on page 171
- Section 16.2.3, "Assigning Resources to Request and Approval Policies," on page 172
- Section 16.2.4, "Setting Global Potential SoD Violation Approval Policy," on page 172

16.2.1 Creating Request Policies

To allow users to request access, you must create request policies. Request policies define what access can be shown and requested in the Access Request interface. Users with the Access Request Administrator and Global Administrator authorization can create request policies.

1. In Identity Governance, select **Policy > Access Request**.
2. On the **Request Policies** tab, select **+** to create a new policy.
3. Name the policy.
4. Select types of requests that all users are allowed to make. For example, if you want all users to be able to request access for themselves and their direct reports, select **Self** and **Direct Reports**.

   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.

   ---

5. For more granular control of specific users and groups, use the **Allowed Users** and **Allowed Groups** sections. For example, if you want specific users or groups to be able to request access for all users, specify that here.

   NOTE: If **All Users** are granted the ability to request for a certain type of user, you do not need to grant that same ability to specific users or groups. For example, if **All Users** are granted the ability to request for **Self**, you do not need to grant the ability to request for **Self** to specific users or groups.

   ---

6. For exclusions, use the **Disallowed Users** and **Disallowed Group** sections.
7. Use **Allowed Business Roles** to add members of business roles as requesters for self, downline reports, direct reports, or all users.
8. Save the policy.
9. (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.
10. Add applications, permissions, and technical roles that you want these an users to be able to request on the appropriate tabs.

16.2.2 Creating Request Approval Policies

To set appropriate approvals for requested access, you must create request approval policies. Identity Governance provides a default approval policy that you can edit. You can also create new request approval policies to further define your approval policies for various situations.

1. In Identity Governance, select **Policy > Access Request**.
2. On the Approval Policies tab, select **+** to add an Access Request approval policy.
3. Name the policy.
4. Add one or more approval steps, depending on how many levels of approval you require. For each approval step:
   - Specify approvers

NOTE: You can use coverage maps to specify approvers. For information about coverage maps, see “Using Coverage Maps” on page 18.

- 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

5 Save the policy.

16.2.3 Assigning Resources to Request and Approval Policies

After you have created request or approval policies, you can assign resources to them, such as applications, permissions, and technical roles.

1 In Identity Governance, select either the applications, permissions, or roles catalog.
2 Select the applications, permissions, or roles you want to apply request policies to.
3 In **Actions**, select the option you want. You can:
   - Assign access request policy
   - Remove access request policy
   - Assign approval policy

You can also assign resources to a policy or remove resources from a policy while editing the policy definition.

1 Select the **Applications**, **Permissions**, or **Roles** tab.
2 Select **+** under the tab to select resources of the specific type to assign to the policy.
3 Select the resources to be removed using the check box next to the ones you want to remove.
4 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.

16.2.4 Setting Global Potential SoD Violation Approval Policy

Global potential SoD violation approval policy applies to *all* access requests that if granted might result in Separation of Duties (SoD) violations. It determines if approvals are required for potential violations and if required are self-approvals allowed. For more information about SoD and SoD violations, see Chapter 12, “Creating and Managing Separation of Duties Policies,” on page 125 and Chapter 13, “Managing Separation of Duties Violations,” on page 131

To set global potential SoD violation approval policy:

1 Log in as Global, Access Request, or SoD Administrator or as policy owner.
2 In Identity Governance, select **Policy > Access Request**.

3 On the **Potential SoD Violation Approval** tab, select **Require approval for potential SoD violations**.

4 (Conditional) If approval is required, select **Allow self approval of potential SoD violations** to allow access requester to approve their own potential violations. Note that regardless of this setting, Global Administrator can always approve their own potential violations.

16.3 Assigning Request to Identity Governance Users

The method for giving Identity Governance users the ability to request and approve access varies.

Access Request Activity	Configuration Method	Configured By
Add items to Browse list	Create an Access Request policy and add items to the policy.	Global Administrator or Request Administrator
Add items to Recommended items list	Add items to a request policy that are covered in a business roles policy.	Global Administrator or Request Administrator
Specify approval rules for request Items	Create a request approval policy and assign permissions, applications, or roles to that policy either while editing the policy definition or in the catalog using bulk select menu.	Global Administrator or Request Administrator
Specify coverage map for request approvals	Create coverage map in CSV format, add/upload it to application (**Configuration > Coverage Maps**), and then specify approvers in a request approval policy as coverage map. For information about creating and loading coverage maps, see "Using Coverage Maps" on page 18.	
Configure request item text or icons	Edit the permission, application, or technical role in the data source, the catalog, or with the bulk edit feature.	Global Administrator or Request Administrator
Manage how requests are fulfilled	Identity Governance **Fulfillment > Configuration.** For information about configuring fulfillment targets, see "Configuring Fulfillment" on page 88.	Global Administrator or Request Administrator
Manage who can request on behalf of others	Requesters tab in appropriate Request Policy.	Global Administrator or Request Administrator
Manage email notifications for request approvals	Notifications section in each approval step of the appropriate Request Approval Policy	Global Administrator or Request Administrator
Create an Access Profile to allow requesting collections of authorizations	Technical role in the catalog added to Request Policy	Global Administrator or Request Administrator

Access Request Activity	Configuration Method	Configured By
Control approval decision support information	Similarity profile settings in Identity Governance **Configuration > Role Mining and Analytics Settings**. For information about configuring similarity profile settings, see "Configuring Analytics and Role Mining Settings" on page 183.	Global Administrator or Request Administrator

16.4 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. Check the current status of Access Request:

   ```
   config> dc com.netiq.iac.access.request.enabled
   ```
3. Disable the Access Request service:

   ```
   config> sp com.netiq.iac.access.request.enabled false
   ```
4. Exit the console and restart tomcat.

17 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 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 **Overview**, **Catalog > Identities** and **Certification** pages, you can drill down to see specific violations to policies when they exist.

17.1 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

17.2 Creating and Editing Certification Policies

NOTE: Reviews should be defined before creating a certification policy. For information about review definitions, see Chapter 10, “Creating and Modifying Review Definitions,” on page 103.

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 Global Administrator, Review Administrator, or a Data Administrator.
2. Under **Policy**, select **Certification**.
3. Select **+** to create a certification policy.
4. Specify the name of the certification policy, validity period in days, months, or year, 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, global, review, or data administrator can function as a policy administrator.
7. Save your settings.
8. Under **Policy**, select **Certification** to view the newly created policy listed with number of violations.
9. (Optional) Select **Set Remediation** to select remediation action. For more information about setting remediation, see “Remediating Certification Policy Violations” on page 179.
10. (Optional) Select the policy, then select **Edit** to edit the policy.
11. (Optional) Select a specific policy or multiple policies, then select **Actions > Delete** to delete policies.

17.3 Scheduling Calculations and Calculating Certification Policy Violations

Identity Governance automatically calculates policy violations when a certification policy is modified, or identity or data application source is published, or when reviews included in the policy are completed. In addition, you can also schedule when certification policy violation calculations will occur. 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 15, “Calculating and Customizing Risk,” on page 161.

To schedule certification policy calculation:

1. Log in as a Global, Review, or Data Administrator.
2. Under **Policy**, select **Certification**.

3 Select **Schedule** tab, and set the schedule.

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

To manually calculate policy violations:

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

17.4 Exporting and Importing Certification Policies

Once you have created your certification policies based on your business requirements, you can easily export the certification policies 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.

To export or import certification policies:

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

2 Under **Policy**, select **Certification**.

3 In the **Policies** tab, select the policy or policies you want to export.

4 Select **Actions > Export**. A zipped file containing certification policies and review definitions files in JSON format will be downloaded to your default download location.

5 Extract the files if you want to import them later.

6 To import certification policies, click **Import Certification Policies** on the Certification page.

7 Navigate to the folder where your certification policies file is located, and click **Open**.

8 Identity Governance detects whether you are importing new or updated policies and whether the updates would create any conflicts or have unresolved references.

9 Select how to continue based on what information is displayed. For example, under **Updates**, you can compare the imported values with current values for each entity by selecting the respective policy before selecting policies to import.

10 Select the policies you want to import, and then click **Import**.

11 Remediation settings such as email recipients and review definitions can be resolved when policy is imported or it can be resolved manually after import.

17.5 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 on the **Overview** page. 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.

17.5.1 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.

17.5.2 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 Section 7.4.3, “Managing Filters,” on page 74.

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.

17.5.3 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 10.3, “Understanding Micro Certification,” on page 109 and “Instructions for Fulfillers” in the *NetIQ Identity Governance User Guide*.

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 Global, Review, or Data 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**.

18 Creating and Managing Delegation

Delegation enables you to assign delegates for users to enable a more consistent workflow for managing the reassignment of user tasks. A global, or data administrator assigns delegate for a user, and the delegate then receives tasks and acts on them instead of the original assignee. If the original assignee acts in one of the review management roles (review owner, escalation reviewer or auditor) then the delegate has the proper access permissions to act in that role.

18.1 Understanding Delegation

Delegation is a one-to-one mapping between two active users in the catalog. 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 cyclical chain related review startup failure, administrators can use the **Validate delegate mapping** bulk action after mapping delegates. The only other times Identity Governance calculates delegates is when review items are escalated, or when a reviewer is reassigned using the **Change Reviewer** option. When using the **Change Reviewer** option during reviews, the option will become inactive when a cyclical chain is detected.

A delegation continues until it is terminated or a different user is assigned. 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, all 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.

18.2 Assigning and Managing Delegates

1. Log in as a **Global Administrator** or **Data Administrator**.
2. Under **Policy**, select **Delegation**.
3. Select **Add Row** to create a new delegation. Add the user, assign a delegate, add a reason, and set the status.
4. Click **Save**.
5. Repeat the above steps to add delegates for other users.

   NOTE: A user can have only one delegate at any given time.

6. (Optional) Select **Edit** to change user, delegate, reason, or status.
7. (Optional) Select **Delete** to terminate a delegation.

8. (Optional) Select rows and then select **Actions > Enable** or **Actions > Disable** to change the status of multiple delegations.
9. Select rows and then select **Actions > Validate delegate mappings** to ensure delegate mappings, if chained, are chained appropriately. Fix invalid mappings, if any.

NOTE: Review owner and review administrator can by-pass delegation for the review management roles (review owner, escalation reviewer, and auditor) by editing the running review instance. These change are only made for the running review instance. Delegates also can assign another user as a reviewer by using the **Change Reviewer** option in review tabs.

---

19 Analyzing Data and Monitoring Governance System

NetIQ Identity Governance uses advanced analytics to analyze your data and provide you with results that enable you to monitor key aspects of your identity governance system. Results include:

- Governance metrics
- Risk scores
- Policy violations
- Role effectiveness and number of entitlement assignments via roles versus direct assignments
- Accounts statistics

Furthermore, Identity Governance enables authorized administrators to configure and customize analytics and metric definitions.

19.1 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 Administrator.

NOTE: Business 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 185.

6 Select **Save** to save all the settings.

7 (Optional) Next to **Metrics Collection**, select the **+** icon to create custom metrics. For more information, see Section 19.1.2, "Understanding Metrics," on page 185 and "Creating Custom Metrics" on page 186.

8 Under **Metric 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.

---

9 Specify start date, time, and hours or deselect the **Active** check box to disable collection.

10 Click **Save**.

11 (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 **Overview** page.

---

12 (Optional) When a custom metric collection is running and you want to cancel it:

12a Select the item or items with an asterisk (*), and then select **Cancel Collection**

12b Click **Cancel Collection** to confirm the cancellation.

13 (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 187.

19.1.1 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. For more information about role mining, see Section 14.2.2, “Understanding Business Role Mining,” on page 140

Log in as a Global, Data, or Business Role Administrator. 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 **Collect Metrics > Business Role Mining metrics** to refresh data.

19.1.2 Understanding Metrics

Identity Governance tracks key risk indicators so that administrators can monitor these risk factors in your governance system and make improvements based on the collected metrics.The key risk factors or facts extracted and collected from various data sources 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. In addition, 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.

Administrators cannot edit the default metrics but can view associated description and metric columns by selecting the metric name. 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**. Administrators can also download all metric results in CSV format.

19.1.3 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 using a SQL statement:

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. Select where you want the custom metric results published, provide additional location information as required, and then specify a name for the metric table. For example, for large volume analytics you can set up a metrics archive in your Vertica or Kafka database. You can provide that information in the storage related fields, and the metrics will collect to those tables, leaving your Identity Governance tables free for standard data processing.

   NOTE: If you do not specify a table name for the metric table, Identity Governance creates a table with `ex_randomGUID` naming convention. However, it is recommended that you provide a meaningful table name.

   ---

7. (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.
8. (Conditional) If you select to store the metric in Kafka using a secure connection, use the Identity Governance Configuration utility to configure the following properties:
   - `com.netiq.iac.kafka.publisher.truststore.location`
   - `com.netiq.iac.kafka.publisher.truststore.password`
   - `com.netiq.iac.kafka.publisher.keystore.location`
   - `com.netiq.iac.kafka.publisher.keystore.password`
   - `com.netiq.iac.kafka.publisher.key.password`

   For more information, see Appendix A, “Running the Identity Governance Configuration Utility,” on page 191.
9. Select **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.

   ---

10. Select **Metric Columns** and then **Add Column** to 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 PostgresSQL 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.

- 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 9 on page 186.

IMPORTANT: Potential issues, such as metric column name mismatch, are indicated with a warning icon. Address metric column section warnings before saving the custom metric. Creating a metric with a warning might not work correctly.

---

11 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 7.4.1, “Searching with Insight Queries,” on page 72.

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.

19.1.4 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.

To download and import custom metric definitions:

1 Log in as a Global or Data Administrator.

2 Select **Configuration** > **Analytics and Role Mining Settings**.

3 Select names starting with an asterisk (*****).

4 Select **Actions > Download Definitions** to download custom metric definitions.

5 To import custom facts, select **Import Custom Metrics**, browse for custom metric JSON files containing exported custom metrics, select entities to import, and then click **Import**.

6 (Conditional) If there is a conflict with an existing metric, resolve the conflict by selecting **Import new** to create a new custom metric or select **Replace Existing** to replace the existing metric.

19.2 Monitoring Your Identity Governance System

Identity Governance provides authorized administrators an overview of real time adaptive statistics related to your governance system on the **Overview** page. The **Overview** page also provides links to the related feature areas such as catalog, risk, and policies. Authorized administrators view details and optionally edit the respective definitions and settings. For configuring detailed queries, see Section 19.1, “Configuring Analytics and Role Mining Settings,” on page 183 and Section 7.4.1, “Searching with Insight Queries,” on page 72

In order to view the widgets on the **Overview** page, requisite tasks must have been completed, and administrators must have the appropriate access authorization. For example, to view the Governance Risk Score widget, you must have previously configured and calculated the governance risk score. Users with Auditor authorization have read-only access to the Governance Risk Score widget. Global and Data Administrators can view the governance risk score and edit risk score configuration. For more information, see Section 15.3, “Configuring Risk Scores,” on page 166 and Section 15.5, “Viewing Calculated Risk Scores,” on page 167.

19.2.1 Viewing Data Collection Statistics and Summary

Global or Data administrators can view data collection statistics such as the number of identity and application sources and collection schedules in the Data Collection widget. They can also select the sources and schedules to configure application sources and collection schedule. For more information, see Chapter 3, “Creating and Managing Data Sources,” on page 33 and Chapter 4, “Creating and Monitoring Scheduled Collections,” on page 51.

In addition to collection statistics, administrators can also view the total number of groups, identities, applications, accounts, and permissions in the Data Summary widget. This data can be viewed as a bar or pie chart and authorized users can select a parameter to view the respective catalog details.

19.2.2 Viewing Number of Policies and Related Violations

Administrators such as the Separation of Duties Administrator, Review Administrator, and Data Administrator can view respective SoD, Certification, and Data policy violation statistics. In order to view the policy widgets, administrators must have defined review definitions and policies. For more information, see Section 12.2, “Creating and Editing Separation of Duties Policies,” on page 126, Section 17.2, “Creating and Editing Certification Policies,” on page 175, and Section 3.4.2, “Creating and Editing Data Policies,” on page 44.

19.2.3 Viewing Entitlement Assignments Statistics to Leverage Roles

To understand how entitlement assignments conform to business polices, Global, Data, and Business Role Administrators can view the Role Leverage widget on the **Overview** page. It includes a graphical overview of effectiveness of roles over a period of time, entitlements assignments using roles versus entitlements assigned directly, and 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, and 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 risk by using role mining to create more roles. For more information, see “Defining Business Roles” on page 141.

19.2.4 Viewing Account Statistics and Details

On the **Overview** page, administrators can see an account statistics summary for their system in the Account Statistics widget. To see data, administrators must collect and publish data sources and then collect metrics on demand or wait the default metrics collection interval of 24 hours.

NOTE: To keep statistics up to date, metrics must be collected after every publication.

Identity Governance displays available metrics on the summary panel followed by a chart for each metric per risk levels.

To change the default settings:

1. Log in as an authorized administrator such as Global, Data, Review, or SoD Administrator.
2. Select the calendar icon to change the time range for account statistics.
3. Select the change option icon to show or hide risk level series.

To drill down to see many more specific charts relating to your accounts:

1. On the **Overview** page in the Account Statistics widget, select **View statistics details**.

   or

   Select a data point on any chart to drill down to statistics details for that chart.
2. Select the calendar icon to change the date for the statistics.
3. Select a chart or table from the drop down menu to change to a different set of statistics. You can modify or delete these.
4. Drag and drop available metrics from the header to columns or rows.
5. (Optional) To create a customized chart or table:
   - **5a** Start with a chart or table that contains the basic elements you want.
   - **5b** Select the type of table, such as heatmap or line chart.
   - **5c** Select the type of statistics, such as count or average.
   - **5d** (Optional) Select additional options, if needed. Some selections add more options to customize. For example, for risk by application count bar chart you can customize risk levels display and add and customize results display by application.
   - **5e** Customize the row and column headings.
6. Specify a name for the customized view and select **Save**.

A Running the Identity Governance Configuration Utility

The Identity Governance Configuration Utility allows you to modify settings for Identity Governance, such as the URL for Identity Governance, the authentication server, OSP, and email notifications. You can also specify an external provisioning system for workflows and the settings for collection and publication.

You can run this utility in GUI or console mode from the Identity Governance installation location. To script changes to the configuration of Identity Governance, use the console mode option.

In the command line, navigate to the installation directory for Identity Governance.

- **Linux:** Default location of `/opt/netiq/idm/apps/idgov`, then enter one of the following commands:
  - **Console mode:** `./bin/configutil.sh -password db_password -console`
  - **GUI mode:** `./bin/configutil.sh -password db_password`
- **Windows:** Default location of `c:\netiq\idm\apps\idgov`, then enter one of the following from a command prompt:
  - **Console mode:** `cmd /c "configutil.bat -password db_password -console"`
  - **GUI mode:** `cmd /c "configutil.bat -password db_password"`

The utility provides settings under the following tabs:

A.1 Identity Governance Server Details

This tab allows you to display your organization’s branding instead of the default branding displayed when your users run Identity Governance.

NOTE: In early versions of Identity Governance (formerly named Access Review), this tab included values for the login page, such as protocol, host name, and port. Starting with Access Review 1.5, those values are on the **Authentication Server Details** tab.

A.2 Authentication Server Details

This tab defines the values for the LDAP authentication server, OSP authentication service, and bootstrap administrator. This tab provides the following groups of settings:

A.2.1 OAuth Server

This section represents the values for the LDAP authentication server.

Same as IG Server

Specifies whether the authentication server runs on the same computer as Identity Governance.

Protocol

Applies only when the authentication server and the Identity Governance server run on different computers.

Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify `https`.

Host Name

Applies only when the authentication server and the Identity Governance server run on different computers.

Specifies the DNS name or IP address of the LDAP authentication server. Do not use localhost.

Port

Applies only when the authentication server and the Identity Governance server run on different computers.

Specifies the port that you want the server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443.

A.2.2 OAuth SSO Client

This section represents the values for OAuth authentication services to Identity Governance.

IG Client ID

Specifies the client ID of Identity Governance with which it is registered to the authentication service.

IG Client Secret

Specifies the client password of Identity Governance with the authentication service.

IG Redirect URL

Specifies the URL used by the authentication service to redirect to the Identity Governance login page if authentication token is valid.

IG Request Client ID

Specifies the client ID of Identity Governance Access Request with which it is registered to the authentication service.

IG Request Client Secret

Specifies the client password of Identity Governance Access Request with the authentication service.

IG Request Redirect URL

Specifies the URL used by the authentication service to redirect to the Identity Governance Access Request page if authentication token is valid.

A.2.3 Bootstrap Admin

This section represents the values for the bootstrap administrator.

Bootstrap Admin

Specifies the name of the bootstrap administrator account. The default value is `igadmin`.

(Conditional) When connecting to an existing Identity Manager authentication server, specify the full DN of a unique identity that already exists and can access Identity Manager Home as a bootstrap administrator. For example, `cn=uaadmin,ou=sa,o=data`.

NOTE: The name of this account must be unique. Do not duplicate any accounts in the `adminusers.txt` file or in the container source or subtrees that you use for authentication.

Authentication Source

Specifies whether the credentials for the bootstrap admin reside in an Identity Vault (LDAP authentication server) or a text file.

(Conditional) If you specify **File**, you must also specify values for **Directory** and **Filename** that correspond to the file that stores your bootstrap admin information.

- **Linux:** Default location of `/opt/netiq/idm/apps/idgov/osp/adminusers.txt`
- **Windows:** Default location of `c:\netiq\idm\apps\idgov\osp\adminusers.txt`

A.3 Security Settings

This tab defines the values for authentication matching and Identity Governance services.

Auth Matching Rules

Specifies how Identity Governance authenticates login requests and grants the appropriate permissions to users. Enter one or more rules that Identity Governance uses to compare attributes in the SUSER table, such as `dn`, with attributes retrieved from the authentication service. Specify the matching rules using properties named `iac.auth.matching.rule.`*`N`*`.attrs` where *N* specifies the order that Identity Governance uses the rule to match users, such as 1, 2, 3, and so on.

Keep in mind the following points:

- For best results, add an index for the matching rule attributes.
- Identity Governance evaluates only collected attribute values for the matching rules, not edited values.
- When an attribute value is a string, Identity Governance performs an exact case match by default.

IMPORTANT: Set all matching rule attributes with the following list and search options in the Identity Governance User (identity) schema:

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

For more information, see "Adding or Editing Attributes to Extend the Schema" in *NetIQ Identity Governance Administrator Guide*.

Auth Attribute Map

Specifies the mapping of SUSER attributes to OSP attributes using a comma-separated list of attribute name pairs. Use the format `SUSER attribute:OSP attribute`. For example, `dn:name,lastName:last_name,firstName:first_name,emails:email` maps the SUSER attributes of dn, lastName, firstName, and emails to the OSP attributes of name, last_name, first_name, and email.

IG Client ID

Specifies the name that you want to use to identify Identity Governance to each service listed.

IG Client Secret

Specifies the password for the corresponding client ID.

Enable test client for utilities

Specifies that you want to use test IDs to run utilities that interact with Identity Governance without creating client IDs for each utility.

A.4 Network Topology Settings

This tab defines network connection settings that Identity Governance uses to connect to the single Tomcat instance or to the load balancer if you are running Identity Governance in a cluster. If you select **https** for the protocol, the **Keystore File** and **Keystore Password** fields become active.

This tab also defines runtime instance settings.

A.5 Miscellaneous Settings

This tab defines additional settings for your configuration. Some fields are self explanatory and some should not be changed. This tab provides the following groups of settings:

A.5.1 Miscellaneous

Do not change the settings in this section except for the **Default Locale**, if needed.

A.5.2 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.

A.5.3 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.

A.5.4 Identity Manager Integration

If you also have Identity Manager installed, these settings help you integrate Identity Governance with Identity Manager.

Enable integration using Identity Manager Driver for Identity Governance

Requires the Identity Manager Driver for Identity Governance (Identity Governance driver)

Specifies whether you want to integrate the permissions and permission assignment tasks in the Identity Governance catalog with the role and resource catalog in Identity Manager.

For more information, see Section 5.1, “Understanding Synchronization and Reflection,” on page 55.

Exclude Identity Manager permissions from review when they provision any native permissions in the same review

Specifies whether you want to review Identity Manager permissions that duplicate native permissions along with the native permissions in a review.

A.5.5 Data Production Timeouts

These settings allow an administrator to tune the timeout values for various data production operations to achieve optimal performance in each environment. The timeout values are expressed in milliseconds. The default values should suffice for the majority of installations.

Heartbeat interval (com.netiq.iac.dataProduction.heartbeat.interval)

The interval between heartbeat updates for data production jobs. The default is 2 minutes (120000 ms).

Job idle cutoff timeout (com.netiq.iac.dataProduction.cutoff.timeout)

The amount of time, after the last heartbeat update, that a running job is deemed to be in an idle state where the data production processing has halted. The default is 6 hours (21600000 ms).

Orphaned job idle add-on timeout (com.netiq.iac.dataProduction.orphan.addon.timeout)

The additional amount of time, combined with the **Job idle cutoff timeout**, that will pass before a runtime instance can detect and clean up data production jobs with a different runtime identifier that have an idle state. The default is 1 hour (3600000 ms), which combined with the default cutoff timeout sets up an overall 7 hour default.

A.6 Bulk Data Update Settings

This tab defines settings that you use to submit multiple attribute updates to objects in the catalog by using a CSV file. For more information about performing bulk data updates, see Section 7.3.2, “Editing Attribute Values in Bulk,” on page 71.

Base Folder

Create a folder on your Identity Governance server for update files. Specify that full path name of that folder in this field. You must also create sub-folders named `input` and `output`. The Identity Governance service must have read/write access permission on both of these folders. Identity Governance creates the CSV data template files in the output folder, and you submit edits by copying the updated template in the input folder.

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.

When you place the `csv` file in the `input` directory, Identity Governance changes the extension name of the file as it process the file. Here are the different extensions and process the file goes through during the bulk process:

File Extension Name	Process
`.csv`	Identity Governance start the bulk process. It is the name on the file when you add it into the `input` directory.
`.ph1`	Phase 1 of the bulk process.
`.fail`	If the bulk process fails, the file name becomes `.fail`.
`.done`	If the bulk process completed, the name becomes `.done`.

A.7 Workflow Settings

This tab defines settings that you use to automate external provisioning and notifications. This tab provides the following groups of settings:

- Section A.7.1, “External Provisioning System,” on page 196
- Section A.7.2, “Notification System,” on page 197
- Section A.7.3, “Message Queue,” on page 197

A.7.1 External Provisioning System

To use an external provisioning system, specify the **URL**, **User ID**, and **Password** that Identity Governance needs to connect to the system. For example:

URL

```
http://$test:8180/IDMProv
```

User ID

```
globaladmin
```

Password

```
adminpassword
```

For more information, see Section 9.5.2, “Using Workflows to Fulfill the Changeset,” on page 101.

A.7.2 Notification System

This section represents the values that Identity Governance uses to send email notifications.

Mail Server

Specifies the IP address or DNS name and port for the mail server. For example, `12.345.675.90:25`.

From Address

Specifies the email address that you want Identity Governance to use as the origination for email notifications.

NOTE: If you are using a Gmail SMTP server for your mail server, Gmail ignores this value and uses the actual Gmail address as the origination for email notifications.

Enable SMTP TLS

Specifies to use secure email delivery.

User ID

Specifies the email address that you want to use for authenticating Identity Governance to the mail server.

Password

Specifies the password associated with the specified **User ID**.

Enable persistent notification message queue

Specifies whether you want to use message queuing functionality.

A.7.3 Message Queue

This section represents the values for the message queue for email notifications. The queue can use TLS/SSL protocol for secure communication.

JMS broker URI

Specifies the Uniform Resource Identifier (URI) for the Java Message Service (JMS) that the mail server uses. For example, `tcp://12.345.675.90:61616`.

(Conditional) In a clustered environment, add `failover:` to the prefix, then specify the host name or IP address and port for each ActiveMQ server. Use commas to separate the server values. For example, `failover:tcp://amq1.mycompany.com:61616,tcp://amq2.mycompany.com:61616`.

SSL

Specifies whether you want to use TLS/SSL protocol for secure communication when sending notifications.

Queue Keystore

Applies when you want to use the SSL protocol.

Specifies the path and filename of the keystore file that contains the authentication server trust certificate for the mail server.

Queue Keystore Password

Applies when you want to use the SSL protocol.

Specifies the password used to load the keystore file.

Queue Trust Store

Applies when you want to use the SSL protocol.

Specifies the path to the Trusted Key Store that contains all trusted signers' certificates.

Queue Trust Store Password

Applies when you want to use the SSL protocol.

Specifies the password for the Trusted Key Store.