docsys (en) 11 November 2016

NetIQ® Identity Governance as a Service

User Guide

June 2018

Legal Notice

Contents

About this Book and the Library

The *User Guide* provides conceptual information about the NetIQ Identity Governance as a Service product. This book provides installation information and step-by-step guidance for administrative and user-oriented tasks.

Intended Audience

This book provides information for a variety of users involved in collecting, reviewing, and updating identities 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 as a Service catalog that correlate with existing sources in the organization. Configure roles and security for Identity Governance as a Service. Help business administrators and application owners to create scheduled collections and reviews. Set up manual or automated fulfillment workflows.

Business administrator

Collect and publish identity and application data for review.

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 as a Service product, such as known issues.

NetIQ Identity Manager Driver for Identity Governance as a Service

Provides information about how to install and configure the Identity Manager Driver for NetIQ Identity Governance as a Service. The Identity Governance as a Service driver allows you to provision application-specific permission catalog data from Identity Governance as a Service to Identity Manager, giving you the ability to review and certify permission assignments using Identity Governance as a Service, 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 the *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide*.

Videos

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

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log on. If you have suggestions for documentation improvements, select **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Overview

The Identity Governance as a Service product enables administrators and managers to easily collect all user and access information in one central location and certify that users have only the level of access that they need to do their jobs. Following the principle of least privilege, this product allows you to ensure that your users have focused access to those applications and resources they use and cannot access resources they do not need to access.

With Identity Governance as a Service, administrators and business managers can ensure that your employees, either individually or as a group, have the appropriate set of permissions. Identity Governance as a Service collects information from various identity and application data sources and manages the entire review and certification process. Identity Governance as a Service provides tools to guide you through the key phases of the access or account review, audit case management, and validation process.

- Collecting identity and application data
- Publishing identities, accounts, permissions, and groups
- Highlighting policy violations
- Grouping common permission sets into technical roles
- Establishing business role policies to describe what is authorized
- Preparing published data for review
- Previewing review data
- Reviewing user access
- Approving the review
- Fulfilling the access changes
- Verifying that the access changes were made

Understanding Installation and Configuration

NetIQ provides Identity Governance as a Service as a hosted solution. We deploy and manage the solution, but you must install any needed identity and application collectors.

Identity Governance as a Service provides authentication and Single Sign-On (SSO) through the One SSO Provider service (OSP). ![EAN: After the client **authenticates** to OSP (with basic authentication, Kerberos or SAML), it can optionally implement a multi-factor authentication method when used with the optional Advanced Authentication Service. NOTE: Removed this because, per Rick, at this time we are only supporting username/password. Jon B said he'd add multi-factor auth to the list for Chan.] The OSP can be a shared service providing single sign-on across Identity Governance as a Service, Identity Manager, and Identity Reporting services.

Understanding Data Collection and Publication

Identity Governance as a Service processes require clean, up-to-date data obtained from a variety of sources such as Identity Manager, Active Directory, and other enterprise applications in the data center and the cloud. Identity Governance as a Service can obtain the data by directly connecting to the systems through protocols such as LDAP and JDBC, or it can simply load the data from a periodically extracted data file such as a Comma Separated Value (CSV) formatted file.

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

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

Permissions are the next major part of the Entitlement Catalog. Applications have their own name spaces and Identity Governance as a Service can collect and publish the permissions per application in parallel. Identity Governance as a Service uses the latest published Identity Catalog to map who has what access to permissions in each application when it is published.

Collection templates are the default mappings of data from identity and application sources to the core Identity Governance as a Service standard schema. At a minimum, connection specific information such as accounts and passwords or API keys and access tokens must be provided to save the template and collect the data.

Identity Governance as a Service provides templates to simplify the collection of data from the applications. For more information about the templates, see “Collecting Identity and Application Data” on page 15.

Understanding Data Sources

Identity Governance as a Service has two categories of data sources: identity and application. An **identity source**, such as SAP User Management or Active Directory, provides attributes of an identity. For example, you import employee names, titles, and human resources attributes. **Identities**, also referred to as **users** in the user interface and in this document, represent the people who are at the core of the processes within Identity Governance as a Service. They are the *who* in the review process of “*who* has access to *what*.” Identities are also the people who manage and perform the reviews, or who serve as the administrators of Identity Governance as a Service. **Identity sources with change events** enable incremental changes to the user and group data without having to frequently collect and publish identities.

To review the access for an application, such as Salesforce, you can create an **application source**. The application source can collect data for accounts and permissions. Accounts and permissions are the *what* in the review process of “*who* has access to *what*.” In general, **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 a self-service human resources application. Accounts often specify the type of permissions granted to the user. **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

Your organization might also have a hierarchy of permissions based on **roles**. For example, a corporate role called *Sales Employee* might consist of various child permissions that apply to all employees, such as *Garage Access*, *Building Access*, and *Read Access to Company Intranet*. The role might also have permissions associated with sales software applications and financial data.

Each application source can contain separate **collectors** for gathering specific account and permission data. Account collectors help you discover accounts that have been added or deleted since the previous data collection. You can also determine whether accounts are being used, such as identifying the last login for that account. When you collect permission data, you can review changes to permissions, such as new groups or roles. You can also view changes in the assignments of permissions to users or accounts.

Collecting Identity and Application Data

During the data collection phase, Identity Governance as a Service collects raw data from specified identity and application data sources. Identity Governance as a Service can collect data from the following types of sources:

![EAN: Added AD Domain Services for IGaaS.]

- Active Directory Domain Services (default)
- Active Directory
- Azure
- CSV file
- eDirectory
- Google Apps
- Identity Manager
- JDBC
- RACF
- Salesforce.com
- SAP User Management
- ServiceNow

NOTE: Active Directory, eDirectory, and Identity Manager identity sources can be configured to generate incremental change events. However, the Identity Governance as a Service hosted solution does not support “AD with changes” against AD Domain Services because there is no cookie provided that reflects a delta.

![EAN: Added the second sentence above for IGaaS.]

![EAN: Added the following para for IGaaS - the wording still needs some work though, and need to verify that I interpreted info from Dev correctly.]

If you are using Active Directory Domain Services in your environment, NetIQ works with you to install and configure the default identity collector. You are free to use any other collector as long as it is not against AD Domain Services. However, in some cases you might need to install additional third-party libraries with Identity Governance as a Service to use a particular collector. Since you do not have access to the server console, you must contact NetIQ Customer Support to coordinate installation of those third-party libraries.

![EAN: Added the following para for IGaaS.]

If your identity and application data is stored in your internal IT infrastructure, you must either open holes in your firewall for the necessary ports to establish a connection with NetIQ or configure site-to-site VPN. Configuring site-to-site VPN will require coordination between your internal administrators and NetIQ hosted solution representatives because configuration is needed at both locations.

Identity Governance as a Service provides several predefined **collector templates** to facilitate data collection. A collector template lets you quickly build and customize a collector. Whenever possible, the collector templates include predefined attribute mappings and value transformation policies suitable for the target data source. To automate the collection process, you can create **scheduled collections** that define the interval and data sources that you want to collect.

For more information about collecting data, see Part IV, “Managing the Identity Governance as a Service Catalog,” on page 131.

Publishing a Catalog of Collected Identities

After collecting identity data, you can publish a snapshot of the Identity Governance as a Service catalog. The snapshot presents a consolidated view of the collected identities. Using Identity Governance as a Service, you can directly associate user identities and permissions. Alternatively, you can associate identities with accounts and associate the accounts with permissions. For more information about publishing, see Chapter 19, “Publishing the Collected Data,” on page 171.

If you use the Identity Manager Driver for Identity Governance as a Service (Identity Governance as a Service driver), you can **synchronize** data that Identity Governance as a Service has collected from application sources with identities, roles, and resources in Identity Manager. For example, the Identity Vault for Identity Manager contains information related to the roles and resources assigned to Joe Smith for applications A, B, and C. Identity Governance as a Service collects Joe’s roles and permissions from applications D, E, and F. When you publish the Identity Governance as a Service catalog to Identity Manager, the driver allows you to **reflect** Joe’s roles, resources, and permissions in the Identity Vault. This option ensures that you do not have duplicate information for Joe Smith. Also, Joe can now request access to resources in applications that Identity Manager does not manage. For more information about synchronizing and reflecting user data, see “Understanding Synchronization and Reflection” on page 159. For more information about the driver, see the *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide*.

Preparing Published Data for Review

The next step is the manual process of preparing the published data for review. During the manual process, you can improve data quality by:

- Defining technical roles
- Defining business role policies
- Setting policies, such as Separation of Duties
- Providing additional meta data
- Defining business-friendly names for various entities
- Specifying risk factors for applications, roles, authorizations, and permissions

You can also **edit** the data by changing the collected values. The Identity Governance as a Service browser-based interface provides an easy way to resolve the mappings that exist among different user, account, and permission object types. For more information about preparing data, see “Editing Attribute Values on Objects in the Catalog” on page 181.

Understanding the Review Process

After you edit and publish the data, you can review particular sets of applications, groups, accounts, roles, or users and permissions. You can focus reviews on selected permissions for all or selected users or accounts, or on the ongoing presence of **unmapped accounts**, which are accounts in an application without an assigned user.

In addition, Identity Governance as a Service allows you to review business role policies and memberships. 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. For more information, see Chapter 10, “Creating and Managing Business Roles,” on page 95.

To run the same review at regular intervals, you create a **review definition** with an optional schedule to automatically start at the intervals you define. Users with the Review Administrator authorization can create review definitions. For more information, see Chapter 6, “Creating and Modifying Review Definitions,” on page 69.

For each review, you assign users to specific Identity Governance as a Service roles, such as:

- Owner of the review who previews, initiates and completes the review
- Users who review the sets of data
- (Optional) User who reviews escalated items
- (Optional) User who audits the review

When a reviewer or fulfiller marks an item complete, Identity Governance as a Service automatically removes the item from the task list.

Reviewing Access and Permissions

After you have a review definition, the Review Owner can preview, and initiate a **review run** or it starts automatically if you set the schedule. The review run generates tasks for reviewers, requesting that they review a set of users and decide whether the current user access should be maintained or revoked. When the Review Owner initiates a review run, Identity Governance as a Service automatically generates tasks for assigned Reviewers and notifies them as specified in the review definition. To help Review Owners ensure that the review process proceeds in a timely manner, you can specify the length of the review period, such as three weeks. In addition, you can set the schedule to run in preview mode so that the Review Owner can preview review definition and items, and change review options, review monitors, duration, and reviewers. You can also instruct Identity Governance as a Service to **escalate the process** and move the tasks to Escalation Reviewers, if specified in the review definition, or to the Review Owner if the Reviewer does not complete all tasks. For more information, see “Escalating Review Items” on page 71. For more information about the review process including preview mode, see Chapter 7, “Running a Review Instance,” on page 81.

Fulfilling Changes Requested in the Review

The review process results in a list of changes, or **changeset** that are then implemented. Identity Governance as a Service refers to the implementation process as **fulfillment**. You can fulfill the changeset in the following ways:

Manual

Use a manual process to modify and remove permissions. For more information about manual fulfillment, see “Fulfilling the Changeset for a Review Instance” on page 82.

Automated

Use Identity Manager to automatically remove permissions. You can use this option if the permissions were collected from an Identity Manager system.

Custom using External Workflow

Use a workflow defined in Identity Manager identity applications to remove permissions.

Service Desk

Identity Governance as a Service 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. For more information, see “Configuring Service Desk Fulfillment” on page 25.

For more information, see “Configuring Fulfillment” on page 23.

Completing and Approving a Review

Review Owners can complete, terminate, review, or partially approve the decisions at any time during a review run. If they want to change the review, all access change requests are sent to fulfillment, which is the step where approved changes are implemented. After approval, a review can be optionally routed to a Review Auditor for legal acceptance.

The review and validation process that begins with data collection and publishing concludes with change request reconciliation. Identity Governance as a Service can track the status of change requests fulfilled manually or through automatic or workflow-based provisioning.

For more information, see Chapter 7, “Running a Review Instance,” on page 81.

Understanding Reporting

![EAN: Updated this section for IGaaS. Per Rick M, RPT is a core component of the IGaaS solution.]

Identity Reporting is a core component of the Identity Governance as a Service solution. With Identity Reporting you can generate reports about identity and application data, data collection and publication, reviews, and fulfillment status. Users with the Global or Report Administrator role can create, run, and view the reports. For more information, see Part V, “Reporting for Identity Governance as a Service,” on page 195.

Understanding Authentication for Identity Governance as a Service

![EAN: The remainder of this chapter is what’s left of Part I - Installing Identity Governance (Ch. 2 through 7). There wasn’t enough of it to leave it on its own, and it fits pretty well in this chapter.]

To verify the identity of users who log in to Identity Governance as a Service, you need an LDAP authentication server. Identity Governance as a Service supports Active Directory and eDirectory. For example, you can use the Identity Vault for Identity Manager as an authentication server. Users can

log in to Identity Governance as a Service immediately after installation if the users in the specified containers of the authentication server have passwords. Without these login accounts, only the bootstrap administrator can log in immediately.

- "Using One SSO Provider for Authentication" on page 19
- "Understanding Authentication with One SSO Provider" on page 19
- "Understanding the Bootstrap Administrator for Identity Governance as a Service" on page 19

Using One SSO Provider for Authentication

Identity Governance as a Service uses the One SSO Provider (OSP) authentication service, which supports the OAuth2 specification. With OSP, you can provide single sign-on access among Identity Governance as a Service and other applications, such as Identity Manager Home and Provisioning Dashboard. All requests to OSP use the http or https protocol.

NOTE: OSP is always the login mechanism for Identity Governance as a Service, even in a non-SSO environment.

Understanding Authentication with One SSO Provider

![EAN: Updated this section for IGaaS - removed all references to Kerberos and SAML, and revised remaining content.]

The OSP authentication service supports the OAuth2 specification and requires an LDAP authentication server. Identity Governance as a Service works with eDirectory and Microsoft Active Directory. You must create the LDAP server before NetIQ installs Identity Governance as a Service. Identity Governance as a Service currently supports only user name and password authentication.

How do OSP and SSO work?

When a user directs the browser to one of the browser-based components, the component determines that authentication is required and temporarily redirects the browser to the OSP service. The OSP service authenticates the user by asking the user for a name and password. OSP then issues an OAuth2 access token and redirects the browser back to the browser-based component. The component uses the token during the user's session to provide SSO access to any of the browser-based components.

How do I set up authentication and single sign-on access?

For OSP and SSO to function, you must specify the URLs for client access to each component, the URL that redirects validation requests to OSP, and settings for the authentication server. You can request that NetIQ provide this information during installation or afterward with the Identity Governance as a Service Configuration Utility. Or, you can specify it in the Roles Based Provisioning Module (RBPM) configuration utility if you integrate with Identity Manager.

Understanding the Bootstrap Administrator for Identity Governance as a Service

![EAN: Updated/removed most of this section for IGaaS.]

During installation, NetIQ creates a **bootstrap administrator** account that can immediately log in and configure Identity Governance as a Service. The bootstrap administrator can access all items in the administration console, except for **Reviews** and **Access Request**.

The bootstrap administrator account does not link to an account for a real person. You should not continue using this account after you have Identity Governance as a Service running in your environment. Instead, as soon as you have collected user accounts, assign one of the collected accounts as a global administrator. For more information about assigning authorizations, see “Understanding Authorizations in Identity Governance as a Service” on page 55.

Understanding Identity Reporting

![EAN: Updated this section for IGaaS.]

Identity Reporting generates a snapshot of the catalog and the state of permissions or reviews. You can use the reports to help meet compliance regulations for your business. You can also create custom reports if the predefined reports do not meet your needs. The user interface for Identity Reporting makes it easy to schedule reports to run at off-peak times for optimized performance.

There are two different versions of Identity Reporting:

![EAN: Reformatted this as bullets for IGaaS to make it easier to read.]

- One version comes with Identity Governance as a Service and is configured only to run with Identity Governance as a Service. This version uses the Identity Governance as a Service security module to determine who has access to the reports. Installed this way you can run both Identity Manager and Identity Governance as a Service reports by configuring an external data source where you store the data. However, Identity Reporting cannot be utilized for Data Collection in Identity Manager.
- The second version of Identity Reporting ships with Identity Manager. If you already have an Identity Manager environment and you want to utilize Data Collection, you must use this version of Identity Reporting. It uses the Identity Manager security module to determine who has access to the reports. It can run both the Identity Manager and Identity Governance as a Service reports by configuring an external data source to where you store the data.

Both versions of Identity Reporting can be installed in the Identity Governance as a Service environment and in the Identity Manager environment so that each system has its own reporting environment. However, if you have both versions of Identity Reporting installed, you must configure and run reports on two different systems. For more information about Identity Reporting, see the *NetIQ Identity Governance Identity Reporting Guide* on the Identity Governance documentation website (https://www.netiq.com/documentation/identity-governance/).

Configuring and Managing Identity Governance as a Service

![EAN: Updated this intro for IGaaS.]

This section helps you configure, manage, and customize Identity Governance as a Service. For example, you can configure Identity Governance as a Service fulfillment methods, as well as analytics and role mining settings. You can customize the labels in the user interface, customize email notification templates and fulfillment target templates, and integrate single sign-on with NetIQ Identity Manager. In addition, for users to log in to Identity Governance as a Service, you must first collect their account information from your environment and then configure authorization assignments to grant appropriate access.

2 Configuring Identity Governance as a Service Settings

![EAN: Updated the following para for IGaaS, and removed the sections in this chapter that obviously relate to the Config Utility. However, the procedures in the following sections - Configuring Fulfillment, and Configuring Analytics and Role Mining Settings - can be done in the main UI, so kept them.]

NetIQ configures many of the Identity Governance as a Service settings for you in the Identity Governance as a Service Configuration Utility. However, you can configure both fulfillment settings, as well as analytics and role mining settings, in the web console.

Configuring Fulfillment

The review process results in Identity Governance as a Service building a list of changes, or **changesets,** that are then submitted for **fulfillment**. The Identity Governance as a Service 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 as a Service users with global, provisioning, or bootstrap administrator authorization assignments can configure fulfillment options.

- “Configuring Identity Manager and Manual Fulfillment Methods” on page 24
- “Configuring Service Desk Fulfillment” on page 25
- “Understanding Fulfillment Status” on page 29

Identity Governance as a Service 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 as a Service fulfillment with your service desk system by adding and configuring a connector to your service desk system in Identity Governance as a Service **Fulfillment Configuration**.

To configure fulfillment methods:

1. Log in to Identity Governance as a Service 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 as a Service to your fulfillment service, and then configure mappings to create an appropriate fulfillment request.

   NOTE: You can download the fulfillment target templates, edit them, and upload them to Identity Governance as a Service instead of configuring the service parameters and mappings in the application. For more information, see “Customizing Fulfillment Target Templates” on page 43.

   ---

4. Make any additional connection updates for the selected fulfillment method 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.

8 (Optional) Select **customize** to change the default configuration for any fulfillment method you want to customize for a given application. Identity Governance as a Service 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 **Save Fulfillment Configuration** when you have made changes.

Configuring Identity Manager and Manual Fulfillment Methods

For Identity Manager automated, Identity Manager workflow, and manual fulfillment methods, Identity Governance as a Service 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 as a Service 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 “Automatically Fulfilling the Changeset” on page 83.

Identity Manager Workflow

Applies only when you integrate Identity Governance as a Service 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`

![EAN: Updated the following para for IGaaS, since customers won’t have access to the Config Utility.]

To connect to the external provisioning system, the workflow settings must be specified in the Identity Governance as a Service Configuration Utility. For assistance, contact NetIQ Customer Support.

For more information about the workflow process, see “Using Workflows to Fulfill the Changeset” on page 83.

Manual

Specify an individual or group of individuals to serve as the fulfiller. For more information about manual fulfillment, see “Manually Fulfilling the Changeset” on page 82.

![EAN: Updated the following para for IGaaS.]

To have Identity Governance as a Service email reminders to the fulfillers, NetIQ must configure email notifications for you in the Identity Governance as a Service Configuration Utility. For assistance, contact NetIQ Customer Support. For information about customizing emails, see “Customizing the Email Notification Templates” on page 39.

Configuring Service Desk Fulfillment

Identity Governance as a Service 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 as a Service Fulfillment target configuration allows you to customize your incidents for these various systems. When you create a service desk fulfillment target in Identity Governance as a Service, you provide the connection information and credentials for the target system as well as a default configuration specifying the fields you want Identity Governance as a Service 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 as a Service exposes the following data fields from each changeset item to the fulfillment target connectors:

changeItemId

A long value containing the internal change item number

changeRequestType

A string value containing one of the following values:

- `REMOVE_BUS_ROLE_ASSIGNMENT`
- `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_TECH_ROLE_ASSIGNMENT`
- `REMOVE_APPLICATION_FROM_USER`

userName

Display name of the user that is the target of the change item

accountName (optional)

Name of the account 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

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 as a Service 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 “Customizing the Collector Templates for Data Sources” on page 42.![EAN: Left this for IGaaS because customers will be able to customize the collector templates in the web UI.]

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 as a Service 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 as a Service 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 as a Service template populates or modify the default mappings of the template, contact your NetIQ 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 as a Service 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 as a Service 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 as a Service 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 as a Service 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 as a Service template populates or modify the default mappings of the template, contact your NetIQ technical support representative for details.

Use the following table to understand the Identity Governance as a Service 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 as a Service 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 as a Service 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 as a Service 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 as a Service template populates or modify the default mappings of the template, contact your NetIQ technical support representative for details.

Use the following table to understand the Identity Governance as a Service 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 as a Service 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"

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 as a

Service 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 as a Service 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 as a Service 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 as a Service 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 as a Service 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 as a Service 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 as a Service 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.

Configuring Analytics and Role Mining Settings

Identity Governance as a Service tracks key risk indicators so that you can monitor these risk factors in your environment and make improvements based on the collected metrics. In addition to the preset metrics, you can also create custom metrics based on your business needs. Additionally, you can also choose to include or exclude specific decision support information, and configure role mining settings.

- “Creating Custom Metrics” on page 33
- “Viewing Entitlement Assignments Statistics to Leverage Roles” on page 34
- “Viewing Account Statistics and Details” on page 34

To configure analytics and role mining settings:

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

   NOTE: A 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 **Administration** > **Analytics and Role Mining Settings**.
3. (Optional) Under **Decision Support**, specify whether business role authorization status, similarity statistics in reviews and access requests, and login statistics for review item users and accounts are included in the guidance provided to reviewers, review owners, review administrators, and access approvers.
   - **3a** Deselect option **Show business role authorization status** either if business roles are not used or if the reviewer of user reviews or access request approver does not need guidance about whether the review or request item was authorized by business role.
   - **3b** Deselect option **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 option **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.
4. (Optional) Under **Similarity Profile**, select additional attributes to use in the similarity profile so that Identity Governance as a Service can provide decision support.

TIP: Use wildcard * to search for attributes.

5 Under **Role Mining**, enter the **Maximum** number of results that should be returned when mining business roles using the directed role mining approach.

6 Specify which additional user **Attributes** should be used for both directed and visual business role mining.

NOTE: User attributes with zero strength will not be displayed in the directed mining recommended attribute bar graph and visual attribute map.

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

8 Under **Metrics Collection**, select one or more items, and then specify **Actions** > **Set collection interval** to change the default setting of 24 hours between metrics collections or disable collection.

TIP: Click an item name to view detailed information about the metric, including a list of metric columns' aliases and corresponding data types.

NOTE: In addition to the default metrics, you can create custom metrics. For more information, see "Creating Custom Metrics" on page 33.

9 Enter **Hours** or **Disable collection**.

10 Click **Save** to set the new interval.

11 (Optional) Select one or more times and then select **Actions** > **Collect metrics** to initiate a metrics collection on demand.

12 (Optional) Select one or more items and then select **Actions** > **Download** to download metrics in CSV format.

13 (Optional) When a collection is running and you want to cancel it, select the item or items, select **Cancel Collection**, then click **Cancel Collection** to confirm.

Creating Custom Metrics

In addition to default metrics, Identity Governance as a Service provides the ability to create SQL statements to query your operations database for additional statistics. The product also displays an * in front of the names of the custom metrics to distinguish them from other metrics. You can click the metric name to view the details of the metric.

After creating custom metrics, you can **Collect Metrics**, and **Download** metrics using the same procedures as for default metrics. In addition, you can select **Actions** > **Delete Custom** to delete custom metrics.

To create a custom metric:

1 Log in as a Global or Data Administrator.

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

3 Next to **Metrics Collection**, select **+**.

4 Enter **Name** for the new metric.

5 (Optional) Select an existing category or **Add Custom** category; and enter **Description**.

6 Select **SQL Statement** and enter a SQL select statement.

NOTE: Identity Governance as a Service automatically checks for statement errors and potential SQL injections to prevent invalid or malicious code. However, ensure that you have defined your query correctly, because once you have created and saved the custom metric you cannot edit it. If needed, you will have to delete the custom metric, and then create a new one to change your definition.

7 Select **Metrics Columns** and then **Add Column** to specify an alias and type for each column selected in the SQL statement. For example, given the SQL statement: `select count(id) as active from role_policy where state = 'ACTIVE'`, add a metric column `active` with a type of `Long`.

8 Select **Save**.

Viewing Entitlement Assignments Statistics to Leverage Roles

To understand how your entitlement assignments conform to your business policies, you can view the **Role Leverage** widget on the **Overview** page. It includes a graphical overview of the effectiveness of your roles over a period of time, the entitlements assignments using roles versus entitlements assigned directly, and the ratio of indirect role-based entitlements versus total entitlement assignments in percentage. To change the default time range, 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 99.

Viewing Account Statistics and Details

On the **Overview** page, you can see an account statistics summary for your environment. To see data, you 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, collect metrics on demand after every publication.

Identity Governance as a Service displays available metrics on the summary panel followed by a chart for each metric per risk levels. To change the default settings:

- Select the calendar icon to change the time range for account statistics.
- 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 under **Account Statistics**, select **View statistic 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 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.

5e Customize the row and column headings.

6 Type a name for the customized view and select **Save**.

3 Customizing Identity Governance as a Service for Your Enterprise

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

Localizing to the User’s Preferred Language

Identity Governance as a Service automatically localizes the attributes and email text according to the user’s preferred language:

- Chinese Simplified
- Chinese Traditional
- Danish
- Dutch
- English
- French
- German
- Italian
- Japanese
- Polish
- Portuguese
- Russian
- Spanish
- Swedish

Identity Governance as a Service cannot always reconcile the differences in language that occur when different users collect data and run reports on that collection. For example, a user in Spain runs a collection for a set of data. Then a user in Russia runs a report against that collection. The fields in the report appear in Russian since that is the report user's default language. However, the reported data is in Spanish because the collection occurred on a computer with Spanish as the default language.

You can customize the content in the provided languages. Alternatively, you can apply a new language to Identity Governance as a Service and OSP.

Customizing the User Interface

![EAN: This section contained only one Sect2 and it's not a long section anyway, so removed the heading "Customizing the Labels in the Identity Governance Interface".]

Identity Governance as a Service and OSP automatically display content in the user interface according to your preferred language. You can customize content such as attributes names and informational messages using a text editor.

You might customize the content if your organization requires special terminology for some or all attributes. For example, you might refer to *user ID* as *account name*. You can change all instances of *user ID* in the catalog.

For more information about translating the content to a new language instead of customizing it, see "Translating Content for Identity Governance as a Service and One SSO Provider" on page 39.

Some organizations might want to customize the default names for the attributes, risk levels, and navigation items in Identity Governance as a Service. The `.properties` file for customizing this content is available from the Identity Governance as a Service interface.

To customize the labels:

1. Log in to Identity Governance as a Service as a Global Administrator.
2. Select **Administration > Localization Import and Export**.

   Identity Governance as a Service lists the `.properties` files by language.
3. For the language that you want to customize, select **Download**.

   Depending on your browser settings, you might be prompted for the download path.

   NOTE: If prompted, do not rename the `.properties` file. Identity Governance as a Service cannot upload a file that does not match the expected name.

   ---
4. In a text editor, customize the displayed text for the attributes that you want to change.

   For example, you want to change all instances of *user ID* to *account name*. When you search for *user ID*, you will find the following type of string:

   ```
   com.netiq.iac.persistence.ops.AttributeDefinition.USER.userID=User ID from source
   ```

   Change `User ID from Source` to `Account Name from Source`.

   WARNING: Do not modify any text in the code string before the = sign. For example, `com.netiq.iac.persistence.ops.AttributeDefinition.USER.userID=`. Identity Governance as a Service might not function appropriately if you change the code string incorrectly.

   ---

5 Save and close the file.

6 To submit the modified file, select **Upload** for the language that you customized.

7 Refresh the browser window to view the changes.

NOTE: Depending on the browser settings, you might need to sign out of Identity Governance as a Service, clear the cache in the browser, then log in again.

Translating Content for Identity Governance as a Service and One SSO Provider

![EAN: There's no way to do this in the IGaaS main UI, so updated the following para and deleted all subsections except the last one. "Adding the Translated Labels ..." can be done in the main web UI, but removed it because it's useless without being able to do the previous steps. Removed the remaining Sect2 heading "Verifying the New Translations" and absorbed the procedure into this section, since customers will be able to do it in the web UI.]

If the default languages for Identity Governance as a Service and OSP do not meet your organization's needs, NetIQ can translate the strings and user interface content to a different language. For example, you might want to interact with Identity Governance as a Service in Norwegian (language code=nb). To use a non-default language, you need to translate the `.properties` files of an existing language. For assistance with translating strings and user interface content, contact NetIQ Customer Support.

For more information about customizing the content for a current new language instead of adding a language, see "Customizing the User Interface" on page 38.

To verify the new translations:

![EAN: Probably need to add a couple of steps here for login, etc. (any particular user account needed?) The procedure originally assumed that the admin would already be in the UI.]

1 In a browser, clear the browser cache.

2 Change the browser language to the language that you requested be added to Identity Governance as a Service.

3 Enter the URL for Identity Governance as a Service.

4 Log in to Identity Governance as a Service.

5 Verify the translated content.

Customizing the Email Notification Templates

Identity Governance as a Service can notify users of tasks in their queue, as well as other review events, as specified in review definitions. Various other events might trigger email notifications depending on your configuration. The application supplies default templates for the email notifications and uses these as is unless you customize them for your environment. Identity Governance as a Service allows you to modify an XML file that contains the email text in the languages supported for Identity Governance as a Service. You can edit the XML file in one of the following programs to customize it for your company:

- XML editor

- Text editor
- Designer for NetIQ Identity Manager

To modify email template content:

1. Log in to Identity Governance as a Service as a Global Administrator.
2. Select **Administration > 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 as a Service cannot upload a file that does not match the expected name.
4. (Conditional) To customize email templates for specific functional areas by language, scroll through the list of functional areas, such as bulk data and business role approval, and select **Download** for the languages for your locale.
5. (Conditional) To customize specific email templates, under **View functional areas by**, select **Email Name**, select an email name from the list, and then select **Download**.

   TIP: Click on an email name and then select **Email source preview (en)** to view the template. Enter an email address to **Send notification preview**.
6. 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 as a Service might not function appropriately if you change the code strings incorrectly.
7. Save and close the files.
8. To submit the modified files, select the **Upload** icon next to **email templates (all languages)**.
9. Select **Save**.

To add an image to the email template:

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

   TIP: Use the base64encode website or similar encoders to encode the image.
2. Download the email template.
3. Add the `<img src=" %base64-value% "/>`tag where you want the image to appear. For example, `<p>Powered by <img src="..."/></p>`.
4. Upload the modified file.

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

Token	Notes
approverName	Business role approver
certifierFullName	Reviewer's full name
certifyTaskLink	Link to task
changesetId	Unused in the Certification External Provisioning Start Error template
content	Used in the generic email template
curatorFullName	Bulk data feed curator
error	Fulfillment error
errorMessage	Error message text
externalPrdLink	Unused in the Certification External Provisioning Start Error template
feedName	Bulk data update definition
fulfillerName	Full name of the fulfiller
host	The workflow hostname
inputFile	Bulk data CSV file
link	URL link
message	The output message from a system process.
newTaskType	Used in the Certification Auto Provisioning Start Failed template
ownerName	Owner of the SoD policy
permissionsToLose	List of application permissions
prdName	Workflow name used in the external fulfillment template
prevReviewerFullName	User that the task was reassigned from
productName	Configured product name, such as Identity Governance or Access Review
reassignedByFullName	User who reassigned the task
reassignComment	Optional comment entered at reassignment
retryCount	Number of fulfillment items in a retry state
reviewLink	URL link to review
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

Token	Notes
violations	Used in the Detected SoD Violation email template.

NOTE: Some email templates expect only certain processing tokens, so 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 real email.

![EAN: Reworded the following para for IGaaS.]

The product name can be customized to brand it for your company instead of the default name of NetIQ Identity Governance as a Service. The email templates also use this product name. For assistance with rebranding the product name, contact NetIQ Customer Support.

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 Service as a Global or Data administrator.
2. Select **Administration**.
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**.

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 Service as a Global or Fulfillment administrator.
2. Select **Administration > Fulfillment Target Templates**.
3. Select a template, and then select **Download** or **Disable**.
4. Edit the content.
5. Under **Fulfillment Target Templates**, select **+**.
6. Enter a template name and description and then browse to the location of the updated file.
7. Select **Save**.

Specifying Additional Fulfillment Context Attributes

By default, the system sends basic information on how to perform fulfillment after a review or a request. Optionally you can 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 Service as a Global or Fulfillment administrator.
2. Select **Administration > Fulfillment Context Attributes**.
3. Specify **Requester**, **Recipient**, **Account**, and **Permission** attributes.

   TIP: Use wildcard * to search for attributes.

   ---
4. Select **Save**.

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 as a Service supported coverage map types, keywords, syntax, and entity-entity relationships in order to create and load coverage maps.

- “Creating Coverage Maps” on page 44
- “Loading Coverage Maps” on page 48

Creating Coverage Maps

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 44
- “Supported Syntax” on page 44
- “Supported Relationships” on page 46
- “User Access Review Coverage Map Examples” on page 46
- “Account Review Coverage Map Examples” on page 47
- “Access Request Coverage Map Example” on page 48

Supported Coverage Map Types and Keywords

Identity Governance as a Service 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

Identity Governance as a Service supports the following 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 as a Service stores only 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 be accessed only from the `Reviewer` or `Approver` criteria cell.

Identity Governance as a Service supports the following 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 as a Service 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 header cells use keywords and the criteria cells use 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, the supervisor of the account owner is specified as the reviewer for all shared accounts and the supervisor of the holder of the account is 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, the policy owner is assigned as the approver.

Loading Coverage Maps

To load coverage maps:

1. Log in to Identity Governance as a Service as a Global or Data Administrator.
2. Select **Administration**.
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** Enter 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.

Customizing Categories

Identity Governance as a Service allows you to set up categories to organize applications, permissions, business roles, and technical roles. You can define these categories in Identity Governance as a Service 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 Service as a Global or Data Administrator.
2. Select **Administration** > **Categories**.
3. To add new categories, select **+** and enter 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.

Customizing Review Display

Identity Governance as a Service enables customization of columns displayed in reviews by enabling you to customize user attributes display per review type and then by using them to customize display for each review definition.

To select user attributes that can be displayed:

1. Log in to Identity Governance as a Service as a Global or Review Administrator.
2. Select **Administration** > **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: Review administrators can either use these default per review type settings or further customize default columns for each review using **Reviews > Definitions > + > Default Reviewer Display Preferences**. Only attributes selected here will appear as an option in **Default Reviewer Display Preferences**.

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**.

Configuring Reasons for Review Actions

Identity Governance as a Service allows you to configure reasons for review actions for analytical and reporting purposes. A 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 the **Modify** action in a **User Access Review** or selects **Modify with instructions** in an **Account Review**.

1. Log in to Identity Governance as a Service as a Global or Review Administrator.
2. Select **Administration** and **Change Reviewer Reasons** or **Modify Review Item Reasons**.
3. To add a new reason, click **+** and enter 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, select 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 on 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.

Extending the Identity Governance as a Service Schema

Identity Governance as a Service 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 as a Service schema.

Extending the schema is a simple process of adding attributes to the default schema provided. You can view the default schema for Identity Governance as a Service in the console. You log in as a global administrator or data administrator to view the schema. The schema is listed under the **Data Administration** heading.

- “Adding or Editing Attributes to Extend the Schema” on page 51
- “Adding Attributes to a Collector” on page 52
- “Viewing Available Attributes in Business Roles” on page 53

Adding or Editing Attributes to Extend the Schema

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

NOTE: You cannot extend the schema for groups. Identity Governance as a Service 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 as a Service 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 allows 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.

Listable Options

Select how you want the attribute displayed in the Identity Governance as a Service 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 as a Service 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 as a Service.

- 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 all listable and searchable options for these attributes.

---

5 Select **Save**.

Adding Attributes to a Collector

If a collector you are using does not contain the schema you need, you can extend the schema of the collector by adding additional attributes. The collector must be created and configured before you perform the following steps. For more information, see Chapter 16, “Creating and Managing Data Sources,” on page 133.

1 Log in to Identity Governance as a Service 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 as a Service 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 allows 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.

Listable Options

Select how you want the attribute displayed in the Identity Governance as a Service 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 as a Service 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 as a Service.

- 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**.

Viewing Available Attributes in Business Roles

When you create a business role, you define a membership expression that searches for all users that meet a certain criteria to be added to the business role. For more information, see “Defining Business Roles” on page 99.

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 “Adding or Editing Attributes to Extend the Schema” on page 51.

---

4 Adding Identity Governance as a Service Users and Assigning Authorizations

Individuals who can log in to Identity Governance as a Service are **Identity Governance as a Service users**. The authentication server for Identity Governance as a Service must include login information for all Identity Governance as a Service 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 as a Service, you can assign them to one of the built-in authorizations.

Understanding Authorizations in Identity Governance as a Service

Identity Governance as a Service relies on authorizations to define a fixed set of authorizations and permissions. Identity Governance as a Service authorizations can be global or runtime:

- **Global authorizations** are constant within Identity Governance as a Service and assigned through the Identity Governance as a Service **Administration** settings. Identity Governance as a Service maintains the set of privileges granted by the authorization. For more information, see "Global Authorizations" on page 55.
- **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 "Runtime Authorizations" on page 57.

![EAN: Updated the following note for IGaaS.]

NOTE: After NetIQ installs Identity Governance as a Service, you 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 as a Service and assign authorizations to them. For more information about the bootstrap administrator, see "Understanding the Bootstrap Administrator for Identity Governance as a Service" on page 19.

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 "Assigning Authorizations to Identity Governance as a Service Users" on page 60.

Global Administrator

The Global Administrator is the primary authorization and can:

- Perform all Identity Governance as a Service actions
- Assign all Identity Governance as a Service 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, fulfillment status, and the **Overview**. However, an account assigned to the Auditor authorization might also be specified as a Review Auditor in a review definition. For more information, see "Runtime Authorizations" on page 57.

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
- Create a business role
- Modify a business role
  - Add or change role owners, 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

- Delegate responsibility by assigning application administrators, application owners, or manual fulfillers to applications in the catalog![can the Data Admin still designate fulfillers now that it has moved from the catalog assignment method?]
- Assign delegates for users
- View data collection, data summary, and system trends in the **Overview**

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 as a Service

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 as a Service
- 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 as a Service.

Separation of Duties Administrator

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

Runtime Authorizations

Assign runtime authorizations when you need them. For more information, see “Assigning Authorizations to Identity Governance as a Service Users” on page 60.

Access Request Approver

Access Request Approvers confirm whether to approve or deny requested access in the Request application. Identity Governance as a Service 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, see Chapter 10, “Creating and Managing Business Roles,” on page 95.

Business Role Manager

A Business Role Manager can edit the assigned business roles, create, and delete new draft versions of the role but cannot delete the business role completely.

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 “Specifying Reviewers” on page 79.

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 “Specifying Reviewers” on page 79.

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

Adding Identity Governance as a Service Users

Until you collect data for your Identity Governance as a Service users, no one can log in to the application without using the bootstrap administrator account. Do not use the bootstrap administrator account after you add your Identity Governance as a Service users to the Identity Governance as a Service 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 as a Service” on page 19. For more information about mapping attributes, see “Configuring the Data Source for Post Authentication Matching” on page 175.

To add Identity Governance as a Service users:

1. Log in to Identity Governance as a Service with an Identity Governance as a Service administrator account, such as the bootstrap administrator.
2. In the **Overview**, select **Identity Sources**.
3. Under **Identity Sources**, select the LDAP authentication server that NetIQ specified during installation.

   Alternatively, you can specify a CSV file.

   NOTE: If Identity Governance as a Service does not list the authentication server, select **+** to add the identity source. For more information, see “Creating Identity and Application Sources” on page 145.

   ---

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 17, “Creating and Monitoring Scheduled Collections,” on page 155.
5. When collection is completed, select the icon for **Publish identities now**.
6. Assign Identity Governance as a Service authorizations to the appropriate identities that you collected.

   For more information, see “Assigning Authorizations to Identity Governance as a Service Users” on page 60.

Assigning Authorizations to Identity Governance as a Service Users

The method for assigning authorizations in Identity Governance as a Service 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	**Administration** 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
Technical Role Owner	Technical role definition	Technical Roles Administrator or Global Administrator

Changing Passwords for Administrative Users

![EAN: This section used to be a chapter and was earlier in the book. After I removed so much content for IGaaS, this section was too short to be a chapter and seemed lost by itself, so I moved it to this chapter and updated the content for IGaaS. (This task would require command line access.)]

Identity Governance as a Service has a number of embedded users to make the product work. For example, there is a bootstrap administrator and database users. You might need to change the passwords for these users to meet security standards at your company. For assistance with changing passwords for these embedded users, contact NetIQ Customer Support.

5 Integrating Single Sign-on Access with Identity Manager

If you have installed Identity Manager, your users can log in a single time to access the Identity Manager applications, Identity Reporting, and Identity Governance as a Service. NetIQ uses the OSP service for OAuth authentication, which provides users single sign-on access from the Identity Manager Home page. To ensure single sign-on access, you must configure both Identity Manager and Identity Governance as a Service. Users can easily shift between the two applications without needing to enter their credentials a second time.

Identity Governance as a Service must use the same authentication server that the identity applications use.

Checklist for Integrating Identity Governance as a Service with Identity Manager

Use the following checklist to ensure a proper integration between the products:

	Checklist Items
❑	1. To ensure that you have the correct software versions for integration, review the latest release notes for Identity Governance as a Service and Identity Manager identity applications. For more information, see the Identity Manager Documentation site (https://www.netiq.com/documentation/identity-manager/).
❑	2. (Conditional) Create an index in eDirectory for the login attribute if you do not use a standard login attribute to ensure a rapid response time. **NOTE:** This step requires OSP changes on the Identity Governance as a Service server. For assistance, contact NetIQ Customer Support. ![EAN: Updated this step for IGaaS.]
❑	3. Ensure that users can link to Identity Manager Home from Identity Governance as a Service. For more information, see "Adding a Link to Identity Manager Home in the Identity Governance as a Service Menu" on page 64.
❑	4. Ensure that Identity Governance as a Service connects to the authentication server for Identity Manager. For more information, see "Using the Same Authentication Server as Identity Manager" on page 64.
❑	5. Update Identity Manager Home to connect to Identity Governance as a Service. For more information, see "Configuring Identity Manager for Integration" on page 65.

	Checklist Items
❑	6. (Optional) Integrate Identity Governance as a Service with the workflows used in Identity Manager. For more information, see "Using Workflows to Fulfill the Changeset" on page 83 and "Configuring Fulfillment" on page 23.

For more information about Identity Manager, see the *NetIQ Identity Manager Home and Provisioning Dashboard User Guide*.

Configuring Identity Governance as a Service for Integration

For proper integration, you must link Identity Governance as a Service to the Identity Manager Home page for the identity applications. You can also choose to use the same authentication server that the identity applications use to verify login attempts. This process includes the following activities:

- "Adding a Link to Identity Manager Home in the Identity Governance as a Service Menu" on page 64
- "Using the Same Authentication Server as Identity Manager" on page 64

Adding a Link to Identity Manager Home in the Identity Governance as a Service Menu

This section describes how to add a link in Identity Governance as a Service so users can easily switch to Identity Manager Home.

1. Log in to Identity Governance as a Service with an account that has the Global Administrator authorization.
2. Select **Administration > General Settings**.
3. For **Home Page URL**, specify the URL for Identity Manager Home.
4. Select **Save**.
5. Sign out of Identity Governance as a Service.
6. (Optional) To verify the integration, complete the following steps:
   - **6a** Log in to Identity Governance as a Service. Verify that Identity Governance as a Service lists **Home** in the navigation pane.
   - **6b** Select **Home**, and verify that it takes you to the Identity Manager Home page.

Using the Same Authentication Server as Identity Manager

![EAN: Another procedure that requires access to Tomcat and the Config Utility. Updated this para for IGaaS.]

Identity Governance as a Service can be configured to use the same authentication server as Identity Manager identity applications for verifying users who log in. However, if the Identity Manager authentication server was not specified during your Identity Governance as a Service installation, for example if you added Identity Manager to your environment afterwards, NetIQ must perform this configuration for you. For assistance, contact NetIQ Customer Support.

Configuring Identity Manager for Integration

![EAN: Another procedure that requires access to the file system on the IG server. Updated this section for IGaaS.]

To ensure proper integration with Identity Manager, your version of the Identity Manager identity applications must be updated to recognize Identity Governance as a Service. The process includes copying files from the Identity Governance as a Service installation to the Identity Manager identity applications installation. Since the steps require access to the file system on the Identity Governance as a Service server, NetIQ must perform this integration for you. For assistance, contact NetIQ Customer Support.

NOTE: Ensure that you have configured single sign-on for the Identity Manager identity applications. For more information, see "Configuring Single Sign-on Access in Identity Manager" in the NetIQ Identity Manager - Administrator's Guide to the Identity Applications (https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/bookinfo.html).

Configuring a File Authentication Source for the Bootstrap Administrator

![EAN: Another procedure that requires access to the file system on the IG server. Updated this section for IGaaS.]

Identity Governance as a Service allows you to use a file as the authentication source for the bootstrap administrator instead of LDAP authentication. However, since the process requires access to the Configuration Utility and file system on the Identity Governance as a Service server, NetIQ must perform this configuration for you. For assistance, contact NetIQ Customer Support.

Creating and Running Reviews

Review Administrators can create several types of reviews to focus reviewers on different types of access, such as user access reviews, mapped and unmapped account reviews, and business role ![or group -- didn't make 2.5 but should be there next release] membership reviews. For each type of review, administrators select the users, accounts, applications, permissions, or roles to be reviewed, and define the review process and participants. Administrators and review owners can also preview reviews before going live with the reviews which generate tasks for reviewers. Reviewers determine whether to keep, remove or modify access, change user assignments, or whether to retain role ![or group] membership for each item assigned to them in the review.

Reviews might contain a single stage, with each review item being assigned to a single reviewer or group of reviewers or multistage, with each review item being assigned to multiple reviewers who act on review items only after the previous reviewer completes an action.

- Chapter 6, "Creating and Modifying Review Definitions," on page 69
- Chapter 7, "Running a Review Instance," on page 81

6 Creating and Modifying Review Definitions

After you have data in your catalog, and (optionally) have customized review display columns and configured reasons for review actions by accessing the **Administration** 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

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

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 a **User Access Review** does not impact this date.

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

Understanding the 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 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.![add policy admin when functional]

NOTE: The Identity Governance as a Service 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 as a Service does not notify you of the failure.

For multistage reviews, if at any stage in the review an exception occurs, Identity Governance as a Service 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.

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 the Sarbanes-Oxley Act (SOX) or the Health Insurance Portability and Accountability Act (HIPAA).

TIP: For information about certification policies, see Chapter 13, “Creating and Managing Certification Policies,” on page 123. Once a review definition is referenced in an active certification policy, it cannot be deleted.

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 the 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 be applicable only to the current review instance. Only changes made in the **Reviews > Definitions** itself will be reflected in future review run instances.

Reviewing Items

When a review run, or **review instance**, is live, the server generates **review items** based on the criteria in the review definition. 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 as a Service 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 as a Service 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 as a Service moves the items to the escalation reviewer, if any, or if not, the review owner exception queue at the start of the review.

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. In addition, it allows you to preview an email source, and add new notifications by selecting an email source and using the preset defaults. Identity Governance as a Service also provides several email templates to address the various parts of a review. You can customize these templates for your environment. For more information, see "Customizing the Email Notification Templates" on page 39.

Escalating Review Items

Identity Governance as a Service 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 as a Service 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 as a Service sends the entire review to the escalation reviewer instead of to the members of the group. To prevent this, enable **Allow self review in all stages**, and Identity Governance as a Service then sends the review to the members of the group instead of to the escalation reviewer.

Setting a Review Expiration Policy

Review definitions contain an expiration policy. Review administrators and owners specify the actions that Identity Governance as a Service 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 assigned accounts, permissions, or roles
- Complete the review with any final decisions that have been made, assign remove decision to all other items, and send all to fulfillment and the auditor, if these are defined
- 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 as a Service 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 as a Service, review definitions have the default expiration policy set to terminate the review and discard any decisions.

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 as a Service 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 as a Service 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**, 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 as a Service takes the following actions:

- Does not forward anything to fulfillment
- Marks the review run as terminated

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 “Fulfilling the Changeset for a Review Instance” on page 82.

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.

Selecting a Review Type

Identity Governance as a Service enables administrators to create four 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 the review definition using the procedures in “Creating a Review Definition” on page 74.

	User Access Review	Unmapped Accounts	Account Review	Business Role Membership Review
Identities	Y	N	Y	N
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
Unmapped Accounts	N	Y	Y	N
Mapped Accounts	Y You can review only a user’s access to an account in this type of review. Use **Account Review** for reviewing an account in totality.	N	Y	N
Applications	Y	Y	Y	N

	User Access Review	Unmapped Accounts	Account Review	Business Role Membership Review
Technical Roles	Y	N	N	N
Business Roles	N	N	N	Y

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.

![EAN: The following procedure is way too long and contains info that could be covered outside the procedure. Leaving as is in IGaaS for now ....]

1. Log in as a Review Administrator.
2. Select **Definitions**.
3. Select **+** to create a new review definition.
4. Select the review type.
5. Name and describe the review.
6. (Optional) For **Review Instructions**, enter 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.

NOTE: The options for specifying review items will differ based on the review type:

- If you select **User Access Review**, go to Step 8 on page 74
- If you select **Unmapped Accounts**, go to Step 9 on page 76
- If you select **Account Review**, go to Step 10 on page 76
- If you select **Business Role Membership Review**, go to Step 11 on page 76

---

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 enter 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 as a Service.

   Select roles

   Indicates that you want to enter 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 enter 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 enter 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.

Risk

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

Indicates that you want to review all users with 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 as a Service 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 182.

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 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 enter specific account names as well as define criteria such as last login, last unmapped account review, or number of logins.

All applications

Specifies 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 that you want to review.

Use the following options:

Accounts

Specifies the combination of mapped and unmapped accounts to review.

Identities

Specifies to review all users or select users.

Applications

Specifies to review all applications or select applications.

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

Use the following options:

All business roles

Specifies to review all business roles.

Select business roles

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

12 (Optional) Further expand or restrict **User Access Review items** and **Account Review items** by selecting related check boxes. For more information, see "Expanding and Restricting Review Items" on page 78.

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

Because the information is a snapshot of the current state of the catalog, Identity Governance as a Service reports approximate numbers. Depending on when you run the review, the catalog might have changed.

Based on the number of items to be reviewed, 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.

14 (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.

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

For more information about types of reviewers, see "Specifying Reviewers" on page 79.

16 (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 "Specifying Reviewers" on page 79.

17 (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 80.

---

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

18a Specify the Escalation Reviewer. If you do not specify a value, Identity Governance as a Service escalates tasks to the Review Owner.

18b For **escalation timeout**, specify the amount of time allowed for the Reviewers to complete their tasks. You must use whole numbers for the value.

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

19a For **Review period**, specify the length of time allowed for the review run.

19b For **Expiration policy**, specify what happens when a review expires without being completed.

19c For **Partial approval policy**, specify whether partial approvals are allowed and if so, whether or not partial approvals will occur automatically.

19d 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`.

20 (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.

---

21 (Optional) For **Schedule**, if you want the review runs to begin automatically and repeat automatically, select **Active** and select the appropriate schedule. Select **Start scheduled review in Preview mode requiring manual go live** to start a review in preview mode.

NOTE: The Identity Governance as a Service 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 as a Service does not notify you of the failure.

---

22 (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 **Administration > 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 a descending or ascending arrow, and change the column display by using the display options settings menu.

---

23 Save the review.

Expanding and Restricting Review Items

![EAN: Technically we shouldn't have a single Sect2 under a Sect1, but leaving this alone in IGaaS for now ....]

In addition to specifying review items using different combinations of users, permissions, accounts, and roles selections, administrators can further expand or restrict items being reviewed in an **User Access Review** and an **Account Review**. For example, selecting **Additionally review accounts for the selected users and permissions** for **User Access Review items** would enable you to review the accounts that grant the specified permission for the selected set of users and make a decision on it, whereas without selecting this option you will see the account name in the detail information, but will not be able to make a decision about it. You can also select options related to roles, such as to show and review permissions that are part of a technical role or limit review items based on whether the items were authorized or not 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 should be added as an authorized resource for the business role. For more information, see "Adding Authorizations to a Business Role" on page 103.

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 as a Service 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.

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:

Reviewing User Access	Reviewing Unmapped Accounts	Reviewing Accounts	Reviewing Business Role Membership
Supervisor of the individual being reviewed	Owner of the application being reviewed	Supervisor of the individual being reviewed	Supervisor of the individual being reviewed
Owners of the applications being reviewed	Selected users or groups	Owner of the application being reviewed	Business role owner
Owners of the permissions being reviewed (not available for roles reviews)	Account custodian	Owner of the account being reviewed	Selected users or groups
Holder of the permission being reviewed, called self review	Business role	Selected users or groups	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 “Understanding Identity, Application, and Permission Management” on page 177. For more information about coverage maps, see “Using Coverage Maps” on page 43.

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 as a Service 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 as a Service 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**. This individual resolves all review tasks that are not completed on time. 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 as a Service 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 “Runtime Authorizations” on page 57.

Improving Performance in Large Scale Reviews

![EAN: Updated this section for IGaaS, since the materialized view has to be enabled in the config utility.]

Identity Governance as a Service supports **materialized view**. Materialized view is a snapshot or an instance of time used to optimize performance in large scale reviews. If NetIQ has enabled this view in your environment, 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. The search and sort features will use the values at the time the materialized view was either created or last refreshed.

NOTE: For small scale reviews, caching of review item names is *not* recommended.

By definition, a materialized view is a snapshot, so 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 viewing the review definition of a review instance, and clicking **Refresh**. In addition, you can **Enable** or **Disable** the caching of review item names for that review instance.

NOTE: If materialized view is not enabled, the **Cache review item names** check box will not be displayed. For assistance in enabling materialized view, contact NetIQ Customer Support.

---

7 Running a Review Instance

When you start a review in live mode, Identity Governance as a Service 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 as a Service notifies fulfillers if they have change items. For more information, see “Checklist for Managing a Review in Live Mode” on page 222.

Completing Review Tasks

Identity Governance as a Service 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 “Runtime Authorizations” on page 57. For automated fulfillment configurations, Identity Governance as a Service sends fulfillment changes to configured systems. For more information about automated fulfillment, see “Configuring Fulfillment” on page 23.

For more information about completing review tasks, see Chapter 25, “Instructions for Reviewers,” on page 215.

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**. Any decisions made before completing an in-progress review are retained and forwarded to fulfillment, when selecting **Approve**, if partial approval was allowed in review definition **Duration > Partial approval policy**.

For more information, see “Approving the Review” on page 225.

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 as a Service determines which applications have change items. Depending on the specified fulfillment type for the application, Identity Governance as a Service performs one of the following actions:

- “Manually Fulfilling the Changeset” on page 82
- “Using Workflows to Fulfill the Changeset” on page 83
- “Automatically Fulfilling the Changeset” on page 83

Data administrators![data or fulfillment?] can configure the fulfillment method for an application. For more information, see “Configuring Fulfillment” on page 23.

Manually Fulfilling the Changeset

During the fulfillment stage of the review instance, Identity Governance as a Service 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 as a Service 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 change sets might have a reason, and a user selection might also be required. For more information, see “Configuring Reasons for Review Actions” on page 50. For more information about specific change request types, and fulfillment status, see “Configuring Fulfillment” on page 23.

Identity Governance as a Service 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 “Customizing the Email Notification Templates” on page 39.

For more information about performing fulfillment tasks, see Chapter 27, “Instructions for Fulfillers,” on page 227.

Using Workflows to Fulfill the Changeset

If you integrate Identity Governance as a Service 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 as a Service. The workflow also must have inputs specified in the following fields:

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

Identity Governance as a Service 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 as a Service, 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*.

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 as a Service 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 as a Service can revert to manual fulfillment or to using an Identity Manager workflow.

Confirming the Fulfillment Activities

When the Fulfiller confirms the review fulfillment, Identity Governance as a Service 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 as a Service. After the administrator collects and publishes application sources again, Identity Governance as a Service updates the status of the fulfillment of all change sets except modify change sets.

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" on page 226.

II Using Policies in Identity Governance as a Service

Policies show external auditors that you have structures in place to ensure compliance in your environment. Separation of duties policies work to keep any single user from having too much access. Business roles automate applying appropriate access based on job function. Risk factors and weighting allow Identity Governance as a Service to calculate the level of risk based on your criteria. Request automates granting access on user requests by letting you define criteria to automatically grant requested access or route approval requests to the appropriate entity. Certification policies provide compliance status of all access review processes included in a policy definition.![Might need to revise last statement. Per doc comments also need to Data Policies (Data comparison policies - shldn't this be in managing catalog)]

8 Creating and Managing Separation of Duties Policies

Separation of Duties (SoD) Administrators can create policies to enable Identity Governance as a Service to look for users and accounts holding too much access. Identity Governance as a Service creates cases when it finds violations, and policy owners review the cases and approve or resolve the violations.

Understanding Separation of Duties

When any one person in your company 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 Separation of Duties (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 as a Service 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 as a Service provides.

When you have active SoD policies, Identity Governance as a Service creates cases for any violations of the policies and lists them on the **Violations** page. The SoD Administrator or policy owners review the cases to determine whether to resolve or approve them.

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 "Understanding the Review Process" on page 70.

Creating and Editing Separation of Duties Policies

After you have published data, you can create separation of duties (SoD) policies that Identity Governance as a Service uses to alert you to possible violations. When you have active SoD policy definitions, Identity Governance as a Service 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 as a Service discover violations of the policy and create SoD violations and cases.

4 Enter the required information. For more information, see “Understanding the Separation of Duties Policy Options” on page 88.

NOTE: Policy names must be unique. When Identity Governance as a Service checks for uniqueness, case is not considered. Therefore, Identity Governance as a Service considers SoD1 and SOD1 to be equivalent.

5 (Optional) Specify one or more compensating controls and a maximum control period. Identity Governance as a Service 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 “Deciding what Occurs when the Separation of Duties Policy is Violated” on page 89.

6 (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.

7 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.

Understanding the Separation of Duties Policy Options

When you create a separation of duties (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.

- “Providing Resolution Instructions for the Separation of Duties Policies” on page 88
- “Deciding what Occurs when the Separation of Duties Policy is Violated” on page 89
- “Defining Separation of Duties Conditions” on page 89

Providing Resolution Instructions for the Separation of Duties Policies

When a violation of the SoD policy occurs, Identity Governance as a Service displays the violations on the **Policy** > **Violations** tab. Users with the proper access can access and review these violations. When you provide resolution instructions, users can see what to do in Identity Governance as a Service without having to wait for further instructions on how to solve the violations. Providing these instructions is optional.

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

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 in the **Compensating Controls** field when you create the SoD policy.

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 as a Service 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 as a Service tests orphaned accounts against the SoD policies.

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 as a Service 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 as a Service 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 is 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 as a Service does not allow an SoD policy with a single condition of this type.

NOTE: Identity Governance as a Service 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 as a Service 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 as a Service 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.

Importing Separation of Duties Policies

You can import separation of duties (SoD) policies by uploading a `json` file.

1. Under **Policy**, select **SoD**.
2. Click **Import Separation of Duties Policies**.
3. Navigate to the file, select the file to import, and click **Open**.
4. Identity Governance as a Service detects whether you are importing new or updated policies and whether the updates would create any conflicts.
5. Select how to continue based on what information is displayed.

Downloading Separation of Duties Policies

You can download separation of duties (SoD) policies in `json` format as a backup to edit offline.

1. Under **Policy**, select **SoD**.
2. Select one or more policies from the list, and click **Actions** > **Download**.
3. Select any options you want to download with each policy, and then click **Download**.
4. To import edited policies, see “Importing Separation of Duties Policies” on page 90.

9 Managing Separation of Duties Violations

Identity Governance as a Service provides the ability for you to define and activate Separation of Duties (SoD) policies so the system can look for 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 as a Service 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 as a Service creates a **changeset** for fulfillment. For more information, see “Fulfilling the Changeset for a Review Instance” on page 82.

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 as a Service can detect an 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 as a Service creates a new SoD violation record for each of those detections. 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 that users have taken with respect to the violation (approve, resolve). An SoD case is closed when Identity Governance as a Service 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.

Listing SoD Violations or SoD Cases

There are multiple places where 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 as a Service displays this tab for a user or account only 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.

Viewing SoD Case Details

After you have a list of the 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.

Understanding SoD Case Status

Identity Governance as a Service 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.

SoD Case Status	Description
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 - i.e. 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 as a Service 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.

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 “Fulfilling the Changeset for a Review Instance” on page 82.

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.

Closing an SoD Case

Identity Governance as a Service 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.

10 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.

Overview of Roles

Identity Governance as a Service enables you to manage both the technical and business roles in your organization. To enable easier management of these roles, Identity Governance as a Service assigns technical role administrators and business role administrators with separate but overlapping responsibilities.

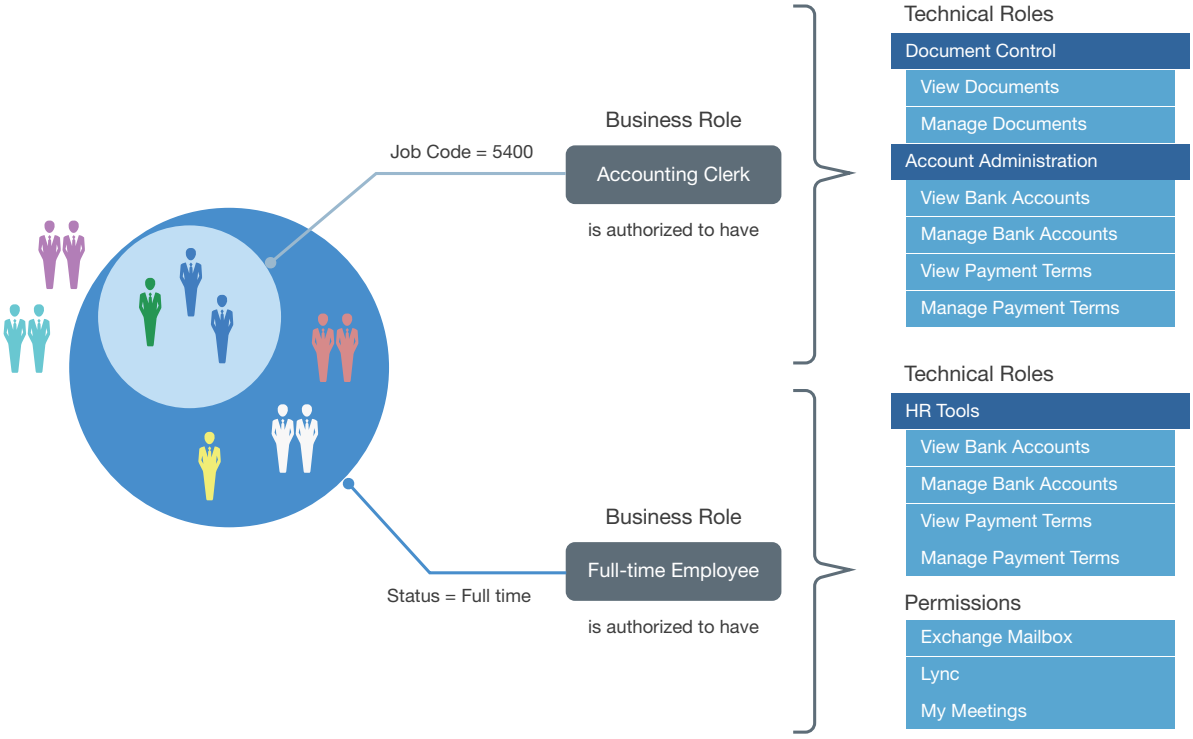
Business roles organize people by their business function and user based attributes to solve questions of what users should have access to because of who they are or what they need or might have an option to request without additional approval.

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 10-1 contains an example of how the different types of roles overlap. All full-time employees are authorized 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 has created in Identity Governance as a Service. When you include a user as a member of a business role of Full-time Employee and Accounting Clerk, Identity Governance as a Service authorizes the user to have any of the mandatory or optional technical roles or permissions listed for the given role. Mandatory permissions could potentially be automatically provisioned, while optional permissions could be assigned 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 34.

Figure 10-1 *Detailed Example of the Overlap between Business Roles and Technical Roles*

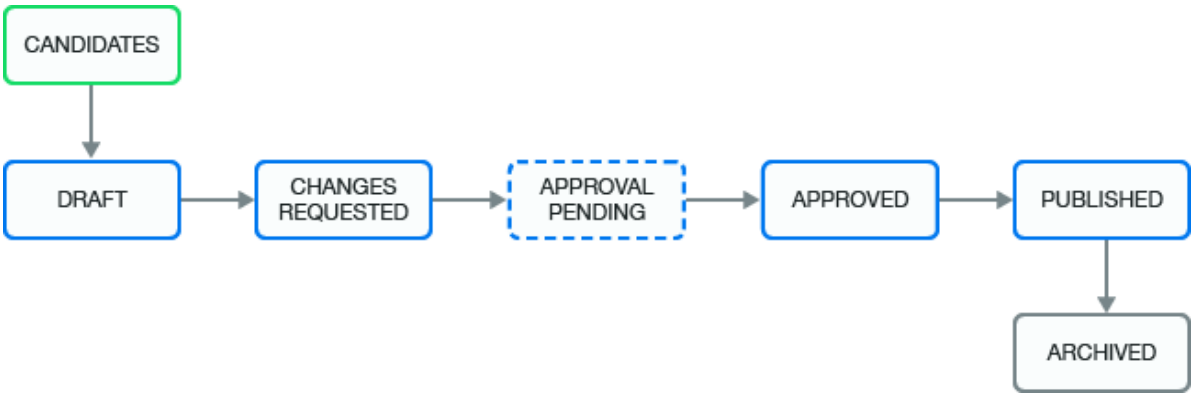


NOTE: This chapter primarily discusses business role policy concepts and procedures. For information about technical roles, see "Managing Technical Roles" on page 185

Understanding Business Role States

There are several states in the life cycle of a business role after they are created, either manually or mined. From beginning to end, the business role goes through the states in Figure 10-2 on page 96. For a detailed description of the states, refer to the following table.

Figure 10-2 *Business Role States*



Business Role State	Description
CANDIDATES	Business role was created by the mining process and must be promoted before it can be approved or published (depending on the approval policy). This state corresponds to the internal state called MINED.
DRAFT	The assigned approval policy requires approval and changes to the business role have not been submitted for approval.
CHANGES REQUESTED	Approval of a business role was denied. This state corresponds to the internal state called REJECTED.
APPROVAL PENDING	Pending changes are ready for approval by the user specified in the approval policy. This state corresponds to the internal state called PENDING_APPROVAL.
APPROVED	Business role is approved but has not yet been published.
PUBLISHED	Business role is approved and has been published.
ARCHIVED	Policy has been deleted or a new version has been created. It is archived for history and reporting. Archived business roles are never displayed in the application.

Understanding Business Role Mining

Identity Governance as a Service 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 or technical role candidate is called Role Mining or Role Discovery. 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 as a Service 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 will display a list of items consisting of department name with 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 width of the attribute circle displays the recommendation strength, and the width and darkness of the lines indicate the affinity of the attribute to other user attributes. Administrators can customize the mining results by modifying the default maximum number of results, minimum potential members, and number of automatic recommendations.

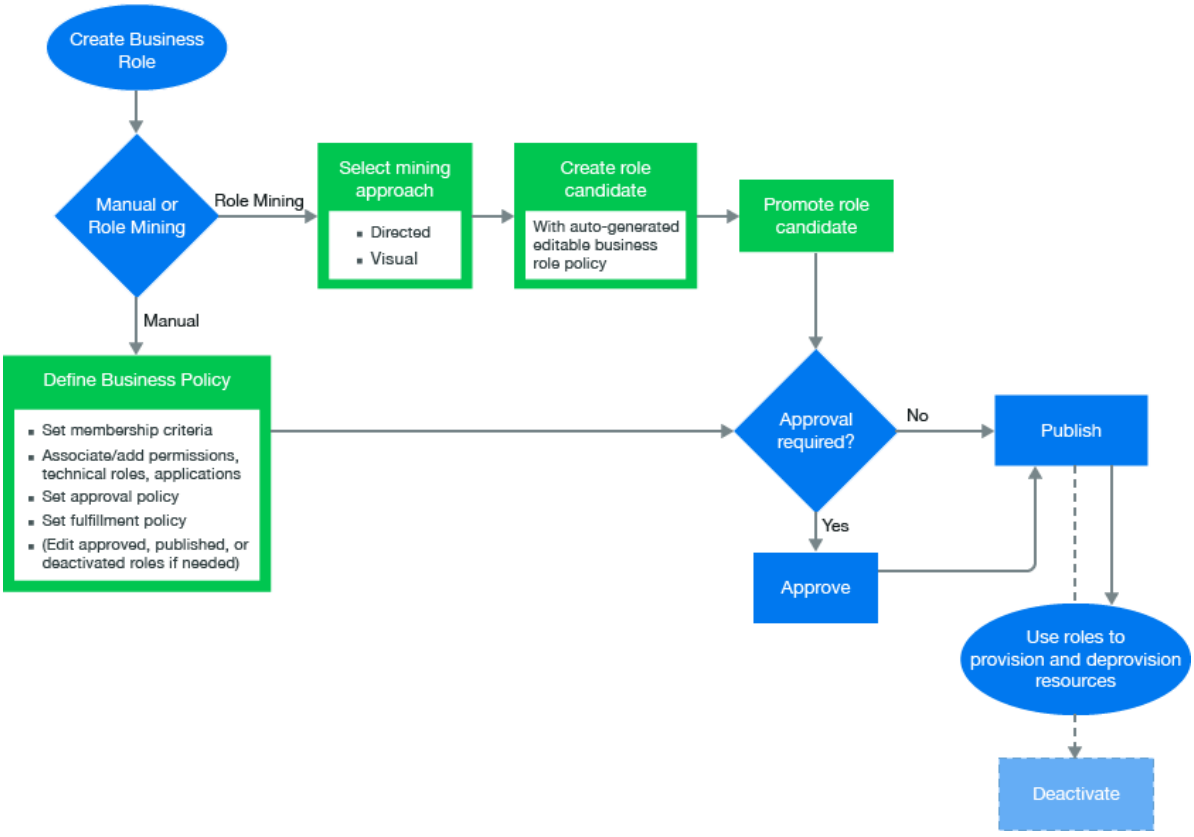
NOTE: To optimize search results, administrators can modify default role mining settings in **Administration > Analytics and Role Mining Settings**. For more information, see “Configuring Analytics and Role Mining Settings” on page 32.

After previewing users and their associated permissions, technical roles, and applications, administrators can select one or more items from the list to either create role candidates for each selected item in the list or a single candidate for all of them. Additionally, common permissions can be grouped under a technical role, and technical role candidates could be generated for each application.

NOTE: Mined business or technical roles are created in a candidate state. Administrators can edit and save role candidates, but candidates must be promoted before they can be approved or published as a role. Administrators can also select multiple role candidates and submit for approval, publish, or delete using the **Actions** options.

Managing Business Roles

Figure 10-3 *Business Role Workflow*



Business Role Management is the process of creating, modifying, and defining business roles and managing business role policy.

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. You add a business role authorization policy when you create or edit the business role.

A business role administrator performs all administrative functions for all business roles. A business role administrator can delegate administrative privileges. For more information, see “Runtime Authorizations” on page 57.

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 using role mining analytics.

To define a business role:

1. Log in to Identity Governance as a Service as a business role administrator or a global administrator.
2. Select **Policy** > **Business Roles**.
3. Select the **Mining** tab if you want the system to recommend role candidates and based on your selection auto-create a membership expression and authorize associated permissions, technical roles, and applications.

   NOTE: If you are confident about your data and want to define a 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 **Settings** gear icon to modify the maximum number of results to display for each recommended attribute, and the minimum number of members for each role candidate. ◆ Click an attribute node/circle to select a role candidate.

If	Then
You want to direct the mining by specifying a user attribute	◆ Select **Directed Role Mining**. ◆ Specify user attributes by entering user attribute names or by clicking search and selecting attributes based on the strength of the recommendation. ◆ Specify the 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.![too much detail or too little?] **NOTE:** The permission, technical role, and application coverage fields are used 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 it to be added as an authorization in the candidate. If it is 100%, then all members must hold the permission for it to be added. ◆ Save the specified values to trigger user catalog analysis. ◆ (Optional) Click the **Settings** gear icon to adjust the settings, and save to refresh the candidate suggestions.

4 Select one or more items from the **Directed Role Mining > Mining Results** list or the **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, enter **Name**.

7 (Optional) Select **Create associated technical for common permissions** to generate 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 Click the **Role** tab and click the newly generated inactive role to view the role description.

10 Click **Edit**.

NOTE: Role candidates are created in pending state and must be promoted before they can be approved or published.

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 is the number of days a user is still considered to be a member of the role when it is detected that they no longer meet 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, only published roles membership will be included and duplicates will be eliminated. For example, you can include role A and role B in the membership of role C. Role C will then be 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, but User1 is excluded by role C, the user will be excluded.

Membership expressions

Membership expressions are criteria that specify a set of users that are considered members of the business role and are auto-generated when you mine for roles. Each expression can have an authorization period for when it is valid. Optionally, add one or more expressions to search for users.

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 the Sales group is included and the Contractors group is excluded. A user who belongs to both of those groups would be excluded from the business role, because exclusion takes precedence over inclusion.

---

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

Permissions

Permissions may be preauthorized when you mine for roles or you may 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 the permission should be automatically granted and/or revoked, or manually fulfilled. If needed, click on the calendar control to set an authorization period for when these permissions are authorized for users in the business role.

Technical Role

Technical roles may be preauthorized when you mine for roles or you may 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 the technical role authorization should be automatically granted and/or revoked, or manually fulfilled. If needed, click on the calendar control to set an authorization period for when the permissions in the technical role are valid for the business role.

Applications

Applications may be preauthorized when you mine for roles or you may need to define them. If needed, define which applications the members of the business role are authorized to hold. This means accounts can be created 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 the application authorization should be automatically granted and/or revoked, or manually fulfilled. If needed, click on the calendar control to set an authorization period for when the members of the business role have access to the application using the calendar control.

NOTE: Auto-grant and auto-revoke requests will be automatically fulfilled if automatic fulfillment has been enabled on the **Owners and Administration** tab and when fulfillment targets have been configured. For information about automatic fulfillment, see "Automatically Fulfilling the Changeset" on page 83.

For more information about authorizing permissions, technical roles, and applications, see "Adding Authorizations to a Business Role" on page 103.

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

- Role owner
- Role manager
- Fulfiller
- Categories
- Approval Policy
- Automatic Fulfillment
- Auto revoke period

Identity Governance as a Service 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.

Select whether you want this role to be automatically fulfilled. When selected, Identity Governance as a Service automatically sends fulfillment requests to provision and revoke mandatory resources for users.

Set the number of days to wait after a user loses authorization for a resource before revoking the access.

15 Estimate what would change if the business role was published and analyze SoD violations and edit the business role definition as required.

16 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 "Adding a Business Role Approval Policy" on page 104.

To have the business role used in reviews or used in the catalog to detect users that meet the business role criteria, you must publish the business role. For more information, see “Publishing or Deactivating Business Roles” on page 105.

Authorizing User Access Through Business Roles

Membership policy determines which users are members of a business role. Membership policy can include membership expressions, user or group inclusion lists, and user or group exclusion lists. Regardless of whether a user is a member of role by virtue of matching a membership expression or because they are explicitly included, they are authorized resources of a business role for as long as they are a member of the business role.

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 whether the user is authorized the access.

A business role can authorize technical roles. This means that users and groups that you add to the business role are authorized all of the permissions included in each technical role. For more information, see “Managing Technical Roles” on page 185.

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

A user in the business role can be authorized to have all the permissions included in the authorization policy.

Authorized Technical Roles

A user in the business role can be authorized for technical roles included in the authorization policy.

Authorized Applications

A user in the business role can be authorized to have an account in all of the applications included in the authorization policy.

Mandatory and Optional Entitlements

Mandatory entitlements include permissions, technical roles, and applications that users are expected to have if they are assigned the business role. Optional entitlements are permissions, technical roles, or applications that users are allowed to have but are not required to have.

Automatic Fulfillment Settings

If you selected **Automatic Fulfillment** on the **Owners and Administration** tab, you can select whether to automatically grant and revoke each permission, technical role, and application. Applications must have an account collector to allow you to specify automatic grant or revoke.

Authorization Period

A user in the business role can be authorized for a set period of time defined in the authorization policy. Typically you may need to set an authorization period only during transitions like mergers or changes related to compliance. Avoid setting an authorization period for business roles to change a specific role authorization, as it can be more efficiently handled using periodic business role membership reviews.

Adding a Business Role Approval Policy

The approval policy for the business role governs all business role life cycle events. Identity Governance as a Service contains a default approval policy that is assigned 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 approval is required when creating or modifying that business role.

NetIQ recommends that your organization's default policy require approval. A default policy that does not require approval could result in roles being approved automatically when they are created. 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.

The default business role approval policy, which does not require approval, is applied 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.

Two additional policies are provided for your convenience. One requires approval by the business owner (recommended) and another one 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 business role 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 Service as a business role administrator or a global administrator.
2. Select **Policy** > **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. Select **Save** to save the policy.

You can change the approval policy for a group of business roles at one 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.

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 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 as a Service creates a draft of the business role that appears on the **Draft** tab that you can send for approval if required, publish, or discard. However, deactivated roles are not available for the governance process or in the general catalog.

The edit and approve cycle is a single cycle that is independent of the publication cycle. When you edit the published business role, Identity Governance as a Service creates a draft version of the business role.

The approval cycle is not independent of the draft. If no approval is required, the draft is automatically approved but not published. If the draft is then published, it replaces the currently published version.

When the business role administrator deactivates a published role, three things can occur:

1. If there is an approved draft, Identity Governance as a Service 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 as a Service 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 as a Service moves the published business role to the approval state.

When a business role is deactivated, the role cannot take part in the review process. The role must be published to be part of the review process. For more information, see “Understanding the Review Process” on page 17.

To publish or deactivate a business role:

1. Log in to Identity Governance as a Service as a business role administrator or a global administrator.
2. Select **Policy** > **Business Roles**.
3. Select the business role to change, then select **Edit**.
4. If you have one version of the business role, select **Publish** or **Deactivate** the business role.

   NOTE: Deactivating disables the role from being a part of the review process but does not automatically revoke all permissions. Permissions are revoked only if a user is no longer a member of the business role.

   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 a number of business roles that need to be published, Identity Governance as a Service 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**.

Analyzing Business Roles

Identity Governance as a Service 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, a business role might be created that has all or almost all of the members as another role or a Technical Role might have the same permissions as another 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 to 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![add how is this different from similarity]
- Members without mandatory authorizations
- Members without auto-grant authorizations

To analyze business roles:

1. Log in to Identity Governance as a Service as a business role administrator or a global administrator.
2. Select **Policy** > **Business Roles**.
3. Select the **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%, the results will display business roles that have 60% of similarity for any authorization or membership.

   NOTE: **Business role similarity** and **Common authorizations** analysis can be performed on published or unpublished business roles, while **Authorization effectiveness**, **Mandatory authorizations**, and **Auto-grant authorization** analysis are performed 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 they will be highlighted, and skipped 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.

Editing Business Roles

Identity Governance as a Service 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 Service as a business role administrator or a global administrator.
2. Select **Policy** > **Business Roles**.
3. Select the business role you want to edit, then select **Edit**.
4. (Conditional) If the business role is published, on the top of the page, select **Edit**.

   ![EAN: Isn't step 3 the same as step 4?]

   Identity Governance as a Service creates a draft of the business role for you to edit on the **Draft** tab.
5. Make the appropriate changes to the business role.

   You can change the name, description, grace period, risk level, memberships, authorizations, and 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 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, the business role is archived for reporting and auditing purposes.

Approving Business Roles

Identity Governance as a Service 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 owner can approve the business role if the role's approval policy specifies **Business role owners**. However, you can 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 Service as a user assigned to approve the business role.
2. Select **Policy > Business Roles**.
3. Select the **Pending Your Approval** tab.
4. Select any of the pending approvals, then read and review the content of the business role.
5. Enter 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 changes to be made.

When you select the **Request changes** option, the creator of the business role receives notification of the change request. After you change the business role, the approval workflow process starts again.

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. The business role must allow automatic fulfillment on the **Owners and Administration** tab. For more information, see "Defining Business Roles" on page 99. In addition, you must configure individual authorized resources to allow automatic granting or revoking of the resource.

Automatic Provisioning Requests

Identity Governance as a Service evaluates whether the system needs to request automatic provisioning of an authorized resource when any of the following events occur:

- A user has become a member of a business role
- A business role is modified to authorize a resource and republished
- A business role resource enters its validity period

Identity Governance as a Service detects changes in business role membership when you publish identities, applications, and business roles. In addition, it periodically runs a task to check if authorized resources have entered their validity period.

When Identity Governance as a Service determines that a user has become authorized to have a resource for any of the above reasons, it issues a provisioning request for the user + resource if:

- The resource authorization specifies automatic granting.
- The user does not already have the resource.

  NOTE: For applications, this means that the user does not currently have an account in the application.

- There is no pending automatic change request for the resource to be granted to the user.

  NOTE: A change request is considered pending until it is verified or fails verification for some reason.

Automatic Deprovisioning Requests

Identity Governance as a Service evaluates whether the system needs to request automatic deprovisioning of a resource when any of the following events occur:

- A user is no longer a member of a business role
- A business role is modified to no longer authorize a resource and is republished
- A business role is deactivated
- A business role is deleted
- A business role resource authorization exits its validity period

Identity Governance as a Service detects changes in business role membership when you publish identities, applications, and business roles. It also periodically runs a task to check if authorized resources have exited their validity period.

The decision whether to issue a deprovisioning request deliberately has more controls than the decision whether to issue a provisioning request. The extra level of control is intended to prevent mistakes that could lead to accidental and unintended deprovisioning of critical resources for users. When the system detects that a business role no longer authorizes a resource for a particular user for any of the above reasons, it will do the following to determine if it should issue a deprovisioning request for the user and resource:

- Determine if the user currently has the resource. If not, a deprovisioning request is not needed. For applications, a user has the resource if they have an account in the application.
- Determine if there is a pending automatic deprovisioning request for the user and resource. If so, no new deprovisioning request will be issued. A change request is considered pending until it is verified or fails verification for some reason.
- Determine if any other business roles currently authorize the resource for the user. If so, no deprovisioning request will be issued. Identity Governance as a Service does not issue automatic deprovisioning requests until the user has lost ALL of its authorizations for a resource. Other business roles might authorize the resource for various other users, but if none of the business roles authorize the resource for the user in question, they are not considered.

When Identity Governance as a Service determines that the user has lost its last authorization for a resource, it creates a list of business roles to consult to determine if a deprovisioning request should be issued. The system adds a business role to this list if it meets ALL of the following conditions:

- Must have authorized the resource for the user at one time. There may be business roles that currently authorize or have previously authorized the resource for other users, but if they have never authorized it for the specific user in question, they are not relevant here.
- Must have authorized the resource for the user in the not too distant past. If the user lost its authorization for the resource from a business role too long ago, we do not want to consider the business role. The auto-revoke period that might be specified for the business role defines what period of time is too long ago. For more information, see “Defining Business Roles” on page 99. The auto-revoke period is defined on the **Owners and Administration** tab.
- Must be currently published, not deactivated or deleted. Deactivated or deleted business roles are not relevant here.
- Must have a current authorization for the resource in question. Business roles that authorized the resource in the past but no longer authorize it are not relevant here.
- Resource must be in the validity period specified by that authorization. Business roles that may have authorized the resource in the past but no longer do are not relevant here.

To issue a deprovisioning request, one or more business roles that meet ALL of these conditions must exist, and they must ALL currently specify automatic revoking for the resource in question. Otherwise, no deprovisioning request will be issued.

11 Calculating and Customizing Risk

Identity Governance as a Service allows custom definition of risk based on your policies and risk tolerance. Customized risk ranges and levels allow Identity Governance as a Service 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 6, “Creating and Modifying Review Definitions,” on page 69.

Understanding Risk Levels and Risk Scoring

Identity Governance as a Service 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 company 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 as a Service 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 as a Service environment:

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

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

Risk Levels

Identity Governance as a Service 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 as a Service 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.

Risk Scoring

A risk score quantifies the level of risk to which an entity, such as a user or account, exposes an organization. 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 as a Service 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. 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 a user risk score has a maximum value of 1000 and 3 risk factors of equal weight. Each risk factor can account for only one-third of the user's risk score.

For some risk factors, Identity Governance as a Service 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 as a Service then looks at the range you have specified. If the value of the risk factor is at or above the high range, Identity Governance as a Service applies the full weight for that risk factor to the risk score. If the value is below the high range, Identity Governance as a Service 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 configure Identity Governance as a Service 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.

Visualizing Risk

Identity Governance as a Service 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 as a Service has assessed the risk:

- As a separate tab on the **User** and **Application** details pages
- As a governance risk score displayed on the **Overview** page
- As a governance risk score and context information on the **Risk** policy administration page

Identity Governance as a Service assigns a color code to each risk level ranging from blue at the low end to red at the high end. These colors appear with risk scores to help you further understand how the score fits into your customized risk level ranges.

Configuring Risk Levels

Identity Governance as a Service 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 as a Service 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 as a Service creates four equally-sized risk levels of 0-25, 26-50, 51-75, and 76-100.

To configure risk levels:

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 as a Service 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.

Configuring Risk Scores

You can customize the way Identity Governance as a Service 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. Identity Governance as a Service uses edited values for extended attributes for risk calculation instead of collected values. For more information, see “Editing Attribute Values on Objects in the Catalog” on page 181.

To have Identity Governance as a Service 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 as a Service 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 as a Service use that factor in the risk score calculation. For more information, see “Creating and Editing Certification Policies” on page 123.

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 as a Service 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 the user risk score.

6. For each risk factor that you want to use, enter the weight for that risk factor and customize the range values that 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.
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 as a Service 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.

Setting and Viewing Risk Calculation Schedules and Status

You can set a regular schedule for Identity Governance as a Service 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 the 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 as a Service to calculate risk in your environment, such as start and end date and time details and whether to repeat on a regular schedule.

Viewing Calculated Risk Scores

After you configure Identity Governance as a Service to calculate risk scores, you can view risk scores of items in the catalog and your overall governance risk score on the **Overview** page.

1 Log in as a Global or Data Administrator.

2 (Conditional) If you have configured Identity Governance as a Service to calculate the Governance risk score, view the Governance risk score for your organization on the **Overview** page.

3 (Optional) Select the score to display the risk factors and other details of how Identity Governance as a Service 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 on the right side of the window.

6 Select **Risk Factors** to display the details for how Identity Governance as a Service calculated the risk score.

12 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.

For more information about using the Access Request interface, see Chapter 24, “Instructions for Access Requesters and Approvers,” on page 209.

Understanding Access Request

The Access Request interface allows users to monitor and request access for items that are available in their organization. The Identity Governance as a Service 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 Access Profiles to request a group of permissions in a single step
- Retract an access request
- Retry a failed request after fixing the cause of the error
- Compare access of multiple users
- Approve requests
- 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 that 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.

Configuring Access Request

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

- Business roles
- Technical roles
- Request policies
- Request approval policies
- Request policies assigned to resources and roles

If you are using business roles in your organization, you can configure Access Request to show users recommended access. If you want to show recommended access to users and do not have any business roles, create business roles first. For more information, see Chapter 10, “Creating and Managing Business Roles,” on page 95.

If you are using technical roles in your organization, you can provide groups of permissions, or Access Profiles, that users can request in a single step. To provide Access Profiles in Access Request, create technical roles to group the permissions. For more information, see “Managing Technical Roles” on page 185.

Request policies define what access can be shown and requested in the Access Request interface. Request approval policies define the approvals needed when users request access. For more information, see the following sections:

- “Creating Request Policies” on page 118
- “Creating Request Approval Policies” on page 119
- “Assigning Resources to Request and Approval Policies” on page 119

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.

To create request policies:

1. In Identity Governance as a Service, select **Policy > Access Request**.
2. On the **Request Policies** tab, select **+** to create a new policy.
3. Name the policy.
4. Select what types of users **All Users** are allowed to make requests for. 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 the ability to request for **All Users** automatically includes the ability to request for **Self**, **Direct Reports**, and **Downline Reports**![Not sure if this happens. Need to chk again.] . Granting the ability to request for **Downline Reports** automatically includes 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 request for **Self** ability to specific users or groups.

   ---

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

Creating Request Approval Policies

To set appropriate approvals for requested access, you must create request approval policies. Identity Governance as a Service 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 as a Service, 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 43.
   - View notification emails, and optionally set reminder email frequency and add recipients
   - Set an escalation period and specify escalation approvers
   - Set an expiration period and assign a default action at the end of the expiration period
5. Save the policy.

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 as a Service, select either the applications, permissions, or roles catalog.
2. Select the applications, permissions, or roles to which you want to apply request policies.
3. In **Actions**, select the option you want. You can:
   - Assign an access request policy
   - Remove an access request policy
   - Assign an 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 be removed from the default approval policy only 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.

Assigning Request to Identity Governance as a Service Users

The method for giving Identity Governance as a Service 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 the 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 (**Administration > 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 43.	
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 as a Service **Fulfillment > Configuration.** For information about configuring fulfillment targets, see “Configuring Fulfillment” on page 23.	Global Administrator or Request Administrator
Manage who can request on behalf of others	Requesters tab in the 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 as a Service **Administration > Role Mining and Analytics Settings**. For information about configuring similarity profile settings, see "Configuring Analytics and Role Mining Settings" on page 32.	Global Administrator or Request Administrator

Disabling the Access Request Service

![EAN: Updated this section for IGaaS - removed config utility procedure.]

You can prevent the Access Request pages from appearing in Identity Governance as a Service by having the Access Request service disabled. For assistance with disabling the Access Request service, contact NetIQ Customer Support. When the service is disabled:

- All Access Request options are removed from navigation
- Users with no rights in Identity Governance as a Service 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 policies. Users will still be able to administer and view policies.

13 Creating and Managing Certification Policies

![New chapter. This feature has only been partially implemented. This chapter will need to be updated for 3.01 patch release.] Certification policies allow you to produce a comprehensive view of your organization's compliance with specific certification controls, such as the Sarbanes-Oxley Act (SOX) or the Health Insurance Portability and Accountability Act (HIPAA). A global, review, or data administrator creates certification policies against review definitions and Identity Governance as a Service evaluates the review items and other criteria defined in the policy and reports violations. From the **Overview** or **Certification Policies** page, you can drill down to see specific violations to policies when they exist.

Understanding Certification Policies

Identity Governance as a Service 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 that includes 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, or permissions. 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
- 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

Creating and Editing Certification Policies

NOTE: Reviews should be defined before creating a certification policy. For information about review definitions, see Chapter 6, "Creating and Modifying Review Definitions," on page 69.

After creating review definitions, create certification policies that Identity Governance as a Service can use to alert you to 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 Enter a name, validity period in days, months, or year, and single or multiple review definitions.

NOTE: Policy names must be unique. When Identity Governance as a Service checks for uniqueness, case is not considered. Therefore, Identity Governance as a Service considers Hippa and HIPPA to be equivalent.

TIP: Use wildcard * to search for reviews, or just start typing the review name to view suggestions.

---

5 (Optional) Set risk.

6 (Optional) Specify a policy administrator.

NOTE: The policy administrator role is not currently functional, but will be functional in the next release of Identity Governance as a Service. Currently, a global, review, or data administrator can function as a policy administrator.

![EAN: If the policy administrator role isn't functional yet, we really shouldn't talk about it. There's no guarantee that it will be functional in the next IG release.]

---

7 Save your settings.

8 Under **Policy**, select **Certification** to view the newly created policy listed with the number of violations.

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

10 (Optional) Select a specific policy or multiple policies, then select **Actions > Delete** to delete policies.

Scheduling and Calculating Certification Policy Violations

![EAN: I think this heading needs to be changed. I don't think you actually schedule certification policy violations.]

![Bug 1061533; in 3.01 schedule will be added and validity period expiration may not be an issue]
Policy violations are automatically calculated when a certification policy is modified, when 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 will occur. However, after the validity period of a policy, you will need to manually calculate policy violations.

![EAN: Is there a word missing in the following sentence: "In addition, you can also schedule when certification policy will occur."? This doesn't make sense to me.]

NOTE: If configured, certification policy violations related risk factors impact Identity Governance as a Service risk scores. Therefore, calculate certification policy violations before calculating risk scores. For information about risk scoring, see Chapter 11, "Calculating and Customizing Risk," on page 111.![EAN: "certification policy violations related risk factors"?? Is there a word missing here?]

To schedule certification policy calculation:

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

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

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

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

To manually calculate policy violations:

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

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

3 On 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, the certification status is defined based on the last review. All calculations can be canceled when in progress by selecting **Cancel** next to the progress status.

Managing Certification Policy Violations

Identity Governance as a Service provides the ability for you to define certification policies so that the system can look for violations to the policies. You can view these violations from the **Overview** page or the **Certification** page.

Selecting the number of violations opens a panel of violations listed by users, accounts, and permissions. On each tab, you can search for the related entity or for a specific violation type for each user, account, or permissions. Types of violations include review items with no decision (No Decision), review items that are past their scheduled review period (Overdue), and review items that are past their scheduled review period and do not have any decision (Overdue with No Decision).

Certification policy violations can be resolved by running the related reviews. Once the review is completed, the number of violations is recalculated automatically. For more information about running a review, see Chapter 7, “Running a Review Instance,” on page 81.

14 Creating and Managing Delegation

![EAN: I think this heading should be changed to Creating Delegates and Managing Delegation. You can create delegates, but you can't really create delegation. Leaving for now ....]

Delegation enables you to assign delegates for users to enable a more consistent workflow for managing the reassignment of user tasks. A global, data, or review administrator assigns a 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 (that is, review owner, escalation reviewer, or auditor), the delegate will have the proper access permissions to act in that role.

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, and 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 as a Service 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 as a Service 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.

Assigning and Managing Delegates

1. Log in as a **Global Administrator**, **Data Administrator**, or **Review 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: The review owner and review administrator can bypass delegation for the review management roles (that is, review owner, escalation reviewer, and auditor) by editing the running review instance. These changes are made only for the running review instance. Delegates also can assign another user as a reviewer by using the **Change Reviewer** option on review tabs.

---

15 Creating and Managing Data Policies

Data policies can help you prove to auditors and internal risk partners that the data collected and published into the Identity Governance as a Service 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 as a Service uses the defined data policies to produce the comparison details. For more information, see “Comparing Collections and Publications” on page 151.

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

![[EAN: The procedure below was a Sect1, but since it was the only one under the chapter heading and wasn’t unique anyway (Creating and Editing Data Policies), I removed the Sect1 and heading tags for IGaaS. Also edited and restructured several steps that weren’t written to our standard.]

To create and edit data policies:

1. Log in as a Global Administrator or a Data Administrator.
2. Under **Data Administration**, select **Data Policy**.
3. To create a new policy:
   - **3a** Navigate to the appropriate tab and select **+**.
   - **3b** Select the desired elements for the policy and enter criteria.
   - **3c** Save your settings.
4. (Optional) To edit a policy, select the policy, then select **Edit**.
5. (Optional) To delete a policy, select the policy, then click the trashcan icon.

IV Part Title Managing the Entity Identity Governance as a Service / Entity Catalog / Title

PartIntro Para The Entity Identity Governance as a Service / Entity 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. / Para

- SubToc ItemizedList ListItem Para XRefInt Chapter 16, “Creating and Managing Data Sources,” on page 133 / XRefInt / Para / ListItem
- ListItem Para XRefInt Chapter 17, “Creating and Monitoring Scheduled Collections,” on page 155 / XRefInt / Para / ListItem
- ListItem Para XRefInt Chapter 18, “Integrating Collected Data with Identity Manager,” on page 159 / XRefInt / Para / ListItem
- ListItem Para XRefInt Chapter 19, “Publishing the Collected Data,” on page 171 / XRefInt / Para / ListItem
- ListItem Para XRefInt Chapter 20, “Managing Data in the Catalog,” on page 175 / XRefInt / Para / ListItem
- ListItem Para XRefInt Chapter 21, “Grooming the Identity Governance as a Service Databases,” on page 193 / XRefInt / Para / ListItem / ItemizedList / SubToc

Para To manage the Entity Identity Governance as a Service / Entity catalog, you must have a Data Administrator, Global Administrator, or bootstrap administrator authorization. / Para / PartIntro

16 Chapter Title Creating and Managing Data Sources / Title

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

Para Entity Identity Governance as a Service / Entity must collect information about users from identity sources. After Entity Identity Governance as a Service / Entity 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 XRefInt "Adding Identity Governance as a Service Users" on page 60 / XRefInt . / Para

- SubToc ItemizedList ListItem Para XRefInt "Understanding Collector Configuration" on page 133 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Transforming Data During Collection" on page 144 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Creating Identity and Application Sources" on page 145 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Managing Identity and Application Sources" on page 150 / XRefInt / Para / ListItem / ItemizedList / SubToc

Para For more information about data sources, see XRefInt "Understanding Data Sources" on page 14 / XRefInt . / Para

Sect1 Title Understanding Collector Configuration / Title

Para When you create an identity or application source, you also create the Strong **collectors** / Strong 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 − Entity Identity Governance as a Service / Entity catalog. / Para

− Para When you configure the collector, you designate the incoming attributes that you want to map to the attributes in the − Entity Identity Governance as a Service / Entity 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 − GUIMenu **multivalue** / GUIMenu 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. / Para

- − SubToc − ItemizedList − ListItem − Para − XRefInt "Understanding the Common Elements in a Collector" on page 134 / XRefInt / Para / ListItem
- − ListItem − Para − XRefInt "Understanding Collector Templates for Identity Sources" on page 136 / XRefInt / Para / ListItem
- − ListItem − Para − XRefInt "Understanding Collector Templates for Application Sources" on page 137 / XRefInt / Para / ListItem
- − ListItem − Para − XRefInt "Understanding the Variations for Data Sources" on page 140 / XRefInt / Para / ListItem / ItemizedList / SubToc

− Sect2 − Title Understanding the Common Elements in a Collector / Title

− IntroPara Every collector has the following configurable elements: / IntroPara

− VariableList − VarListEntry − Term **Collector template** / Term

− ListItem − IntroPara 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 − GUIMenu **AD Identity** / GUIMenu to collect identities from Active Directory. The templates support the following types of data sources: / IntroPara

- − ItemizedList − ListItem − IntroPara Active Directory / IntroPara / ListItem
- − ListItem − IntroPara Azure Active Directory / IntroPara / ListItem
- − ListItem − Para CSV file / Para / ListItem
- − ListItem − Para eDirectory / Para / ListItem
- − ListItem − Para Google Apps / Para / ListItem
- − ListItem − Para Identity Manager / Para / ListItem
- − ListItem − Para JDBC, such as Oracle or PostgreSQL / Para / ListItem

- ListItem Para Resource Access Control Facility (RACF) / Para / ListItem
- ListItem Para Salesforce.com / Para / ListItem
- ListItem Para SAP User Management / Para / ListItem
- ListItem Para ServiceNow / Para / ListItem
- ListItem Para SharePoint 2013 Server / Para / ListItem / ItemizedList

---

Note **NOTE:** Para Template names ending in GUIMenu **with changes** / GUIMenu can be enabled for incremental change events processing. / Para / Note

---

Para To see all the data source types, select GUIMenu **Collector Template** / GUIMenu when you create the data source. To collect data from a JDBC or SAP User Management source, Entity Identity Governance as a Service / Entity needs the appropriate third-party connector libraries to be installed on the Entity Identity Governance as a Service / Entity server. If you have any questions or concerns about the appropriate libraries being installed, contact NetIQ Customer Support. / Para

Para You can also customize an existing template or create your own. For more information, see XRefInt "Customizing the Collector Templates for Data Sources" on page 42 / XRefInt . / Para / ListItem / VarListEntry

VarListEntry Term **Service Parameters** / Term

ListItem Para 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 GUIMenu **Test connection** / GUIMenu button to verify the settings. / Para

Para Select GUIMenu **Test connection** / GUIMenu to verify the settings. / Para / ListItem / VarListEntry

VarListEntry Term **Test Collection and Troubleshooting** / Term

ListItem Para 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. / Para / ListItem / VarListEntry / VariableList / Sect2

Understanding Collector Templates for Identity Sources

Identity sources provide core identity information to Identity Governance as a Service. 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 as a Service 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 as a Service 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 as a Service 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.

VarListEntry Term **Collect Group** / Term

ListItem Para An identity in the catalog can have attributes for one or more organizational groups. 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. / Para

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

VarListEntry Term **Collect Group to User Membership** / Term

ListItem Para 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. / Para / ListItem / VarListEntry

VarListEntry Term **Collect Parent Group to Child Group Relationships** / Term

ListItem Para 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. / Para / ListItem / VarListEntry / VariableList / Sect2

Sect2 Title Understanding Collector Templates for Application Sources / Title

Para 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

Entity Identity Governance as a Service / Entity identities and to join application permissions to either Entity Identity Governance as a Service / Entity identities or to the application accounts as needed. / Para

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

VariableList VarListEntry Term **Collect Account** / Term

ListItem Para 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 Entity Identity Governance as a Service / Entity is similar to an association in Identity Manager. / Para / ListItem / VarListEntry

VarListEntry Term **Collect Permission** / Term

ListItem Para Permissions can describe any of the following: / Para

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

Para A permission in Entity Identity Governance as a Service / Entity is similar to an entitlement in Identity Manager. / Para

---

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

---

VarListEntry Term **Permission and Holders Mapping** / Term

ListItem Para (Optional) These views exist to allow you to specify how a permission will be joined to either an Entity Identity Governance as a Service / Entity 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, − Entity Identity Governance as a Service / Entity provides two optional views: / Para

- − ItemizedList − ListItem − Para − Strong **Permission to Holder Mapping** / Strong 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. / Para

  − Para When Mapping permissions to holders in any application where it exists, you must use − GUIMenu **Account ID from Source** / GUIMenu not − GUIMenu **User ID from Source** / GUIMenu if you want the permission to be linked to the user (which is the usual expectation). / Para / ListItem
- − ListItem − Para − Strong **Holder to Permissions Mapping** / Strong 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. / Para / ListItem / ItemizedList

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

− VarListEntry − Term **Collect Provisioning Applications** / Term

− ListItem − Para − Emphasis *Applies only to Identity Manager data sources* / Emphasis / Para / ListItem / VarListEntry

− VarListEntry − Term **Collect Connected Accounts** / Term

− ListItem − Para − Emphasis *Applies only to Identity Manager data sources* / Emphasis / Para / ListItem / VarListEntry

VarListEntry Term **Collect Permissions hierarchy** / Term

ListItem Para (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: / Para

- ItemizedList ListItem Para Strong **Child to parent** / Strong where the collected permissions include an attribute that points to child permissions / Para / ListItem
- ListItem Para Strong **Parent to child** / Strong where the collected permissions include an attribute that points to a parent permission, such as eDirectory user / Para / ListItem / ItemizedList / ListItem / VarListEntry / VariableList / Sect2

Sect2 Title Understanding the Variations for Data Sources / Title

IntroPara In Entity Identity Governance as a Service / Entity, 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 Entity Identity Governance as a Service / Entity. Also, some identity sources might be configured to generate incremental change events. / IntroPara

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

- SubToc ItemizedList ListItem Para XRefInt “Collecting from Active Directory with Azure Active Directory” on page 141 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Collecting from a CSV File” on page 141 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Collecting from Google Apps” on page 142 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Collecting from Identity Sources with Change Events” on page 142 / XRefInt / Para / ListItem / ItemizedList / SubToc

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`.

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 as a Service 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.

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 as a Service 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 as a Service 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 as a Service translates the organizational units into Identity Governance as a Service -style groups. In Identity Governance as a Service , 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 as a Service 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:

Remark ![EAN: Updated the first bullet for IGaaS (removed content relating to the Identity Source Migration Utility, since customers on IGaaS 1.0 won't be migrating from anything).]

- An identity source is configured as an identity event source by having created an identity source from a suitable template. For more information, see “Creating Identity and Application Sources” on page 145 .
- 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.

- ListItem Para Identity event source collection, identity publication, or application publication is not in progress. / Para / ListItem
- ListItem Para (Conditional) For eDirectory, the Change-Log module must be installed to support event processing. For more information, see Quote “ XRefProdExt Installing the Change-Log Module on a Remote eDirectory server / XRefProdExt ” / Quote in the CiteTitle XRefProdExt *NetIQ Driver for Bidirectional eDirectory Implementation Guide* / XRefProdExt / CiteTitle . / Para / ListItem
- ListItem Para (Conditional) For Identity Manager, the Identity Gateway Integration Module must be installed to support event processing. For more information, see CiteTitle XRefProdExt *NetIQ Identity Manager Driver Administration Guide* / XRefProdExt / CiteTitle . / Para / ListItem / ItemizedList

Para Once event collection is enabled, Entity Identity Governance as a Service / Entity uses the global configuration parameters Command `com.netiq.iac.rtc.event.polling.interval` / Command and Command `com.netiq.iac.rtc.max.polling.timeout` / Command 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 GUIMenu **Batch Size Limit** / GUIMenu as configured in the GUIMenu **Service Parameters** / GUIMenu is less than one hundred, that batch size is the upper limit for event collection also. / Para

---

Important **IMPORTANT:** Para 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. / Para / Important

---

Para 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 GUIMenu **Data Sources >** / GUIMenu GUIMenu **Activity** / GUIMenu page, as part of the detail of the most recent collection for that collector. / Para

Note **NOTE:** Para For more efficient event processing, change events are not generated for any dynamic changes in eDirectory or IDM dynamic groups. Also, removing a member from an eDirectory or IDM 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 a membership query. / Para / Note / Sect3 / Sect2 / Sect1

Sect1 Title # Transforming Data During Collection / Title

Para 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 Entity Identity Governance as a Service / Entity collection process. For example, the application might store dates as a string (Literal `20151202` / Literal) which needs to be converted to the Entity Identity Governance as a Service / Entity date format. Also, an application might use field lengths that do not match the field length in Entity Identity Governance as a Service / Entity. These variations in collected data affect your ability to use the data or merge it with data collected from other sources. / Para

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

Para The following example translates the values Command `true` / Command and Command `false` / Command from the connected system to Command `active` / Command and Command `inactive` / Command in the Entity Identity Governance as a Service / Entity catalog. / Para

Screen
```
if (inputValue == 'true') {
    outputValue = 'active';
}
else {
    outputValue = 'inactive';
}
```
/ Screen / Sect1

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. ![EAN: Removed a statement about upgrading from IG 2.5 here, since this isn't supported in IGaaS.]

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 as a Service 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" in the *NetIQ Identity Governance 3.0.1 Release Notes*.
- If you collect data from two or more identity sources that have duplicate information for the `Primary Supervisor ID from Source` attribute, Identity Governance as a Service 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.

- ListItem Para You must export data sources from the current version of Entity Identity Governance as a Service / Entity to be able to correctly import them. / Para / ListItem
- ListItem Para You can use the Entity Identity Governance as a Service / Entity Custom Collector SDK to create collectors. For more information, see the Ulink NetIQ Identity Governance 3.0.1 Release Notes / Ulink . / Para / ListItem / ItemizedList / Note

---

Procedure Title **To create a data source:** / Title

1. Step Para Log in to Entity Identity Governance as a Service / Entity as a Data Administrator. / Para / Step
2. Step Para Select GUIMenu **Data Sources** / GUIMenu . / Para / Step
3. Step Para (Conditional) To create an identity source collector, select GUIMenu **Identities** / GUIMenu . / Para / Step
4. Step Para (Conditional) To create an application source collector, select GUIMenu **Applications** / GUIMenu . / Para / Step
5. Step Para Select GUIMenu **+** / GUIMenu to create a data source collector from a template. / Para

   Or or / Or

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

   ---

   Important **IMPORTANT:** Para You must export a data source from the current version of Entity Identity Governance as a Service / Entity to import an updated version. Data source files exported from earlier versions of Entity Identity Governance as a Service / Entity do not import correctly to the current version. Hence, the data source must be recreated in the current version of Entity Identity Governance as a Service / Entity . / Para / Important / Step

   ---

6. Step Para (Conditional) To configure an identity source with change events collector, select a template name ending in GUIMenu **with changes** / GUIMenu and observe the conditions listed in XRefInt "Collecting from Identity Sources with Change Events" on page 142 / XRefInt . For more information, see XRefInt "Understanding Change Event Collection Status" on page 148 / XRefInt and XRefInt "Supported Attributes for eDir and IDM Change Events Collection" on page 149 / XRefInt . / Para

Note **NOTE:** Para 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. / Para / Note

Important **IMPORTANT:** Para For large scale changes, disable event collection, and enable it only for incremental change events. / Para / Important / Step

7 Step Para Enter all the mandatory fields for the data source. / Para

Para For more information, see the following content in XRefInt Understanding Collector Configuration / XRefInt : / Para

- ItemizedList ListItem Para XRefInt "Understanding the Common Elements in a Collector" on page 134 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Understanding Collector Templates for Identity Sources" on page 136 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Understanding Collector Templates for Application Sources" on page 137 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Understanding the Variations for Data Sources" on page 140 / XRefInt / Para / ListItem / ItemizedList / Step

8 Step Para Save your settings. / Para / Step

9 Step Para (Optional) If you want to preview all or part of the data, select GUIMenu **Test Collection and Troubleshooting** / GUIMenu. For more information, see XRefInt "Testing Collections" on page 153 / XRefInt . / Para / Step / Procedure

Para The first time you set up Entity Identity Governance as a Service / Entity , you must collect and publish data after creating your data sources so that your catalog contains the data. / Para

Procedure Title **To populate the catalog:** / Title

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

Para You need to collect and publish the data for Entity Identity Governance as a Service / Entity to add the data to the catalog. / Para / Step

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

Para For more information, see XRefInt "Setting the Merge Rules for Publication" on page 172 / XRefInt . / Para / Step

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

---

Note **NOTE:** Para When you publish any identity source, Entity Identity Governance as a Service / Entity publishes all identity sources. For more information, see XRefInt "Publishing Identity Sources" on page 171 / XRefInt . / Para / Note / Step

---

4 Step Para When you see that publication has completed, go to GUIMenu **Catalog** / GUIMenu to view the collected information. / Para / Step / Procedure

Sect2 Title Understanding Change Event Collection Status / Title

Para The event collection displays the following status: / Para

InformalTable TGroup / InformalTable / Sect2

Para **Change Event Collection Status** / Para	Para **Description** / Para
Para DISABLED / Para	Para 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. / Para
Para BLOCKED / Para	Para Event processing is enabled, but cannot proceed because the preconditions for processing change events were not met. For more information, see XRefInt "Collecting from Identity Sources with Change Events" on page 142 / XRefInt . / Para
Para READY / Para	Para Event processing is enabled and not blocked, but awaiting scheduling to proceed. / Para

Para **Change Event Collection Status** / Para	Para **Description** / Para
Para IN_PROGRESS / Para	Para Events are being polled for and processed. / Para Note **NOTE:** Para Event processing will be in progress either until a polling request returns no events, or until the configured maximum event processing time is reached. / Para / Note

Sect2 Title Supported Attributes for eDir and IDM Change Events Collection / Title

Para Entity Identity Governance as a Service / Entity supports the collection of the following attributes during eDir and IDM change events collection: / Para

- ItemizedList ListItem Para Command `Boolean` / Command / Para / ListItem
- ListItem Para Command `Case Exact String` / Command / Para / ListItem
- ListItem Para Command `Case Ignore List` / Command / Para / ListItem
- ListItem Para Command `Case Ignore String` / Command / Para / ListItem
- ListItem Para Command `Class Name` / Command / Para / ListItem
- ListItem Para Command `Counter` / Command / Para / ListItem
- ListItem Para Command `Distinguished Name` / Command / Para / ListItem
- ListItem Para Command `Integer` / Command / Para / ListItem
- ListItem Para Command `Integer 64` / Command / Para / ListItem
- ListItem Para Command `Interval` / Command / Para / ListItem
- ListItem Para Command `Numeric String` / Command / Para / ListItem
- ListItem Para Command `Object ACL` / Command / Para / ListItem
- ListItem Para Command `Octet String` / Command / Para / ListItem
- ListItem Para Command `Path` / Command / Para / ListItem

- ListItem Para Command `Postal Address` / Command / Para / ListItem
- ListItem Para Command `Printable String` / Command / Para / ListItem
- ListItem Para Command `Telephone Number` / Command / Para / ListItem
- ListItem Para Command `Time` / Command / Para / ListItem
- ListItem Para Command `Typed Name` / Command / Para / ListItem
- ListItem Para Command `Unknown` / Command / Para / ListItem / ItemizedList / Sect2 / Sect1

Sect1 Title Managing Identity and Application Sources / Title

Para Entity Identity Governance as a Service / Entity offers several ways to help you manage your data sources. / Para

Remark ![EAN: Removed an Important note here about turning on SQL Tuning Advisor for Oracle databases.] / Remark

- SubToc ItemizedList ListItem Para XRefInt “Exporting and Importing Collectors” on page 150 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Comparing Collections and Publications” on page 151 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Testing Collections” on page 153 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Creating Emulation Packages” on page 154 / XRefInt / Para / ListItem / ItemizedList / SubToc

Sect2 Title Exporting and Importing Collectors / Title

Para The ability to export and import collectors helps you manage your environment in several ways: / Para

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

Para 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. / Para

Remark ![EAN: Removed the following sentence from the para above for IGaaS (don't think IGaaS would work this way): "You can also use exported collectors to replicate an environment, either in a test environment or to use in another office location."] / Remark

Para 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 GUIMenu **Administration** / GUIMenu in Entity Identity Governance as a Service / Entity . For more information, see XRefInt "Customizing the Collector Templates for Data Sources" on page 42 / XRefInt . / Para

Procedure Title **To export and import collectors:** / Title

1. Step Para Select a data source, and then select GUIMenu **Test Collection and Troubleshooting** / GUIMenu . / Para / Step
2. Step Para Select GUIMenu **Download and Emulation** / GUIMenu , and then select GUIMenu **Download Data Source Configuration** / GUIMenu . / Para / Step
3. Step Para Select a location for the file, and then select GUIMenu **OK** / GUIMenu . / Para / Step
4. Step Para If you make changes and want to import a collector, under GUIMenu **Data Sources** / GUIMenu , select GUIMenu **Identities** / GUIMenu or GUIMenu **Applications** / GUIMenu , and then select GUIMenu **Import an identity source** / GUIMenu or GUIMenu **Import an application source** / GUIMenu . / Para / Step
5. Step Para Select the file to import. / Para / Step / Procedure / Sect2

Sect2 Title Comparing Collections and Publications / Title

Para 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. Entity Identity Governance as a Service / Entity uses the defined data policies to produce the comparison details. For more information, see XRefInt Chapter 15, "Creating and Managing Data Policies," on page 129 / XRefInt . / Para

Procedure Title **To compare collections and publications from the same source:** / Title

Remark ![EAN: Noticed that some of these procedures don't specify that you have to log in with a particular type of account - should check whether this info needs to be added.] / Remark

1. Step Para Under GUIMenu **Data Sources** / GUIMenu, select GUIMenu **Activity** / GUIMenu. / Para / Step
2. Step Para (Optional) Select the calendar icon to focus the list on a specific time period. / Para / Step
3. Step Para (Optional) Enter a data source name in the search to focus the list on specific data sources. / Para / Step
4. Step Para (Optional) Change the number of rows per page to show a longer list. / Para / Step
5. Step Para (Optional) To quickly compare a collection or publication with the previous collection or publication, select the item from the GUIMenu **Date and status** / GUIMenu column. / Para / Step
6. Step Para Select a listed collection or publication using the checkbox. / Para / Step
7. Step Para Select a collection or publication from the same source to compare to the first selection. / Para

---

Note **NOTE:** Para You are able to select only one additional item from the same source and type. / Para / Note / Step

---

8. Step Para Under GUIMenu **Action** / GUIMenu, select GUIMenu **Compare** / GUIMenu. / Para / Step
9. Step Para 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. / Para / Step

10 Step Para (Optional) To quickly view or open the applicable data policies, complete the following: / Para

10a SubSteps Step Para Select GUIMenu **Refine comparison options** / GUIMenu . / Para / Step

10b Step Para Select or clear listed policies to change your comparison results. / Para / Step

10c Step Para Select GUIMenu **Edit Policies** / GUIMenu to open the GUIMenu **Data Administration** / GUIMenu > GUIMenu **Data Policy** / GUIMenu page. For more information see, XRefInt "Creating and Managing Data Policies" on page 129 / XRefInt . / Para / Step / SubSteps / Step / Procedure / Sect2

Sect2 Title Testing Collections / Title

Para 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. / Para

Para 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 Entity Identity Governance as a Service / Entity until you delete them. / Para

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

- ItemizedList ListItem Para All records / Para / ListItem
- ListItem Para Some records / Para / ListItem
- ListItem Para Raw data / Para / ListItem
- ListItem Para Transformed data / Para / ListItem / ItemizedList

Para 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. / Para

Para Strong **Raw** / Strong 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 Entity Identity Governance as a Service / Entity transforms it. / Para

Para Strong **Transformed** / Strong data contains attribute names that you have mapped from the native application to the attribute names you are using within Entity Identity Governance as a Service / Entity . Testing the transformed data collection lets you verify that your mappings within the data collector meet your expectations. / Para

Procedure Title **To test a sample collection from a data source:** / Title

1. Step Para Select a configured data source. / Para / Step
2. Step Para Select GUIMenu **Test Collection and Troubleshooting** / GUIMenu . / Para / Step
3. Step Para Under GUIMenu **Test Collection** / GUIMenu , select the collectors, and then select GUIMenu **Run Test Collection** / GUIMenu . / Para / Step
4. Step Para Select the specific entities to collect and type the number of records to collect or leave GUIMenu **All** / GUIMenu to collect all records. / Para / Step
5. Step Para Select the option for the type of collection to run. / Para / Step
6. Step Para After the test collection shows GUIMenu **Complete** / GUIMenu , select GUIMenu **Action** / GUIMenu to view, download, or delete test collection results. / Para / Step / Procedure / Sect2

Sect2 Title Creating Emulation Packages / Title

Para 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 Entity Identity Governance as a Service / Entity until you delete them. / Para

Procedure Title **To create an emulation package:** / Title

1. Step Para Select a configured data source. / Para / Step
2. Step Para Select GUIMenu **Test Collection and Troubleshooting** / GUIMenu . / Para / Step
3. Step Para Under GUIMenu **Download and Emulation** / GUIMenu , select GUIMenu **Create emulation package** / GUIMenu . / Para / Step
4. Step Para When the emulation status shows GUIMenu **Complete** / GUIMenu , select GUIMenu **Action** / GUIMenu to view, download, or delete the emulation package. / Para / Step / Procedure / Sect2 / Sect1 / Chapter

17 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 as a Service automatically publishes the data.

- "Creating a Scheduled Collection" on page 155
- "Monitoring Scheduled Collections" on page 157
- "Understanding the Cron Expression for a Custom Interval of Collection" on page 157

Creating a Scheduled Collection

You can schedule collections to run 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 to Identity Governance as a Service as a Global Administrator.
2. Under **Data Sources**, select **Schedules**.

3 Step Para (Conditional) When adding a new scheduled collection, complete the following steps: / Para

3a SubSteps Step Para Select GUIMenu + / GUIMenu to create a new schedule. / Para / Step

3b Step Para Specify a name and description. / Para / Step

3c Step Para Specify the identity and application sources for collection. / Para / Step / SubSteps / Step

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

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

5a SubSteps Step Para For GUIMenu **Repeat** / GUIMenu, select an interval or specify GUIMenu **custom** / GUIMenu. / Para

---

Important **IMPORTANT:** Para 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. / Para / Important / Step

---

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

5c Step Para For GUIMenu **Custom** / GUIMenu, use the following syntax to indicate the collection time: / Para

Screen Replaceable *second minute hour day_of_month month year* / Replaceable / Screen

Para For example, Command `0 20 10 ? * *` / Command. For more information about specifying the parameter values, see XRefInt "Understanding the Cron Expression for a Custom Interval of Collection" on page 157 / XRefInt. / Para / Step / SubSteps / Step

6 Step Para (Conditional) To see a list of the first 10 scheduled runs, select GUIMenu **Preview** / GUIMenu. / Para / Step

7 Step Para To ensure that the schedule runs, select GUIMenu **Active** / GUIMenu. / Para / Step

8 Step Para Save the schedule. / Para / Step / Procedure / Sect1

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 as a Service displays the collection in a gray field.

To observe the details of a scheduled collection, select its name. Identity Governance as a Service 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 as a Service indicates the success and time of collection and publication for each data source. If you select a data source, Identity Governance as a Service 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 as a Service displays the **Identity Sources** overview page.

Understanding the Cron Expression for a Custom Interval of Collection

Identity Governance as a Service 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`.

VarListEntry Term ***** / Term

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

VarListEntry Term **-** / Term

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

VarListEntry Term ***/*** / Term

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

VarListEntry Term **?** / Term

ListItem Para Emphasis *Applies only to* Command *`day_of_month`* / Command / Emphasis / Para

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

VarListEntry Term **L** / Term

ListItem Para Emphasis *Applies only to* Command *`day_of_month`* / Command / Emphasis / Para

Para Specifies that you want to run the collection on the last day of the month. For example, Command `0 20 10 L *` / Command . / Para / ListItem / VarListEntry / VariableList

Para 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 Command `0 0 0/6 5,7,21,24 MAR-JUN,OCT *` / Command . 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: Literal `MAR-JUN,OCT` / Literal . / Para / Sect1 / Chapter

18 Integrating Collected Data with Identity Manager

This section provides guidance for using the **NetIQ Identity Manager Driver for NetIQ Identity Governance as a Service** (Access Review 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 as a Service can collect data from identity and application sources that are not connected to Identity Manager. With the Access Review 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 a Service, as well as to request and provision these permissions using Identity Manager. The driver can also provision users in the Identity Vault for Identity Manager as needed.

- "Understanding Synchronization and Reflection" on page 159
- "Ensuring Best Performance for Identity Matching" on page 162
- "Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager" on page 163
- "Synchronizing Changes in Identity Governance as a Service Data with Objects in the Identity Vault" on page 165
- "Migrating User Objects to the Identity Vault" on page 167

Understanding Synchronization and Reflection

The Access Review driver helps synchronize changes to identities and applications in Identity Governance as a Service 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 Entity Identity Governance as a Service / Entity . / IntroPara

- SubToc ItemizedList ListItem Para XRefInt “Reflecting Application Permissions in Identity Manager” on page 160 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Synchronizing Data Changes between Identity Governance as a Service and Identity Manager” on page 161 / XRefInt / Para / ListItem / ItemizedList / SubToc

Sect2 Title Reflecting Application Permissions in Identity Manager / Title

Para For each application source in Entity Identity Governance as a Service / Entity , you can Strong **reflect** / Strong 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 Entity Access Review driver / Entity can create resources in Identity Manager that match the permissions and permission assignments in Entity Identity Governance as a Service / Entity . Identity Manager users can then request access to these resources even when the application is not a connected system in Identity Manager. / Para

Para 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, you might want to enable reflection for the application source. / Para

Para When you reflect an application’s permissions, the Entity Access Review driver / Entity 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 Entity Identity Governance as a Service / Entity has for the application. For example, if an application source in Entity Identity Governance as a Service / Entity is named “SAP Permissions,” the driver creates a Resource Category named “SAP Permissions” in Identity Manager. / Para

Para 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 “Synchronizing Data Changes between Identity Governance as a Service and Identity Manager” on page 161.

When integrating application data with Identity Manager, the Access Review 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 “Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager” on page 163.

Synchronizing Data Changes between Identity Governance as a Service and Identity Manager

When you stop reflecting an application’s permissions or you delete an application from Identity Governance as a Service, 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 as a Service. When you publish the latest snapshot of collected data to Identity Manager, the Access Review driver uses the Publisher Resource Object Unlink GCV to communicate that the ABC Money application no longer exists in Identity Governance as a Service. 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 as a Service 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 as a Service notes that the identity for Joe Smith has been deleted. This generates an event in Identity Governance as a Service 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 Access Review driver creates user objects only for the identities that you add to Identity Governance as a Service after you enable synchronization. If you have identities in Identity Governance as a Service already, you can migrate those identities to the Identity Vault.

Para For more information, see the following sections: / Para

- ItemizedList ListItem Para XRefInt "Migrating User Objects to the Identity Vault" on page 167 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Synchronizing New User Objects" on page 165 / XRefInt / Para / ListItem / ItemizedList / Sect2 / Sect1

Sect1 Title Ensuring Best Performance for Identity Matching / Title

Para Review the following recommendations to ensure the best performance among the Entity Access Review driver / Entity , Entity Identity Governance as a Service / Entity , and Identity Manager components: / Para

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

    IntroPara For more information, see XRefInt "Migrating User Objects to the Identity Vault" on page 167 / XRefInt . / IntroPara / ListItem / ItemizedList

  Para If you enable reflection first, the process might generate a large number of synchronization events and assignment operations. / Para / ListItem
- ListItem Para Tune the Identity Vault to index the attributes that the Entity Access Review driver / Entity uses for matching a large number of 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: / Para
  1. OrderedList ListItem Para SystemItem `workforceID` / SystemItem / Para / ListItem
  2. ListItem Para Internet Email Address / Para / ListItem
  3. ListItem Para Given Name + Surname / Para / ListItem / OrderedList / ListItem
- ListItem Para Review the migration queries to reduce the amount of data that the driver transfers through the Remote Loader and the Identity Manager engine. / Para / ListItem

- ListItem Para Order your identity sources in Entity Identity Governance as a Service / Entity 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, otherwise user authorizations fail. / Para

  Para For more information, see XRefInt Chapter 17, "Creating and Monitoring Scheduled Collections," on page 155 / XRefInt and XRefInt "Setting the Merge Rules for Publication" on page 172 / XRefInt . / Para / ListItem / ItemizedList / Sect1

Sect1 Title Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager / Title

IntroPara Entity Identity Governance as a Service / Entity can collect account and permission data from application sources that do not have role and resource objects in Identity Manager. The Entity Access Review driver / Entity serves as the proxy for the application sources. For more information, see XRefInt "Reflecting Application Permissions in Identity Manager" on page 160 / XRefInt . / IntroPara

---

Note **NOTE:** Para The driver needs both a system account and a workflow in the User Application to create resources. For more information, see " Quote " XRefProdExt Installing and Configuring the Access Review Driver / XRefProdExt " / Quote in the CiteTitle XRefProdExt *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide* / XRefProdExt / CiteTitle . / Para / Note

---

1 Procedure Step Para Log in to Entity Identity Governance as a Service / Entity as a Global Administrator. / Para / Step

2 Step Para Add the Identity Manager information to Entity Identity Governance as a Service / Entity . / Para

   2a SubSteps Step Para Select GUIMenu **Administration** / GUIMenu , then expand the GUIMenu **Identity Manager system connection information** / GUIMenu section. / Para / Step

   2b Step Para Provide the Identity Manager URL. For example:
   Command `http://myserver:8180/IDMProv` / Command . / Para / Step

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

2d Step Para Select GUIMenu **Test Connection** / GUIMenu . Ensure that you have a valid connection before proceeding. / Para / Step / SubSteps / Step

3 Step Para Under GUIMenu **Catalog** / GUIMenu , select GUIMenu **Applications** / GUIMenu . / Para / Step

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

5 Step Para Select the icon for GUIMenu **Edit application** / GUIMenu . / Para / Step

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

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

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

Para In Entity Identity Governance as a Service / Entity , the name for this user is the concatenation of the account Literal `GivenName` / Literal and Literal `Surname` / Literal attributes. For more information about this account, see “ Quote “ XRefProdExt Creating an Identity Manager Provisioning Service Account for the Driver / XRefProdExt ” / Quote in the CiteTitle XRefProdExt *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide* / XRefProdExt / CiteTitle . / Para / Step

9 Step Para For each application, repeat XRefInt Step 4 / XRefInt through XRefInt Step 8 / XRefInt . / Para / Step / Procedure / Sect1

Synchronizing Changes in Identity Governance as a Service Data with Objects in the Identity Vault

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

- "Synchronizing New User Objects" on page 165
- "Synchronizing Resource Objects" on page 167

Synchronizing New User Objects

The Access Review driver synchronizes only the identities that are created in Identity Governance as a Service after you enable synchronization with Identity Manager. If you already have identities in Identity Governance as a Service when you enable synchronization, you need to migrate the existing user objects. For more information, see "Migrating User Objects to the Identity Vault" on page 167.

The following GCVs allow you to configure how the Access Review 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 as a Service identities with Identity Manager identities, the Identity Governance as a Service driver looks first in this sub-tree to determine whether an identity from Identity Governance as a Service 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 Entity Identity Governance as a Service / Entity user object to a value of the Literal `DirXML-Accounts` / Literal attribute on the user object. / Para

Para The default value is Literal `\data\users\arusers` / Literal. 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 Entity Identity Governance as a Service / Entity, you can efficiently remove users collected from Entity Identity Governance as a Service / Entity. / Para / ListItem / VarListEntry

VarListEntry Term **Publisher User Object Deletion** / Term

ListItem Para Provides options for Identity Manager when responding to an identity deleted from Entity Identity Governance as a Service / Entity. When the Entity Access Review driver / Entity communicates the delete event through the driver, you can configure Identity Manager to perform one of the following actions: / Para

- ItemizedList ListItem Para GUIMenu **Remove Association** / GUIMenu: Removes the SystemItem `DirXML` / SystemItem association for the identity between Identity Manager and Entity Identity Governance as a Service / Entity. The user object remains in the Identity Vault. / Para / ListItem
- ListItem Para GUIMenu **Disable Users, Remove Association** / GUIMenu: (Default setting) Breaks the relationship for the identity between Identity Manager and Entity Identity Governance as a Service / Entity. 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. / Para / ListItem
- ListItem Para GUIMenu **Delete Users** / GUIMenu: Deletes the user object from the Identity Vault. / Para / ListItem / ItemizedList / ListItem / VarListEntry / VariableList

Para For more information about configuring GCVs in a driver, see Quote “ XRefProdExt When and How to Use Global Configuration Values / XRefProdExt ” / Quote in the CiteTitle XRefProdExt *NetIQ Identity Manager Driver Administration Guide* / XRefProdExt / CiteTitle. / Para / Sect2

Synchronizing Resource Objects

The **Publisher Resource Object Unlink** GCV specifies how Identity Manager responds when you remove an application source from Identity Governance as a Service. 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 as a Service. For more information about reflecting permissions, see the following sections:

- "Reflecting Application Permissions in Identity Manager" on page 160
- "Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager" on page 163

Migrating User Objects to the Identity Vault

The Access Review driver has an optional Publisher channel functionality that enables the driver to capture identities added to Identity Governance as a Service and 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 as a Service 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 as a Service 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 **NOTE**

- ItemizedList ListItem Para You cannot migrate identities if you have not configured synchronization. For more information about synchronizing identities, see XRefInt "Synchronizing New User Objects" on page 165 / XRefInt . / Para / ListItem
- ListItem Para Before starting user migration to the Identity Vault, enable GUIMenu **Adds and Migrate Allowed** / GUIMenu in the driver configuration then restart the driver. / Para / ListItem / ItemizedList / Note

IntroPara For more information, see the following sections: / IntroPara

- SubToc ItemizedList ListItem Para XRefInt "Targeting Identities that Do Not Exist in Identity Manager" on page 168 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Adding Application Permissions after Migrating Identities" on page 169 / XRefInt / Para / ListItem / ItemizedList / SubToc

Sect2 Title Targeting Identities that Do Not Exist in Identity Manager / Title

Para To support migration, the Entity Access Review driver / Entity 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 Entity Access Review driver / Entity recognizes these synchronized identities by the value of their Literal `Distinguished Name` / Literal attribute.

To avoid duplicating identities, you can add the − Literal `DirXML-Accounts` / Literal attribute to the migration query. The − Literal `DirXML-Accounts` / Literal attribute has the following values: / Para

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

− Para To target all of the − Entity Identity Governance as a Service / Entity identities, regardless whether they already exist in the Identity Vault, do not use the − Literal `DirXML-Accounts` / Literal attribute in the migration query. / Para / Sect2

− Sect2 − Title Adding Application Permissions after Migrating Identities / Title

− Para When you migrate identities to Identity Manager, the − Entity Access Review driver / Entity 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: / Para

- − ItemizedList − ListItem − Para − XRefInt “Ensuring Best Performance for Identity Matching” on page 162 / XRefInt / Para / ListItem
- − ListItem − Para − XRefInt “Reflecting Application Permissions in Identity Manager” on page 160 / XRefInt / Para / ListItem / ItemizedList / Sect2 / Sect1 / Chapter

19 Chapter Title Publishing the Collected Data / Title

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

- SubToc ItemizedList ListItem Para XRefInt “Publishing Identity Sources” on page 171 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Publishing Application Sources” on page 174 / XRefInt / Para / ListItem / ItemizedList / SubToc

Sect1 Title Publishing Identity Sources / Title

Para Entity Identity Governance as a Service / Entity publishes all identity sources concurrently to ensure that each unified identity receives the latest merged information. Identity sources always get published before application sources. / Para

- SubToc ItemizedList ListItem Para XRefInt “Understanding Publication Behavior” on page 171 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Setting the Merge Rules for Publication” on page 172 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Publishing the Identity Sources” on page 174 / XRefInt / Para / ListItem / ItemizedList / SubToc

Sect2 Title Understanding Publication Behavior / Title

Para 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: / Para

VariableList VarListEntry Term **Publish and merge** / Term

ListItem Para 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 Literal `first_name` / Literal and Literal `last_name` / Literal attributes for Jane Smith. This option allows you to combine the duplicate attributes from the sources into one identity for Jane in the Entity Identity Governance as a Service / Entity catalog. / Para

Para 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 Strong **attribute authority** / Strong , Entity Identity Governance as a Service / Entity 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 XRefInt "Setting the Merge Rules for Publication" on page 172 / XRefInt . / Para / ListItem / VarListEntry

VarListEntry Term **Publish without merging** / Term

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

VarListEntry Term **Do not publish** / Term

ListItem Para 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. / Para / ListItem / VarListEntry / VariableList / Sect2

Sect2 Title Setting the Merge Rules for Publication / Title

Para 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 do not select priorities using merging rules, − Entity Identity Governance as a Service / Entity uses the first collected value. / Para

1 − Procedure − Step − Para Log in to − Entity Identity Governance as a Service / Entity as a Data Administrator. / Para / Step

2 − Step − Para Select − GUIMenu **Data Sources > Identities** / GUIMenu . / Para / Step

3 − Step − Para (Optional) Arrange the order of the identity sources to set their priority for merging the published attributes. / Para / Step

4 − Step − Para (Optional) To use a specific identity source as the attribute authority, complete the following steps: / Para

4a − SubSteps − Step − Para Under − GUIMenu **Publish and merge** / GUIMenu , expand − GUIMenu **Set merging rules** / GUIMenu . / Para / Step

4b − Step − Para For the attribute that you want to modify, specify the identity source. / Para

− Para The − GUIMenu **None (go by order)** / GUIMenu option instructs − Entity Identity Governance as a Service / Entity to use the first identity source as the attribute authority. / Para / Step / SubSteps / Step

5 − Step − Para Select the − GUIMenu **Save** / GUIMenu icon. / Para / Step

6 − Step − Para (Optional) Publish your pending changes. / Para / Step

7 − Step − Para (Optional) Verify the changes that you published to the catalog. / Para / Step / Procedure / Sect2

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

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

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 Service as a Data Administrator.
2. Publish your identity sources.

   For more information, see "Publishing the Identity Sources" on page 174.
3. Select **Data Sources > Applications**.
4. For each application source that you want to publish, select **Publish**.

20 Managing Data in the Catalog

Para Entity Identity Governance as a Service / Entity 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, Entity Identity Governance as a Service / Entity 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. / Para

- SubToc ItemizedList ListItem Para XRefInt "Configuring the Data Source for Post Authentication Matching" on page 175 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Understanding Identity, Application, and Permission Management" on page 177 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Editing Attribute Values on Objects in the Catalog" on page 181 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Searching for Users or Groups" on page 183 / XRefInt / Para / ListItem
- ListItem Para XRefInt "Managing Technical Roles" on page 185 / XRefInt / Para / ListItem / ItemizedList / SubToc

Sect1 Title Configuring the Data Source for Post Authentication Matching / Title

Para A user is a valid Entity Identity Governance as a Service / Entity user when the user is authenticated by a One SSO provider (OSP) and has been mapped to a published Entity Identity Governance as a Service / Entity catalog user. The post authentication mapping occurs based on the User Mapping configuration. NetIQ configures the values for authentication matching in the Configuration Utility. / Para

Remark ![EAN: Added the last sentence in the above para for IGaaS. Previously there was a link to the Auth Matching Rules under the Security Settings section, which has been removed. Didn't add anything about contacting anyone because presumably this configuration would already be done as part of the deployment for the customer.] / Remark

Para 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. / Para

Para By default, all Entity Identity Governance as a Service / Entity users must have the GUIMenu **LDAP Distinguished Name** / GUIMenu attribute mapped in the attribute catalog. Entity Identity Governance as a Service / Entity uses this attribute to authenticate users who log in to the application. / Para

1 Procedure Step Para Log in to Entity Identity Governance as a Service / Entity as a Global Administrator or Data Administrator. / Para / Step

2 Step Para Select GUIMenu **Data Sources > Identities** / GUIMenu . / Para / Step

3 Step Para Select the authentication server that you specified during installation. / Para / Step

4 Step Para Ensure that you have collected data from the data source and it is enabled for user view. For more information, see XRefInt "Assigning Authorizations to Identity Governance as a Service Users" on page 60 / XRefInt . / Para / Step

5 Step Para Scroll down to the GUIMenu **Collect User** / GUIMenu or the GUIMenu **Collect Identity** / GUIMenu section. / Para / Step

6 Step Para For GUIMenu **LDAP Distinguished Name** / GUIMenu , specify the attribute in your identity source that you want to map to the login attribute for Entity Identity Governance as a Service / Entity users. / Para

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

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

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

   8a SubSteps Step Para Select GUIMenu **Add Attribute** / GUIMenu . / Para / Step

   8b Step Para Specify the settings for the new attribute, and then select GUIMenu **Save** / GUIMenu . / Para / Step

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

8d − Step − Para Select − GUIMenu **Save** / GUIMenu . / Para / Step / SubSteps / Step

9 − Step − Para (Optional) Add the new login users to authorizations in − Entity Identity Governance as a Service / Entity . For more information, see − XRefInt "Assigning Authorizations to Identity Governance as a Service Users" on page 60 / XRefInt . / Para / Step / Procedure / Sect1

− Sect1 − Title Understanding Identity, Application, and Permission Management / Title

− Para This section addresses changing identity, application, and permission information: / Para

- − SubToc − ItemizedList − ListItem − Para − XRefInt "Managing Identity Information" on page 177 / XRefInt / Para / ListItem
- − ListItem − Para − XRefInt "Managing Application Information" on page 178 / XRefInt / Para / ListItem
- − ListItem − Para − XRefInt "Reviewing Application Fulfillment Settings" on page 179 / XRefInt / Para / ListItem
- − ListItem − Para − XRefInt "Managing Permission Information" on page 180 / XRefInt / Para / ListItem / ItemizedList / SubToc

− Sect2 − Title Managing Identity Information / Title

− Para Identity information includes the attributes and relationships you collect through the identity collectors, status in − Entity Identity Governance as a Service / Entity , 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. / Para

− Procedure − Title **To view or edit identity details:** / Title

1 − Step − Para Navigate to − GUIMenu **Catalog > Users** / GUIMenu and select a user. For example, Lisa Haagensen. / Para / Step

2 − Step − Para View basic information about that user, and select − GUIMenu **More** / GUIMenu to see more details. / Para / Step

3 − Step − Para Select available tabs to view items such as group membership, role assignments, and source for the user information. / Para / Step

4 Step Para (Optional) Select the GUIMenu Edit / GUIMenu icon next to user. / Para / Step

5 Step Para Modify the available attribute values, and then select GUIMenu Save / GUIMenu . / Para / Step / Procedure / Sect2

Sect2 Title Managing Application Information / Title

Para 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. / Para

Procedure Title **To manage the application information:** / Title

1 Step Para Navigate to GUIMenu **Catalog > Applications** / GUIMenu . / Para / Step

2 Step Para Select the name of an application. For example, Literal `MoneyHoney Financials` / Literal . / Para / Step

3 Step Para Select the GUIMenu **Edit** / GUIMenu icon. / Para / Step

4 Step IntroPara Modify the application settings, such as: / IntroPara

VariableList VarListEntry Term **Risk** / Term

ListItem Para Specifies the importance the application in terms of limited access and security / Para

Para For example, you might want to review access to applications with a GUIMenu **high** / GUIMenu risk more often than applications with a GUIMenu **mild** / GUIMenu risk. / Para / ListItem / VarListEntry

VarListEntry Term **Administrators** / Term

ListItem Para Specifies users who can access the Catalog and can manage data / Para / ListItem / VarListEntry

VarListEntry Term **Tags** / Term

ListItem Para Specifies a string that creates a new tag or shows existing tags from another application that match the string / Para / ListItem / VarListEntry

VarListEntry Term **Owners** / Term

ListItem Para Specifies a user who is responsible for reviews where the review definition references the Application Owner / Para / ListItem / VarListEntry

VarListEntry Term **Show permission hierarchy in review** / Term

ListItem Para 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 / Para / ListItem / VarListEntry

VarListEntry Term **Show account name in review and fulfillment details** / Term

ListItem Para Specifies whether you want to hide account names / Para

Para 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. / Para / ListItem / VarListEntry

VarListEntry Term **Permission ID for granting accounts** / Term

ListItem Para Specifies whether you want to use an autocompleter of permissions published in the system / Para / ListItem / VarListEntry / VariableList / Step / Procedure / Sect2

Sect2 Title Reviewing Application Fulfillment Settings / Title

Para Entity Identity Governance as a Service / Entity allows you to specify a fulfillment method for each application. In the catalog, you can see the fulfillment settings for each application. / Para

Procedure Title **To review current fulfillment settings:** / Title

1. Step Para Log in to Entity Identity Governance as a Service / Entity . / Para / Step
2. Step Para Under GUIMenu **Catalog** / GUIMenu , click GUIMenu **Applications** / GUIMenu , and select an application. / Para / Step
3. Step Para Under GUIMenu **Fulfillment Information** / GUIMenu , view the fulfillment type and details. / Para / Step / Procedure

Para For information about configuring fulfillment methods, see XRefInt “Configuring Fulfillment” on page 23 / XRefInt . / Para / Sect2

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 as a Service 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

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 GUIMenu **Catalog** / GUIMenu, 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. Entity Identity Governance as a Service displays any attributes that the Data Administrator has designated as editable, along with the current attribute value. When you change a value, Entity Identity Governance as a Service 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, Entity Identity Governance as a Service always truncates the string at 2000 characters.

For more information, see the following sections:

- "Editing Data" on page 181
- "Editing Attribute Values in Bulk" on page 182

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.

Editing Attribute Values in Bulk

You can edit attribute values for multiple objects at the same time by importing the data into Identity Governance as a Service 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 (|).

![EAN: Removed the following para for IGaaS because presumably it would be done automatically during deployment and shouldn't need to be mentioned:
"Before you follow this procedure, make sure you have configured the bulk database folder in the Identity Governance Configuration Utility. For more information, see "Bulk Data Update Settings" on page 52."]

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. Complete 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 as a Service 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. Contact NetIQ Customer Support to get the template from the appropriate location on the Identity Governance as a Service server. The template location is specified through the Identity Governance as a Service Configuration Utility.

   ![EAN: Updated step 9 for IGaaS, since customers would need to get the template location info from COE.]

10 Step Para Add the update information to the template. Once you have done so, contact NetIQ Customer Support to request that the updated template be copied to the appropriate location on the Entity Identity Governance as a Service / Entity server. Entity Identity Governance as a Service / Entity automatically detects updated files and applies the updated information to your data. / Para

Remark ![EAN: Updated step 10 for IGaaS because it would require access to the file system on the IG server.] / Remark

---

Note **NOTE:** Para You can specify multiple users as permission owners. / Para / Note

---

Remark ![EAN: The Note above previously had some text that said, when performing bulk edits of permission owners, the ID name had changed from uniqueUserId to uniqueOwnerId, and the uniqueOwnerId required a new #true flag with each permission owner ID. Removed this text for IGaaS because new customers wouldn't care what the previous version of IG had.] / Remark / Step / Procedure

Para You can also undo an edited value or explicitly set a value to null. Entity Identity Governance as a Service / Entity recognizes certain keywords in cells that perform specific actions: / Para

- ItemizedList ListItem FormalPara Title **UNDO_CURATION:** / Title

  Para Removes any previously edited values for this attribute. / Para / FormalPara / ListItem
- ListItem FormalPara Title **SET_NULL:** / Title Para Sets the appropriate null or empty value on this attribute. / Para / FormalPara / ListItem / ItemizedList / Sect2 / Sect1

Sect1 Title Searching for Users or Groups / Title

Para You can search for specific items in the catalog by selecting the type of item under GUIMenu **Catalog** / GUIMenu, such as GUIMenu **Users** / GUIMenu or GUIMenu **Groups** / GUIMenu. Then type your search criteria in the search box, and select the search icon. / Para

Para Entity Identity Governance as a Service / Entity 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. / Para

Para Some areas of the catalog provide advanced search options. If available, the search box contains a down arrow icon to access advanced search. The advanced search acts differently from the other searches in Entity Identity Governance as a Service / Entity . / Para

Para You can add additional criteria to the advanced search by clicking GUIMenu + / GUIMenu icon. The advanced search ANDs all search criteria, which means that for an advanced search to return a catalog item, it must meet all of the search criteria. Some attributes, such as applications or owners, support specifying multiple values in a single criteria to perform OR operations. For example, searching for permissions from either application A or B. / Para

Para 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. Advanced search does not currently support partial names for applications or owners. / Para

Para The attributes that appear in the refinement list are fixed for Technical Roles. However, they can be configured for User and Permission catalog items. / Para

Procedure Title **To add or remove user attributes from the refinement list:** / Title

1. Step Para Select GUIMenu **Data Administration** / GUIMenu > GUIMenu **User** / GUIMenu or GUIMenu **Permission** / GUIMenu . / Para / Step
2. Step Para Select an attribute to edit the attribute definition. / Para / Step
3. Step Para Select the desired searchable option for the attribute to have it appear in the catalog or not: / Para

   VariableList VarListEntry Term **Available in catalog searches. Change takes effect after publication.** / Term

   ListItem Para 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. / Para / ListItem / VarListEntry

   VarListEntry Term **Display as refine search option** / Term

   ListItem Para Select this option to enable the attribute for advanced searches. / Para / ListItem / VarListEntry

   VarListEntry Term **Display in review item selection criteria** / Term

   ListItem Para Select this option when you want the attribute displayed in review items. For more information, see XRefInt Chapter 7, “Running a Review Instance,” on page 81 / XRefInt . / Para / ListItem / VarListEntry

VarListEntry Term **Display in business role selection criteria** / Term

ListItem Para 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 XRefInt Chapter 10, “Creating and Managing Business Roles,” on page 95 / XRefInt . / Para / ListItem / VarListEntry / VariableList / Step

4 Step Para Select GUIMenu **Save** / GUIMenu , then publish the changes to the catalog. / Para / Step / Procedure / Sect1

Sect1 Title Managing Technical Roles / Title

Para 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. / Para

Para After you have published application data, you can create technical roles to group permissions that are common to these technical roles. When you have created technical roles, Entity Identity Governance as a Service / Entity detects users with permissions that match the technical roles you have defined and lists the technical roles that a user has in the user catalog. When you have defined technical roles, you can create user access review definitions for technical roles reviews. / Para

- SubToc ItemizedList ListItem Para XRefInt “Understanding Technical Role States” on page 185 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Understanding Technical Role Mining” on page 186 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Creating Technical Roles” on page 187 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Activating Technical Roles” on page 190 / XRefInt / Para / ListItem
- ListItem Para XRefInt “Editing and Deleting a Technical Role” on page 191 / XRefInt / Para / ListItem / ItemizedList / SubToc

Sect2 Title Understanding Technical Role States / Title

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

InformalTable TGroup / InformalTable / Sect2

Para **Technical Role State** / Para	Para **Description** / Para
Para CANDIDATE / Para	Para 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. / Para
Para ACTIVE / Para	Para Valid, meaning all included permissions are available in the catalog, and the role is included in the detection process. / Para
Para NOT ACTIVE / Para	Para Valid; however, the role is excluded from the detection process. This state corresponds to the internal state called REJECTED. / Para
Para INVALID / Para	Para Invalid and excluded from the detection process due to a detected error. Detection errors are usually the result of a deleted permission that is included in the technical role. / Para

Sect2 Title Understanding Technical Role Mining / Title

Para Entity Identity Governance as a Service / Entity uses advanced analytics to mine business data and identify role candidates. This process of discovering and analyzing business data to group multiple users and access rights under one business or technical role candidate is called Role Mining or Role Discovery. Global or Technical Role administrators can use role mining to create technical roles with common permissions. Entity Identity Governance as a Service / Entity uses two approaches to technical role mining to identify technical role candidates: / Para

- ItemizedList ListItem FormalPara Title **Automatic Suggestions** / Title

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

Note **NOTE:** Para Technical role candidates can also be generated when using mining to create business roles. For more information about business roles, see XRefInt Chapter 10, “Creating and Managing Business Roles,” on page 95 / XRefInt / Para / Note

Note **NOTE:** Para 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. / Para / Note / Sect2

Sect2 Title Creating Technical Roles / Title

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

Para 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. / Para

Para 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 Entity Identity Governance as a Service / Entity and add the appropriate permissions to the technical role. You cannot activate a technical role until you have added permissions to the technical role. / Para

Procedure Title **To create a technical role:** / Title

Remark ![EAN: Steps 1 and 2 below were previously combined in one step. Separated them for IGaaS.] / Remark

1. Step Para Log in to Entity Identity Governance as a Service / Entity as a Global Administrator or a Technical Roles Administrator. / Para / Step
2. Step Para In the GUIMenu **Catalog,** / GUIMenu select GUIMenu **Roles** / GUIMenu . / Para / Step
3. Step Para Select the GUIMenu **Mining** / GUIMenu tab. / Para

InformalTable > TGroup > / InformalTable > / Step

Para If / Para	Para Then / Para
Para You want to direct role mining calculations and create more than one technical role / Para	• ItemizedList > ListItem > Para Select GUIMenu **Automatic Suggestions** / GUIMenu . / Para / ListItem • ListItem > Para Save default options, or specify options, and save. / Para / ListItem • ListItem > Para Select one or more items from the list and GUIMenu **Create Roles** / GUIMenu . / Para Note **NOTE:** Para Suggestions are sorted by number of users multiplied by 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. / Para / Note / ListItem / ItemizedList

Para If / Para	Para Then / Para
Para You want to use a user access map to create a role candidate / Para	• ItemizedList ListItem Para Select GUIMenu Visual Role Mining / GUIMenu . / Para / ListItem • ListItem Para Click the map and drag to select an area. / Para / ListItem • ListItem Para Click GUIMenu View Candidate / GUIMenu . / Para / ListItem • ListItem Para (Optional) Click GUIMenu more / GUIMenu to add a description, risk, cost, or category. / Para / ListItem • ListItem Para (Optional) Click GUIMenu + / GUIMenu to add permissions, or click GUIMenu Remove / GUIMenu next to a permission to remove permissions. / Para / ListItem • ListItem Para Estimate impact. / Para / ListItem • ListItem Para Click GUIMenu Create candidate / GUIMenu . / Para / ListItem / ItemizedList

4 Step Para On the GUIMenu Roles / GUIMenu page, click the mined role. / Para / Step

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

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

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

8 Step Para Select GUIMenu **Yes** / GUIMenu to promote the role candidate. / Para

---

Note **NOTE:** Para If a role candidate is not promoted, it cannot be activated and published as a role. / Para / Note / Step

---

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

10 Step Para Enter the required information. / Para / Step

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

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

13 Step Para Save your settings. / Para / Step / Procedure

Note **NOTE:** Para When you add a permission to a role, the dialog displays all application permissions in Entity Identity Governance as a Service / Entity . You can quickly sort or filter permissions by name, description, or application. You can also use the advanced search options to limit the displayed permissions further. / Para / Note / Sect2

Sect2 Title Activating Technical Roles / Title

Para 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, Entity Identity Governance as a Service / Entity does not identify the users that hold the permissions in the technical role. / Para

---

Note **NOTE:** Para Mined technical roles are created in a candidate state and must be promoted before they can be activated and published. / Para / Note

---

Procedure Title **To activate a technical role:** / Title

Remark ![EAN: Steps 1 and 2 below were previously combined in one step. Separated them for IGaaS.] / Remark

1. Step Para Log in to Entity Identity Governance as a Service / Entity as a Global Administrator or a Technical Roles Administrator. / Para / Step
2. Step Para In the GUIMenu **Catalog** / GUIMenu, select GUIMenu **Roles** / GUIMenu. / Para / Step
3. Step Para Select the role from the list, then select GUIMenu **Edit** / GUIMenu. / Para / Step
4. Step Para In the role definition, select GUIMenu **Active** / GUIMenu. / Para / Step / Procedure

Para Activating and deactivating a technical role both start a detection process. Entity Identity Governance as a Service / Entity detects users in the catalog that contain the permissions when you activate a technical role. When you deactivate a technical role, Entity Identity Governance as a Service / Entity removes the detected technical roles in the catalog. Similarly, if you change the permissions in an active technical role definition, Entity Identity Governance as a Service / Entity goes through the detection process and updates the catalog. / Para

Para You can quickly search for a role by name or description. Entity Identity Governance as a Service / Entity 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. / Para / Sect2

Sect2 Title Editing and Deleting a Technical Role / Title

Para When you edit a technical role, you can change permissions assigned to the technical role and either leave the technical role active or disable it. However, Entity Identity Governance as a Service / Entity 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. / Para

Procedure Title **To edit or delete a technical role:** / Title

Remark ![EAN: See previous comment - add separate step for logging in with specific role.] / Remark

1. Step Para In the catalog, select GUIMenu **Roles** / GUIMenu as a Global Administrator or a Technical Roles Administrator. / Para / Step
2. Step Para Select the role you want to edit or delete. / Para

   Para 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. / Para / Step
3. Step Para Select GUIMenu **Edit** / GUIMenu at the end of the details panel to edit the technical role. / Para / Step
4. Step Para (Conditional) Select GUIMenu **Delete** / GUIMenu to delete the technical role. / Para

   Para You must edit the technical role to delete the technical role. / Para / Step / Procedure

Para You can also download technical roles as Filename `json` / Filename files using the bulk action menu. After editing, you can import the roles on the page that lists all technical roles. / Para / Sect2 / Sect1 / Chapter

21 Chapter Title Grooming the Entity Identity Governance as a Service / Entity Databases / Title

Remark ![EAN: Reworded the following para for IGaaS, and removed the rest of the chapter per feedback from Chan and Rick. Hosted customers don't need to know specifics about the Data Purge utility or how it works.] / Remark

IntroPara In addition to regularly backing up the Entity Identity Governance as a Service / Entity databases, NetIQ periodically grooms the databases to remove old and unused data. NetIQ must perform these tasks for you because they require access to the Entity Identity Governance as a Service / Entity server. If you have an environment with lots of reviews and you notice any performance lags, NetIQ can perform additional database grooming as needed to improve performance. For assistance, contact NetIQ Customer Support. / IntroPara / Chapter / Part

V Reporting for Identity Governance as a Service

Identity Governance as a Service integrates with Identity Reporting to generate reports about the status of reviews, collected and published data, and fulfillment. The Report Administrator can create, run, and view reports. You can have NetIQ install Identity Reporting with Identity Governance as a Service or you can run reports from an existing installation of Identity Manager Identity Reporting. You must decide which scenario works best for your environment.

![EAN: Modified the above para for IGaaS. There was a missing cross-ref at the end of the above para, but I removed it for IGaaS because I wasn't sure where it was supposed to link to.]

This section assumes that you intend to use Identity Reporting with Identity Governance as a Service in an environment without Identity Manager. For more information about using Identity Reporting in an Identity Manager environment, see the Identity Manager Documentation (https://www.netiq.com/documentation/) website.

![EAN: The link above was previously two bullets linking to the specific Linux and Windows setup guides. For IGaaS, removed these and made the link more general, partly because this was confusing, given the SubToc bullets below.]

22 Setting Up Identity Reporting

![EAN: Updated this intro for IGaaS.]

After NetIQ has installed the Identity Reporting component with Identity Governance as a Service in your environment, many of the installation properties of Identity Reporting can be modified as needed using the Configuration Utility. For assistance, contact NetIQ Customer Support.

Preparing Identity Reporting for Use

Identity Reporting requires a Report Administrator and at least one data source. You assign the administrator authorization in Identity Governance as a Service. In general, your data source is the Identity Governance as a Service database.

To prepare Identity Reporting for daily use, you need to complete the following activities:

Assigning the Report Administrator Authorization

To log in to Identity Reporting, your account must have the Report Administrator authorization in Identity Governance as a Service.

1. Log in to Identity Governance as a Service as the Global Administrator.
2. Select **Administration > Authorization Assignments**.
3. Assign users or groups to the Report Administrator authorization.
4. Save the change.
5. Select **Identity Manager System Connection Information**.
6. For **Identity Manager URL**, specify the URL for Identity Reporting.

   For example, `http://myserver.mydomain.com:8080/IDMRPT`.
7. Save the change, then refresh the browser to see the change.

Testing the Integration with Identity Governance as a Service

As a Report Administrator, you can access Identity Reporting from the Identity Governance as a Service interface. You can also log in directly from the Identity Reporting URL. Only accounts with the Report Administrator authorization should be able to log in to Identity Reporting.

![EAN: Above wording: “Only accounts .... *should* be able ....” ? Reword this. Need to review this procedure again - I don’t think these steps are quite right.]

1 To verify that you can access Identity Reporting from Identity Governance as a Service, complete the following steps:

   1a Log in to Identity Reporting, then select **Home** in the upper right corner.

   1b Select the **Reporting** module icon near your user name.

   1c Verify that you are redirected to Identity Reporting.

2 To verify that other authorizations are denied access to Identity Reporting, complete the following steps:

   2a Log in to Identity Governance as a Service, as a Global Administrator or Security Officer.

   2b Remove the Report Administrator authorization from the account that successfully logged in to Identity Reporting.

   2c Log in to Identity Reporting with that account, which no longer has the authorization.

   You should attempt the login from both Identity Governance as a Service and the Identity Reporting URL.

   2d Verify you cannot access Identity Reporting.

   You can also attempt to log in to Identity Reporting by using a Global Administrator or Security Officer account to verify that accounts with high-level privileges cannot access Identity Reporting without the Report Administrator authorization.

Adding Data Sources to Identity Reporting

Identity Reporting runs reports against your connected data sources. Before you can run reports, you need to add the data sources.

NOTE: You must add the Identity Governance as a Service `igops` database as a data source in Identity Reporting.

![EAN: Left this section/procedure for IGaaS for now, and reworded some steps to make it work. However, it might be something that we do for customers as part of setup, in which case the steps should be removed. Or, we might provide a list of data sources that they could choose from and there wouldn’t be an option for them to provide the details for the source, in which case steps 4 and 5 would need to change. Left this as is for now; can change it later once we figure out the details of our processes.]

1 Log in to Identity Reporting as the Report Administrator.

2 Select **Data Sources**.

3 Select **Add**.

4 Specify whether you want to select from the list of data sources or provide the details for the source.

5 (Conditional) If you selected **Provide database details**, specify the values that NetIQ provided you for the data source. For example, the database platform, the host name or IP address of the database server, the name of the database, and an account that can access the tables and views in the database.

6 (Optional) Test the connection to your data source.

7 Select **Save**.

8 ![EAN: Rewrote this step for IGaaS, but it’s probably not needed at all.]

Contact NetIQ Customer Support to request that the Tomcat folders be cleaned up and Tomcat restarted if necessary.

9 Run a test report to verify functionality in Identity Reporting.

For more information about running reports, see “Running Identity Governance as a Service Reports” on page 204.

Enabling Auditing for Identity Reporting after Installation

![EAN: Updated the following para and removed the procedure in this section for IGaaS.]

If NetIQ did not enable auditing for Identity Reporting in your environment during the installation, you can request that auditing for Identity Reporting be enabled later. For assistance, contact NetIQ Customer Support.

23 Managing Identity Governance as a Service Reports

The Report Administrator can create, run, and view reports.

To use Identity Reporting, your login account must have a Report Administrator authorization. Use a browser to log in to Identity Reporting. For example: `http://server1.mycompany.com:8080/IDMRPT`.

Understanding the Provided Reports

Identity Reporting provides several pre-defined reports for Identity Governance as a Service. For the most recent changes to reports, see the latest release notes at the NetIQ Identity Governance as a Service Documentation (http://www.netiq.com/documentation) website.

NOTE: For reports in CSV format, you must select CSV as the output format. All CSV reports are downloadable CSV files that can be opened with spreadsheet software and enable user manipulation of the data.

Report	Description
Account Ownership	Shows the average number of accounts owned by identities across all applications. Optionally, it shows average numbers broken down by all applications or specified applications. Averaging across all applications supersedes specific application selection.
Accounts in Review - CSV	Lists all account reviews and displays details such as application sources, reviewers, review status, and final decisions for each review in a downloadable CSV file that can be opened with spreadsheet software and enables user manipulation of the data. Select CSV as the output format.![AN- Selecting user step will be removed per Jon. Check before finalizing document.]
Bulk Data Update Details	Provides details of bulk data update operations for identity and application sources.
Bulk Data Update Overview	Provides an overview of bulk data update operations for identity and application sources.
Catalog Account Details	Displays information about specified applications including associated permissions, accounts, and Identity Manager System information.
Catalog Account Overview	Provides high-level information about accounts in the catalog.

Report	Description
Catalog Applications Details	Displays information about specified applications including associated permissions, accounts, and Identity Manager System information.
Catalog Applications Overview	Displays high-level information about each application in the catalog.
Catalog Curated Data Details	Provides details of attribute data curated for users, accounts, and permissions, comparing effective values with the most recently collected and published values.
Catalog Curated Data Overview	Displays high-level information about each group in the catalog.
Catalog Extended Attributes	Displays high-level information about each extended attribute in the catalog.
Catalog Group Details	Displays information about the specified groups in the catalog, including group membership.
Catalog Permissions Details	Displays information about specified permissions, their associated users, and their affiliated permissions.
Catalog Permissions Overview	Displays high-level information about each permission in the catalog, grouped by application, and which business roles has authorized it.
Catalog Users Ad Hoc	Displays user-defined information pertaining to identities as well as their associated permissions and applications.
Catalog Users by Supervisor	Provides information about each user in the catalog, grouped by supervisor. Optionally, it includes users without a supervisor.
Catalog Users Details	Displays information about specified users in the catalog, including group membership, permissions held, associated accounts, and direct reports.
Catalog Users Overview	Lists all identity sources and applications, and the times they are collected and published in the system.
Collection Details	Provides the status and details for all collection and publication instances of each identity and application source.
Collection Overview	Lists all identity sources and applications, and the times they are collected and published in the system.
Database Statistics for Identity Governance	Displays Identity Governance database statistics for the selected data source. You must have Administrator-level access to the Identity Governance database to retrieve the statistics from the database.
Fulfillment Status and Closed Loop Verification	Lists the status of application provisioning requests, identifying which requests have been verified as fulfilled and which remain open.
Fulfillment Status and Closed Loop Verification - CSV	Lists the status of application provisioning requests, identifying which requests have been verified as fulfilled and which remain open in CSV format.

Report	Description
Permission Assignment Changes by Permission	Displays permission holders at the beginning and end of the specified date range, as well as permission assignment additions and removals between the displayed lists of permission holders.
Permission Delta by Permission	Displays the changes in permissions held by a specified user within a given date range. Permissions are sorted by application.
Permissions Delta by User	Displays the changes in permissions held by a specified user within a given date range. Permissions are sorted by application.
Permissions in Review - CSV	Lists permissions in review in CSV format.
Preview Changes - CSV	Lists changes made to review instances, and reassigned review items while in preview mode in CSV format.
Privileged Account Ownership	Shows the privileged accounts owned by users across all applications along with the users for each account. Output can be grouped by application.
Review Definitions	Lists details for all review definitions including User Access Review and Unmapped Account Review.
Review Details	Lists all reviews and displays details such as application sources, permissions, reviewers, review status, and final decisions for each report.
Review Details - CSV	Lists all reviews and displays details such as application sources, permissions, reviewers, review status, and final decisions for each report in CSV format.
Review Item Exception	Lists all reviews that contain exception items along with their exception reason and time of exception.
Review Overview	Lists a summary of all reviews, their status, and dates.
Reviewer Status	Lists review status information grouped by supervisor.
Role Details	Provides detailed information about roles, including associated permissions and separation of duties policies.
Role Overview	Provides a summary of technical roles and business roles.
Separation of Duties Open Violations Details	Provides detailed information about open separation of duties violations including violators, violations details, and actions taken.
Separation of Duties Open Violations Overview	Displays high-level information about each Separation of Duty open violation.
Separation of Duties Policies Details	Provides detailed conditions and compensating controls for separation of duties policies.
Separation of Duties Policies Overview	Provides a summary of separation of duties policies.

Report	Description
Unmapped Accounts	Lists application accounts and any permissions that they hold that do not have associated users. The accounts are grouped by application. Duplicate account names across multiple applications can also be highlighted.
User Permissions Snapshot	Displays permission information about the specified user on a selected date. Intended for Identity Governance.

Running Identity Governance as a Service Reports

You can run reports at any time. You can also create a schedule to run reports regularly.

NOTE: Scheduled reports should always use the date and time for the server where you installed Identity Reporting. When you use Identity Reporting in an environment distributed across multiple time zones, scheduled reports might run at a time other than the scheduled hour. This occurs because of the discrepancy between the time zones for the server that hosts Identity Reporting compared to the computer from which you scheduled the report. For example, a user in London schedules a report to run at 4 a.m., with the assumption that the report runs according to Greenwich Mean Time. However, the reporting server in New York City runs the job at 4 a.m. Eastern Daylight Time, which is five hours later than the user planned.

1. Log in to Identity Reporting as the Report Administrator.

   You can enter the reporting URL directly in the browser or select the **Reporting** module icon near your user name in Identity Governance as a Service.
2. Select **Repository**.
3. (Conditional) If the Repository does not contain any Identity Governance as a Service reports or you want to add or update reports, complete the following steps:
   - **3a** Select **Download**.
   - **3b** (Optional) Change the filter to **Identity Governance Reports**.![does the filter now say IdGov?]
   - **3c** Browse to **Updated reports** or **New reports**.
   - **3d** Select the Identity Governance as a Service reports that you want to use, and in **Bulk Actions**, select **Install report definition archives (RPZ)**.![do we need to say AR or IdGov here?]
   - **3e** Select **Apply**.
4. (Conditional) If you want to change any report values, specify the report values with the following considerations:

   Criteria

   Ensure that you specify a data source that relates to the report type. If Identity Reporting cannot run the report against the specified data source, Identity Reporting displays an **<!>** icon beside **Data source**.

   You can specify the language for fields in the report. The data in the report will always be in the language of its data source.

   Default Notifications

   You can send the report to anyone. Simply specify the values for the notifications.

Schedule

You can add and remove scheduled runs of the report. You can also have several scheduled runs with different names. To ensure that the report includes the most recent data, select **Attempt data collection before scheduled run**.

5 Select **Repository**, and then select the reports that you want to run.

Reports for Identity Governance as a Service have a tag of “Identity Governance.”

6 In **Bulk Actions**, select **Run Now**, and then select **Apply**.

7 Select **Reports** to view completed reports.

VI Instructions for Identity Governance as a Service Users

This section provides instructions for the following Identity Governance as a Service users:

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

Users with these transient authorizations might not need access to the administrative functions in Identity Governance as a Service and do not need to read the entire *Identity Governance as a Service User Guide*. Instead, these users can print their particular instructions or access the information on the Identity Governance as a Service Documentation (https://www.netiq.com/documentation/) website.

24 Instructions for Access Requesters and Approvers

This section provides information for individuals using the Identity Governance as a Service Access Request interface to request or approve access for themselves or others.

For more information about configuring and administering Access Request, see Chapter 12, “Administering Access Request,” on page 117.

Understanding the Access Request Process

The Access Request interface allows you to request application access and permissions for other resources in your environment. These requests might be subject to an approval chain before they are granted, and Access Request also manages these approvals. Additional features include the ability to view access request-related activity timelines, the ability to view SoD violations if any, and the ability to compare granted permissions between users, allowing you to standardize their access. Finally, based on your authorization, it allows you to examine your own current access, or the access of another user, revoke a request, retry a failed request, or terminate a failed request.

Access Request allows you to request the following types of items:

- Application request, which usually gives login privileges to that application
- Permission request, which usually gives more rights within an application
- Access profile (technical role), which is a collection of permissions requested as a single request

Identity Governance as a Service administrators define the policies that govern who can request access, what they can request access for and for whom, and any required approvals. Approvers are notified by email of pending requests according to these Access Request policies, which contain a fine-grained mechanism for controlling the frequency of these notifications. Access Request policies may also designate CC and BCC email recipients, as well as an escalation policy in case the approver does not act in a timely fashion. For more information, see Chapter 12, “Administering Access Request,” on page 117.

Reviewing Current Access

Current Access lists all the permissions you currently own. If you have permission to view access for others, you can change to another user to see their access. You might also have permission to remove access items for yourself and others.

1. In the Access Request interface, select **Current Access** to review the permissions you hold. Dynamic resources appear as a link that you can select to show additional information.
2. Select your name under **Current Access** to see any other users whose access you have permission to view.
3. (Optional) If a permission appears as a link, select it to view more information.
4. Select another user to view their current list of access items.

NOTE: The current list of access items is always for the user listed under Current Access.

---

5. (Optional) Select the trash can icon next to any item you want to remove, type a reason, and then select **Add to request**.

NOTE: If there is no trash can next to an item, that item is not removable.

---

6. (Conditional) If you have any items in the shopping cart, select the shopping cart, and then select **Submit**.

NOTE: Selecting a trash can next to a request in the shopping cart immediately removes the request from the cart but does not submit the request.

Requesting Access and Viewing a Timeline

Under **Request**, you can:

- View and refresh a list of your requests, their current status, and a timeline showing details of the request, approval, and fulfillment events
- View and request an application access, application permission, or access profile recommended for you or a user for whom you are authorized to request permissions
- Browse and request an application access, application permission, or access profile for you or a user for whom you are authorized to request permissions

---

NOTE: Dynamic resources, a specific type of permission, might require additional input. For example, if the dynamic resource is a phone, you might have to select a phone model.

To view a list of your requests, their status, and timeline:

1. Select **Request > My Requests**.

TIP: Requests that violate SoD policies have a warning icon next to the request name. Click the icon to view violated SoD policies.

---

2. (Optional) Use **Search** to filter the requests and the page control (if shown) to page through them.
3. Select a request item status to view and collapse the timeline of underlying events associated with the request, including fulfillment information.

NOTE: Select the **Refresh** icon next to **My Requests** to refresh the status. Do not refresh the browser as it might require you to log in again or lead to an error condition.

If the Identity Governance as a Service administrators have created and assigned business roles in your environment, you might see recommended items to request. Business role assignments determine these recommended items. You can also browse other items that you can request for yourself or others.

To view and request items:

1. Select **Request > Recommended**.
2. (Optional) Use **Search** to filter the recommended items and the page control (if shown) to page through them.

   NOTE: Business role assignments determine these recommended items. If in your environment, Identity Governance as a Service administrators have not created and assigned business roles, you might not see any recommended items to request.
3. (Conditional) If there are recommended items, for example applications or access profiles, select an item, enter a reason, and select **Add to request**. Repeat this to add more items.
4. (Conditional) If you have rights to request on behalf of others:
   - **4a** Select the current user to change who you are requesting for.
   - **4b** Select an item, enter a reason, and select **Add to request**. Repeat this to add more items.
   - **4c** (Optional) Select a different user to review and request items for that user.
5. Select **Request > Browse**.
6. On the **Applications** tab, select an application to expand the items to request.
7. Select the application to request login access to the application or select individual permissions, review SoD violation if any, enter a reason, and select **Add to request**.
8. On the **Access Profiles** tab, select an access profile (technical role) to request multiple permissions in a single step, enter a reason, and select **Add to request**.
9. (Optional) Select a different user to review and request items for that user.
10. After you have requested items for all users, select the cart to submit your choices.

    NOTE: Selecting **X** next to a request in the shopping cart immediately removes the request from the cart but does not submit the request.

When you review permissions available to request, items have the following icons signifying the state of the item:

Shopping cart

Item has been requested and is in the shopping cart, but the request has not been submitted.

Lock

Item needs approval after being requested.

Clock

Item has been requested and is in progress awaiting fulfillment or approval.

Check mark

User already owns item.

Approving Access Requests

You might have to approve requested items if the Access Request policy specifies you as an approver for requests. Your Access Request administrators might have flagged some items as needing further approval if someone requests them. Some administrators require business role members, a person's supervisor, or an application owner to approve requested items, and some items might require multiple approvers. In these situations, you must approve items before the next designated approver receives them.

To see and act on your approval items:

1. In the Access Request interface, select **Approvals**.
2. Select a request item on the left to display the details on the right. A request might contain more than one requested item.
3. (Optional) Select a requested item to see details about the request, including decision support information.

   NOTE: By default, Identity Governance as a Service enables decision support information, including business role authorization status. If you do not use business roles, and if you are also an administrator, you can disable the status display by deselecting the **Administration > Analytics and Role Mining Settings > Show business role authorization status** option.
4. Select **Approve** or **Deny** for each requested item.
5. Select **Confirm approval** to submit your approval tasks.

Comparing Access of Multiple Users

If you have permission to see and request items for others, you can also show multiple users with their permissions listed to compare their access. When you are comparing a user to other users, you can request items for the first user in the list, making it easy to ensure that users in the same job role have the same access.

1. In the Access Request interface, select **Compare**.
2. Under **User Access Comparison**, select the user whose access you want to compare with others.
3. Select **Compare to** for a list of users to compare with the first user.
4. (Optional) Select **Compare to** and choose additional users to continue adding to the table. As you add users to compare with the first user, Identity Governance as a Service adds permissions in the first column to reflect all the listed users' permissions, adds check marks in the appropriate columns to show that a user owns a permission, and puts a link to add or remove permissions for the first column for any permissions you are allowed to change for that user.
5. (Optional) Select **Add** or **Remove** to change the permissions for the first user in the table, enter a reason, and select **Add to request**.

   NOTE: Dynamic resources might require additional input. For example, if the dynamic resource is a phone, you might have to select a phone model.
6. (Conditional) If you have added requests to your cart, select the cart and submit the requests.

   NOTE: Selecting a trash can next to a request in the shopping cart immediately removes the request from the cart, but does not submit the request.

Retracting an Access Request

Occasionally, you might need to retract an access request that has not been fulfilled. Instead of creating a help desk ticket to terminate the request, you can now revoke it directly in Identity Governance as a Service. A retracted request item will move from a tentatively retracted to a completed retracted state.![why two states- can a retract be canceled? can a request with completed retract status, be submitted again?]

NOTE: You can revoke a request only for a request item that is either in approval pending or failed state. After fulfillment, use procedures in “Requesting Access and Viewing a Timeline” on page 210 to remove or add access.

To retract an access request:

1. Select **Request > My Requests**.
2. If the **Status** of a request item is Approval Pending or Approval Failed, click **Retract**.

Restarting a Failed Access Request

Occasionally, access requests may fail. For example, if OSP is configured for HTTPS, but the server where the request workflow is running does not have the proper certificate in the cert store to be able to communicate with it, the request item will fail. Once you have fixed the issue, instead of requesting access again, you can retry the failed request item.

To restart a failed access request:

1. Select **Request > My Requests**.
2. Check the error message for information about the request item with Approval Failed status.
3. Fix the issue or contact your system administrator to fix the issue.
4. Once the issue has been fixed, click **Retry**.

25 Instructions for Reviewers

This section provides information for individuals assigned the Reviewer authorization for a review run in Identity Governance as a Service. Reviewers confirm whether permissions or membership granted to a user or account should be kept or removed or, in some cases, modified.

Understanding Reviews

Identity Governance as a Service collects information from a variety of identity and application data sources in your environment. This allows your organization to periodically review and verify that users have only the level of access that they need to do their jobs.

Understanding the Steps in a Review Run

In Identity Governance as a Service, Review Administrators create **review definitions** for a particular set of users or accounts that need review. A single instance of a review definition is a **review run** or review campaign, which has a Review Owner. The Review Owners can see only the review runs that they own.

Reviews can be started either in a preview or a live mode. Review Administrators can set up a review to automatically start in preview mode or they can set up a regular schedule in a review definition so the review runs start automatically in live mode, according to the schedule.

Understanding the Steps in a Preview Review Run

When the owner initiates a review run in preview mode, or when a review run starts automatically in preview mode, the following activities occur:

1. Identity Governance as a Service generates lists of **Reviewers**, **Review items**, and **Notifications**.
2. The Review Owner previews the review definition for the current run and optionally changes the review owner or auditor, and modifies review options and schedule.
3. The Review Owner reviews all the review items and assigned reviewers, or searches for specific review items, to decide whether the items should be assigned to another reviewer.
4. The Review Owner also verifies that appropriate notifications are being sent to the correct recipients, and if required, emails the notification template for preview.

NOTE: The changes made by the Review Owner are applied only to the current run. If permanent changes need to be made to the review definition, or reviewers need to be changed for all subsequent runs, the changes must be made by editing the review definition itself.

5. Optionally, the Review Owner downloads all or select review items as a CSV file to review it manually.

Understanding the Steps in a Live Review Run

When the owner initiates a review run in live mode, or when a review run starts by the schedule, the following activities occur:

1. Identity Governance as a Service generates tasks for the assigned Reviewers and notifies them as specified in the review definition.
2. Reviewers review their assigned set of review items and decide whether the items should be kept, modified, or removed. If a review item is assigned to multiple reviewers, the first reviewer who acts on that item becomes the decision-maker, and the item continues to the next phase of the review. For more information, see “Performing a Review” on page 217.
3. (Conditional) If the review definition specifies that a permission requires multiple stages of approval, Identity Governance as a Service forwards the affected review items to the next assigned reviewer.

   For example, the application owner, permission owner, or Review Owner might be required to review the permissions and confirm decisions before action is taken to remove any permissions. Reviewers must complete the review in the assigned order.
4. (Conditional) If a Reviewer does not complete tasks in the specified timeframe and the review definition specifies an escalation process, Identity Governance as a Service forwards the tasks to the assigned Escalation Reviewer or the Review Owner.

   For multiple serial reviewers the escalation will forward to the next reviewer before it finally ends up in the escalation reviewer or review owner queue.
5. The Review Owner approves the changes.

   NOTE: Review Owners can override reviewer decisions, if the review definition specifies it as allowed, at any point during a review run. When a Review Owner overrides a decision, the review item is removed from the reviewer’s task list.
6. Identity Governance as a Service initiates the fulfillment process to enable the requested changes.
7. (Conditional) In a manual fulfillment process, Identity Governance as a Service generates tasks that the assigned Fulfillers must complete and notifies them by email.
8. (Optional) An Auditor might be required to certify the results of the review run.

   For more information, see “Understanding the Review Process” on page 17.

Understanding the Reviewer's Authorization

Reviewers represent individuals who have the information and authority to determine whether account permissions are correct. You might be assigned to review items in multiple active review runs. Depending on how the review is defined, Identity Governance as a Service might send you emails to remind you of incomplete tasks and approaching deadlines.

As a Reviewer, you can:

- Filter the list to show only incomplete review items
- Sort the review items by many different characteristics, such as by user, permission, account, type, attribute, application, roles (technical and business), or action
- Process review items individually or in a batch
- Add a comment to a review item with your decision to keep or remove, individually or in a batch
- View the details of the review item
- View guidance on how the permission was assigned, such as through a direct assignment or authorized by a role
- Choose to keep, modify, or remove the items
- View activity for a review item
- Change Reviewer of a review item, individually or in a batch, if you do not have the information you need to confirm the assigned permissions
- Submit decisions for your tasks in the allotted timeframe

If you are an **Escalation Reviewer**, you must resolve all review items that are not completed on time.

Secondary reviewers in a multi-stage review can confirm the previous decision or they can override the decision.

For more information, see "Performing a Review" on page 217.

Performing a Review

This section provides the steps required for you to complete Reviewer tasks associated with a review run. Usually, Identity Governance as a Service sends an email notification when you have tasks in a review run.

For more information about the Reviewer's authorization and the review process, see "Understanding Reviews" on page 215.

1. In Identity Governance as a Service, select **Reviews**.
2. Select the review run on which you want to act.
3. (Optional) Adjust display options to help you manage your review items:
   - **3a** Select **Show submitted items** to see all review items in the list.
   - **3b** Click **Show all** to see a list of grouping options. This is especially helpful when you have a long list of review items.
   - **3c** Click the gear icon to change display options by adding, removing, or rearranging columns.
4. For each review item, click the review item link to view system guidance to assist you with making your decision, and then select one of the following:
   - **Keep** to specify that you believe that the user should have the account or role

- (Conditional) **Assign** if there are unmapped accounts to map the account
- (Conditional) **Modify** if the review definition allows this option
- **Remove** to specify that you believe that the user should not have the account or role
- **View Activity** to decide what actions to take or what actions have been taken
- **Change Reviewer** to pass the decision to another reviewer

---

NOTE: If you select User B, who has a delegate User C who has a delegate User B, as the new reviewer, a warning will be issued, and the **Change Reviewer** option will be disabled to prevent cyclical delegation.

![I don’t think a reviewer can see items that they can’t act on in 1.5. Commenting out until I verify this. LST If you cannot modify a review item, it is possible that another individual already acted on the item. For example, the Review Owner might have overridden your action.]

5 Review your changes to ensure accuracy.

6 Select **Submit** to confirm your actions on the review items.

This action locks your decisions and moves the items out of your queue. Identity Governance as a Service then moves the items to the next reviewer’s queue if this is a multistage review and you are not the last reviewer. If you are the last reviewer, Identity Governance as a Service notifies the Review Owner that the review is ready for certification.

If one of your review items is in the **Multiple Reviewers** queues, then your decision gets locked in when you **Submit** the decision. If you have not yet submitted a decision and another reviewer makes a decision and submits before you, it is the other reviewer's decision that gets locked. You can see the decision in the **View Activity** option.

Viewing Completed Reviews

Reviewers and Review Owners can view the details of review items they had submitted during an active review, as well as when the review instance is complete. Select **Show completed reviews** to view a completed review’s start and end date, status including certification percentage, and review items that you submitted. Optionally, sort review items by decision, and select **View Activity** to view actions related to the review item, including change reviewer and modify reasons, if any.

26 Instructions for Review Owners

Identity Governance as a Service enables your organization to review and verify that users have only the level of access that they need to do their jobs. As a Review Owner, you are responsible for managing one or more review runs in progress. You can view the details of any user, permission, roles (technical or business), or application entity within the context of the review run. However, depending on your authorization assignments, you might not have access to the Identity Governance as a Service catalog.

Understanding the Review Process for Review Owners

As a Review Owner, you can see only the review runs that you own. You can start the review run in preview mode or go live. The preview mode enables you to preview review definitions, notifications, and review items before going live. The live review process starts with the initiation of a review run and ends when the Review Owner or Auditor, if specified, certifies the review. Between those two events, Reviewers and Fulfillers perform their assigned tasks.

This section provides the following information:

For an overview of the review process, see "Understanding the Review Process" on page 17. For steps in a review run, see "Understanding the Steps in a Review Run" on page 215

Understanding the Review Definition

Each review runs according to its **review definition**, which specifies the following items:

- Review type and name
- (Optional) Review description and instructions for reviewers
- Review items, such as user accounts, roles (technical and business), and permissions, to be reviewed by the specified Reviewers
- Review options, such as whether certain actions require comments, and whether to allow self-reviews
- Individuals who serve as Reviewers, such as supervisors, permission owners, and application owners
- (Optional) Individuals who monitor reviews, such as owners and auditors
- (Optional) Escalation process for review items
- Review timeframe that contains an expiration policy and partial approval policy

- Notifications to be sent throughout the review
- (Optional) Schedule for automatically starting the next review and repeating the review on a regular basis
- (Optional) Default grouping of request items

For more information, see Chapter 6, “Creating and Modifying Review Definitions,” on page 69.

Understanding Reviewers and Escalation

When you initiate a review run, Identity Governance as a Service generates tasks for the assigned Reviewers. The Reviewers are responsible for reviewing a set of users and deciding whether the current user access should be maintained or revoked or, in some cases, modified. Identity Governance as a Service can also escalate the process and send reminders until the Reviewer completes the task. The Review Owner can reassign Reviewers, review their actions on review items, and override their review actions.

Reviews that contain reviewers specified by a coverage map can result in an escalation if no matches could be found from the coverage map. For more information about Reviewers, see “Specifying Reviewers” on page 79. For more information about managing Reviewers, see “Managing the Progress of Reviewers” on page 225.

Understanding the Fulfillment Process

The source of the identities and permissions under review drives how requested changes are fulfilled. The fulfillment process can be manual tasks, automated actions in Identity Manager, actions sent to help desk services, or actions initiated by workflows in Identity Manager. In a manual fulfillment process, the applications catalog specifies the individuals responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset. If a Reviewer changes a user’s permissions, Identity Governance as a Service creates tasks for the specified Fulfillers.

For more information about fulfillment, see “Fulfilling Changes Requested in the Review” on page 17 and “Viewing Fulfillment Status” on page 226.

Managing a Review in Preview Mode

This section provides the steps required to run a review in preview mode.

![EAN: Did some edits to this section for consistency, but should these be steps? Do the items need to be completed in order?]

- Start the review in preview mode
- View the review definition version, review items, assigned reviewers, and recipients of notifications
- Change the Review Owner, Escalation Reviewer, or Auditor for the current review run
- Change the review period, escalation timeout period, expiration policy, partial approval policy, or validity period of the current run
- Reassign Reviewers within the current review run, including bulk actions
- Search for email recipients by name
- Sort notifications by type
- Send the notification preview to a specific recipient

NOTE: Notifications sent during review preview mode, which enable administrators and review owners to preview notifications, might have blanks for values, and names seen in the preview might not be the name as those sent in the real email.

- Cancel the preview if review properties and items were not as expected and the review definition needs to be modified, or go live

Managing a Review in Live Mode

This section provides the steps required for you to run and complete a review. As the owner of an active review, you can:

![EAN: Same question as the previous section - if these are steps that are required, don't they need to be numbered?]

- Start in preview mode and go live, or start the review in live mode, and monitor the review progress
- View review status in **Reviews**
- View **Quick Info** details about a catalog item
- Reassign Reviewers within the review, including bulk actions
- Send a reminder email to a Reviewer using the **Nudge** option
- Override a Reviewer's decisions
- Change the Review Owner or add more Review Owners
- Change the Escalation Reviewer or Auditor
- Resolve access policy violations in the review
- Complete a partial review
- Terminate the review before completion
- Approve Reviewer decisions
- Run reports against the review

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

If you assign a new review owner while a review run is in progress, the review definition does not change, and the new review owner is in effect for only that review run. The next review run that starts from the same review definition assigns the review owner specified in the review definition.

For example, a review definition specifies Mary Smith as the review owner. During an instance of the review, or a review run, the global administrator realizes that Mary is on vacation. To keep the review moving, the administrator changes the review owner to Sam Butler, who approves that review run when reviewers have submitted all their final decisions. Both Mary and Sam can see the details of this review run. The next time a review run starts from this review definition, Mary is assigned as the review owner.

For more information, see the following sections:

- "Checklist for Managing a Review in Live Mode" on page 222
- "Starting a Review Run" on page 223
- "Managing a Review Run" on page 223

- “Modifying the Settings of a Review Run” on page 224
- “Managing the Progress of Reviewers” on page 225
- “Approving the Review” on page 225
- “Viewing Fulfillment Status” on page 226
- “Managing the Audit Process” on page 226
- “Viewing Run History” on page 226

For more information about running reports, see “Running Identity Governance as a Service Reports” on page 204.

Checklist for Managing a Review in Live Mode

	Checklist Items
❑	1. Ensure that you understand the review process. For more information, see “Understanding the Review Process for Review Owners” on page 219.
❑	2. Start the review run. For more information, see “Starting a Review Run” on page 223.
❑	3. (Optional) Modify the timeframe for the review. For more information, see “Modifying the Settings of a Review Run” on page 224.
❑	4. Check the progress of each Reviewer. For more information, see “Managing the Progress of Reviewers” on page 225.
❑	5. Approve the actions taken by the Reviewers. For more information, see “Approving the Review” on page 225.
❑	6. (Conditional) Check the status of manual fulfillment activities. If the process is automated or uses external workflows, Identity Governance as a Service sends the changeset to Identity Manager for processing. For more information, see “Viewing Fulfillment Status” on page 226.
❑	7. (Conditional) Confirm the completion of all fulfillment tasks, if any occurred.
❑	8. (Conditional) If a review run generated a changeset, collect and publish all identities and the application sources related to the review run. You might not have an authorization in Identity Governance as a Service that allows you to collect and publish. A user with the Global Administrator or Data Administrator authorization can perform this action.
❑	9. (Conditional) Check the status of the review audit. For more information, see “Managing the Audit Process” on page 226.
	10. (Optional) View the run history. For more information, see “Viewing Run History” on page 226

Starting a Review Run

In Identity Governance as a Service, you can see all review definitions assigned to you, including the date that the Review Administrator specified the review should be run.

1. In Identity Governance as a Service, select **Definitions**.
2. In the **Actions** column, select **Start Review** on the row of the definition that you want to run.
3. Select **Start and Go Live**.

Managing a Review Run

You can view the status of the review runs in progress, send reminder emails, change the assignments for reviewers and the auditor, override reviewer decisions, complete, approve, or terminate the review run, and approve the completed review.

1. In Identity Governance as a Service, select **Reviews**.

   Identity Governance as a Service displays an overview of runs in progress, which indicates progress of completed tasks.
2. To manage the run, select the review.
3. To see a status of each of the review items, select **Review Items**.
4. Act on individual review items either individually or using the bulk selection options. Actions you can take depend on settings in the review definition and may include:

   ![EAN: Each of the following items needs a “click” or “select” to follow our standard - can’t just use the UI item as the verb.]

   - **View activity** to see review item details
   - (Conditional) **Override** a Reviewer’s decision to make a decision final and remove it from all reviewer queues
   - **Change reviewer** to transfer the review item to another reviewer
   - **Approve** to move the decision to fulfillment while allowing the review to continue
   - **View fulfillment status** to view status of review requests such as removing a permission, or assigning a new user
5. To complete the review as-is, accepting all final decisions and leaving items without final decisions as **No decision**, select **Complete** in the review completion overview at the top of the review.
6. To move all final decisions to fulfillment while allowing the review to continue, select **Approve** in the review completion overview at the top of the review.
7. To cancel the review, select **Terminate** in the review completion overview at the top of the review.

Why would I override a Reviewer’s action?

As the owner of the software application being reviewed, you might disagree with a Reviewer’s decision that grants a user access to the application. Alternatively, you might see the need for a user to have access where the Reviewer did not. For example, you know that a manager in Human Resources requires administrative permissions to the application.

Why would I complete or approve an in-progress review?

As the owner of a review, you might want to implement decisions that have been made without waiting for all reviewers to complete their tasks. Approving individual review items or the overall review sends final decisions to fulfillment while keeping the review running. Completing an in-progress review accepts final decisions, ends the review, marks items without decisions as **No decision**, and sends items with decisions to fulfillment.

Modifying the Settings of a Review Run

As the Review Owner, you can edit the review timeframe and escalation timeout; change the Escalation Reviewer, the assigned Auditor, and the Review Owner; and add multiple Review Owners. Depending on your entitlements, you might also be able to modify the full review definition. However, this section explains how to perform the simple modifications.

1. In Identity Governance as a Service, select **Reviews > Reviews**.
2. Select the active review run that you want to modify.
3. To determine whether the number of review tasks can be performed in the specified timeframe, complete the following steps:
   - **3a** Under the review name, select **more**, and then select the edit icon.
   - **3b** Observe the number of review items that still must be completed.
   - **3c** Compare the estimated number of review items with the date in **Review end**.
   - **3d** Change the end date for the review if needed.
4. Change or add review owners if needed.
5. Modify the appropriate settings, then select **Save**.

Why would I modify the review's timeframe?

When Review Administrators create a review, they can estimate the number of users, permissions, accounts, and review items affected by the review. Then they set the timeframe of the review. However, that estimation is based on a snapshot of the catalog at the time that they created the review definitions. Depending on when you run the review, the number of accounts might have increased or decreased considerably. The timeframe might no longer match the current state of the catalog.

Why would I change the Review Owner?

In general, the Review Owner is the owner of the software application with user accounts that the review run affects. However, your authorization in the organization might have changed. You can assign ownership of the review run to an individual more suited to the task. You might also want to assign multiple Review Owners.

Why would I change the Auditor?

If the assigned Auditor is not available to perform the tasks for the review run, you can assign a different individual to the authorization.

Managing the Progress of Reviewers

To ensure that the review run stays on schedule, you can view the progress of each Reviewer. You can also reassign tasks to a different Reviewer and override a Reviewer's action for a review item. Reviewers can change the reviewer for any items.

1. Select the active review that you want to manage.
2. Under **Reviewers**, select the name of the Reviewer that you want to manage.
3. Observe the actions taken by the Reviewer.

   You can view the items that have not been completed or all review items. You can send reminder emails, using the **Nudge** option, for items not yet reviewed. You can also change the sort of the items in various ways based on the selectable column headers.
4. (Optional) To expand a window that allows you to compose an email, click **Nudge** to send a reminder email to the reviewer.
5. (Optional) To assign a review item to a different Reviewer, select **Change Reviewer**.

   You can also reassign items in a batch.
6. (Optional) To review a Reviewer's decision, select **View Activity** for the task.

Why would I reassign a review item?

If the Reviewer is not able to perform one or more tasks for the review run, you can assign a different individual to the authorization. For example, the Reviewer might be sick or on vacation. Also, some Reviewers might complete tasks faster than others. You might want to reassign items from the slower Reviewers. For more information, see "Reviewing Access and Permissions" on page 17.

What if I have multiple reviewers?

If the reviewer is listed as **Multiple Reviewers**, then more than one reviewer shares the responsibility making a decision on the review item. You can see who are members of the shared queue and send a reminder email to all of the members or delegates, if mapping exists. When changing reviewer out of a **Multiple Reviewers** queue, the item is no longer under shared responsibility.

![EAN: I don't understand the last sentence (above).]

Approving the Review

The approval process allows the Review Owner to confirm the actions taken by all Reviewers.

1. Select the active review that you want to manage.
2. Observe the actions taken by the Reviewers.
3. (Optional) Override actions as needed.
4. To approve the decisions made in the review run, select **Approve**.
5. (Optional) Add a comment.
6. (Conditional) If the review run included changes to user accounts, ensure that the affected data sources are collected and published.

   After the administrator collects and publishes the data sources, Identity Governance as a Service updates the status of the fulfillment items.

Viewing Fulfillment Status

The source of the identities and permissions under review drives how requested changes are fulfilled. The changes can be fulfilled manually, by a help desk service, or sent to Identity Manager, which automatically makes the changes or initiates external workflows. In a manual fulfillment process, the applications catalog specifies the individuals responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset.

As the Review Owner, you can **View fulfillment status** for each review item which was fulfilled manually.

For more information about the fulfillment process, see the following sections:

- “Fulfilling Changes Requested in the Review” on page 17
- Chapter 27, “Instructions for Fulfillers,” on page 227

Managing the Audit Process

Some review definitions require an Auditor to certify the results of the review run. 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.

Viewing Run History

Identity Governance as a Service tracks all reviews, and maintains a history of previews and review runs associated with a review definition. The run history is searchable and sortable, and displays the start and end date of the run, status including certification percentage, review owner, and list of review items and associated actions including change reviewer and modify actions, and remove comments, if any. The run history also displays fulfillment status of review items.

To view run history:

1. Select **Reviews > Definitions**.
2. Search for the review definition and click the review name, or directly click the review name.
3. Select **View run history**.

NOTE: Except for terminated previews, all other previews and reviews will be listed in the run history.

---

27 Instructions for Fulfillers

This section provides information for individuals assigned the Fulfiller authorization for a review run in Identity Governance as a Service. Periodically, individuals in your organization participate in a review to determine whether permissions granted to user accounts should be kept or removed. For each change, Identity Governance as a Service creates tasks for the Fulfiller who has been assigned to manually fulfill the requests.

Understanding the Fulfillment Process

Identity Governance as a Service collects information from a variety of identity and application data sources in your environment. This allows your organization to periodically review and verify that users have only the level of access that they need to do their jobs. The review process results in a list of changes, or **changeset**, that is then implemented. Additionally, request for access also results in a list of changes. Identity Governance as a Service refers to the implementation process of a changeset as **fulfillment**.

Managing the Fulfillment Process

The source of the identities and permissions under review drives how requested changes are fulfilled. The changes can be fulfilled manually, by a help desk service, or sent to Identity Manager, which automatically makes the changes or initiates external workflows. In a manual fulfillment process, the applications catalog specifies the individuals responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset.

Fulfillment Administrators can configure fulfillment targets, keep track of the fulfillment process, and reassign manual fulfillment items if needed. Identity Governance as a Service provides the following status conditions for fulfillment items:

- Error or time out
- Fulfilled
- Pending fulfillment
- Verified
- Ignored
- Retry

When the fulfiller confirms the fulfillment activities, Identity Governance as a Service updates the status of the fulfillment item. Global and Fulfillment administrators, as well as Auditors, can access the Fulfillment page![deleted fulfiller but need to confirm] . After the administrator collects and publishes application sources again, Identity Governance as a Service updates the status of these fulfillment items.

For an overview of the fulfillment process, see “Fulfilling Changes Requested in the Review” on page 17. For more information about status conditions, see “Understanding Fulfillment Status” on page 29.

Understanding the Fulfiller’s Authorization

As part of the review, managers might change the permissions assigned to individuals in your organization. Business role membership changes can also generate change requests. Only Global Administrators and Fulfillment Administrators can assign Fulfillers to complete a fulfillment.

As a Fulfiller, you can:

- Sort the items by column. The available columns depend on the tab you are accessing.
- Add a comment to an item, individually or in a batch.
- View the details of the item at the list level, including where the change request originated, and view additional details including potential SoD violations, if any, and the reason for the request by clicking on the task link.
- Make the changes to the user account in the affected application.
- Declare your tasks complete in Identity Governance as a Service.
- View fulfillment errors.

For more information, see “Performing a Review” on page 217.

Performing a Manual Change

![EAN: Is this heading accurate? The first sentence suggests otherwise.]

This section provides the steps required for you to complete Fulfiller tasks associated with a review run. Usually, Identity Governance as a Service sends an email notification when you have tasks in a review run.

![EAN: Sentence above: “Usually”? When doesn’t IG send an email?]

For more information about your authorization and the review process, see “Understanding Reviews” on page 215.

1. In Identity Governance as a Service, select **Requests** to view the fulfillment requests.
2. Change between tabs to see requests from different areas or to see fulfillment errors.
3. Click the fulfillment task link to expand the task description and determine the changes to be made, reason for the change, and potential SoD violations if any.
4. In the application affected by the requested change, modify the permission according to the fulfillment task. This might impact the SoD policies or uncover unmapped users.
5. (Conditional) The Fulfillment Administrator can view the status of the fulfillment requests on the **Fulfillment Status** page.

   ![EAN: Step 5 doesn’t work. What’s it Conditional on? Why isn’t it written in second person/ command - isn’t the person doing the other steps the Fulfillment Admin too?]
6. Return to Identity Governance as a Service to specify one of the following outcomes for the fulfillment task:
   - **Fulfilled**: to indicate that you successfully changed the permission

- **Declined**: to indicate you could not or did not remove the permission with a comment
- **Reassign**: to assign the fulfillment task to a different user

7 (Conditional) If any errors occur during the fulfillment process, access the **Fulfillment Errors** tab to see more details. From this list you can try to resolve the errors:

7a Click **Fix** to go to the **Fulfillment Configuration** page if you have administrator access, otherwise ask your administrator to do the next step.

7b Click **Application Setup**, view the settings for the application producing errors, and adjust the settings.

7c Go back to the **Fulfillment Requests** > **Fulfillment Errors** tab, and click **Retry** to route the item to the correct fulfiller.

7d If it is not possible to fix the problem, click **Terminate** to remove this change request item from the **Fulfillment Errors** tab.

8 To complete your tasks, select **Submit**.

The fulfillment process starts only after the Review Owner completes the review. Any manual fulfillment changes to the fulfillment request do not affect the Review run.