NetIQ® Identity Governance

User Guide

June 2019

Legal Notice

Contents

About this Book and the Library

The *User Guide* provides an overview of NetIQ Identity Governance access request, review, and fulfillment processes and a step-by-step guidance for related user-oriented tasks.

Intended Audience

This book provides information for a variety of users responsible for requesting access; reviewing users, business roles, and access permissions; and fulfilling change requests in your environment. Specifically, it provides instructions for users with the following Identity Governance runtime authorizations:

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

Other Information in the Library

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

Release Notes

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

Installation Guide

Provides installation and initial configuration information for the Identity Governance product. Also provides upgrade information for current product installations.

Administrator Guide

Provides conceptual information and step-by-step guidance for administrative tasks in the Identity Governance product. Specifically, it provides instructions for the following Identity Governance users:

- All administrators
- Business Role managers
- SoD Policy owners
- Application owners

Reporting Guide

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

NetIQ Identity Manager Driver for Identity Governance

Provides information about how to install and configure the Identity Manager Driver for NetIQ Identity Governance. The Identity Governance driver allows you to provision application-specific permission catalog data from Identity Governance to Identity Manager, giving you the ability to review and certify permission assignments using Identity Governance, as well as to request and provision these permissions using Identity Manager. The driver also can provision users in the Identity Vault for Identity Manager. For more information, see *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide*.

Technical References

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

Videos

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

1 Overview

The Identity Governance 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, administrators and business managers can ensure that your employees, either individually or as a group, have the appropriate set of permissions and roles. Identity Governance collects information from various identity and application data sources and manages the entire review and certification process. Identity Governance provides tools to guide you through the key phases of the access, identity attributes, reporting relationships, role memberships, and account reviews; SoD (Separation of Duties) and audit management; and validation and remediation processes.

This guide provides guidance for:

- Requesting access
- Approving access requests
- Previewing review data
- Reviewing user access, user profile, accounts, business role memberships, and direct reports
- Approving review changes
- Fulfilling change requests
- Viewing completed reviews and fulfillment status

For information about administrative functions in Identity Governance, see the *Identity Governance Administration Guide* on the Identity Governance Documentation (https://www.netiq.com/documentation/) website.

2 Instructions for Access Requesters and Approvers

This section provides information for individuals using the Identity Governance Request interface to request or approve access for themselves or others.

For more information about configuring and administering Access Request, see "Administering Access Request" in the *NetIQ Identity Governance Administrator Guide*.

2.1 Understanding the Access Request Process

The Access Request interface allows you to examine your own current access and request application access and permissions for 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 status, ability to view SoD (Separation of Duties) violations if any, and the ability to compare granted permissions between users, allowing you to standardize their access. Finally, based on your authorization, it also allows you to request access for 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
- Technical role request, which is a collection of permissions requested as a single request

Identity Governance administrators define the policies that govern who can request access, what they can 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 "Administering Access Request" in the *NetIQ Identity Governance Administrator Guide*.

2.2 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 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**.

   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.

2.3 Requesting Access and Viewing 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 application access, application permission, or a technical role recommended for you or a user for whom you are authorized to request permissions
- Browse and request application access, application permission, or a technical role 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 lead to an error condition or require you to log in again. Identity Governance updates the request fulfillment status when fulfillers fulfill a request, and when the application or a data or global administrator collects and publishes the application data source.

If the Identity Governance administrators have created and assigned business roles in your environment, you *might* see recommended items to request. You can also browse other items that you can request for yourself or others.

To 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 administrators have not created and assigned business roles, you might not see any recommended items to request.
3. (Conditional) If there are recommended items, such as applications or technical roles, 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 violations, if any, enter a reason, and select **Add to request**.

   NOTE: If Identity Governance warns you of SoD violations, either change your request to resolve the violation or submit the request with the violations for an SoD administrator, SoD policy owner, or an SoD or Access Request policy to approve or resolve the violation.
8. On the **Technical Roles** tab, select a technical role (previously also known as access profile) 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 the item.

2.4 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 when 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.

1. In the 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 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.

2.5 Approving Potential SoD Violations

Only users with Global or SoD administrator authorization or users assigned as SoD policy owners can approve or decline potential SoD violations. For more information, see "Managing Separation of Duties Violations" in the *NetIQ Identity Governance Administrator Guide*.

2.6 Comparing Access of Multiple Users

If you have permission to see and request items for others, you can also show multiple users with their permissions listed to compare their access. When you are comparing a user to other users, you can request items for the first user in the list, making it easy to ensure that users in the same job role have the same access.

1. In the 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 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.

2.7 Retracting Access Requests

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 the application. A retracted request item will move from a tentatively retracted to a completed retracted state.

NOTE: You can revoke a request only for a request item that is either in an approval pending or failed state. After fulfillment, use procedures in "Requesting Access and Viewing Timeline" on page 10 to remove or add access.

---

1 Select **Request > My Requests**.

2 (Conditional) If the **Status** of a request item is Approval Pending or Approval Failed, click **Retract**.

2.8 Restarting Failed Access Requests

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.

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**.

3 Instructions for Review Owners

Identity Governance enables your organization to review and verify that users have only the level of access that they need to do their jobs. As a Review Owner, you are responsible for managing one or more 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 catalog.

3.1 Understanding the Review Process for Review Owners

As a Review Owner, you can view 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 by on-demand action, schedule, or micro certification and ends when the Review Owner or Auditor, if specified, certifies the review. Between those two events, Reviewers and Fulfillers perform their assigned tasks.

NOTE: Micro certifications are focused reviews which are always run in live mode. For an overview of the review process and an understanding of micro certification, see “Understanding the Review Process” and “Understanding Micro Certification” in the *NetIQ Identity Governance Administrator Guide*.

This section provides the following information:

For steps in a review run, see “Understanding the Steps in a Review Run” on page 25.

3.1.1 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), permissions, user access rights, and direct reports 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 time frame that contains an expiration policy and partial approval policy
- Notifications to be sent throughout the review
- (Optional) A 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 "Creating and Modifying Review Definitions" in the *NetIQ Identity Governance Administrator Guide*.

3.1.2 Understanding Reviewers and Escalation

When a review run is initiated, Identity Governance generates tasks for the assigned Reviewers. The Reviewers are responsible for reviewing a set of users and deciding whether the current user access should be maintained or revoked, or, in some cases, modified. Identity Governance can send reminders to the Reviewer or escalate the review items to the Escalation Reviewer, if one was specified in the Review Definition, or to the Review Owner. Also, review items in the exception queue (unmapped accounts) are automatically assigned to the Escalation Reviewer if an escalation reviewer was specified for that review.

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" in the *NetIQ Identity Governance Administrator Guide*. For more information about managing Reviewers, see Section 3.3.5, "Managing the Progress of Reviewers," on page 21. For more information about performing a review, see "Performing a Review" on page 27.

3.1.3 Understanding the Fulfillment Process for Review Changes

The source of the identities, permissions, accounts, and roles under review drives how review-related 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. Review Owners and Review Administrators can view fulfillment status of review items as soon as a review run is partially or fully approved.

For more information about fulfillment and viewing fulfillment status, see Section 5.1, "Understanding the Fulfillment Process," on page 29 and Section 3.3.7, "Viewing Fulfillment Status," on page 22.

3.2 Managing a Review in Preview Mode

This section provides the tasks required to run a review in preview mode. As the owner or an administrator of a review, you can do any or all of the following tasks:

- Start the review in preview mode
- View review definition version, review items, assigned reviewers, and recipients of notifications
- Customize the column display for the review items
- 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 a 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 that is 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

3.3 Managing a Review in Live Mode

This section provides the tasks required for you to run and complete a review. As the owner or an administrator of an active review, you can do any or all of the following tasks:

- Start in preview mode and go live, or start the review in live mode and monitor the review
- Customize the review definition and the column display for the review items
- Review details including related micro certification progress in the review definition area based on your column display options
- View the 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:

3.3.1 Checklist for Managing a Review in Live Mode

	Checklist Items
❑	1. Ensure that you understand the review process. For more information, see Section 3.1, “Understanding the Review Process for Review Owners,” on page 15.
❑	2. Start the review run if needed. In addition to manually starting a reviews, you can initiate a review by schedule or micro certification. For more information about manually starting a review, see Section 3.3.2, “Starting a Review Run,” on page 19.
❑	3. (Optional) Modify the time frame for the review. For more information, see Section 3.3.4, “Modifying the Settings of a Review Run,” on page 20.
❑	4. Check the progress of each Reviewer. For more information, see Section 3.3.5, “Managing the Progress of Reviewers,” on page 21.
❑	5. Approve the actions taken by the Reviewers. For more information, see Section 3.3.6, “Approving and Completing the Review,” on page 22.
❑	6. (Conditional) Check the status of manual fulfillment activities. If the process is automated or uses external workflows, Identity Governance sends the changeset to Identity Manager for processing. For more information, see Section 3.3.7, “Viewing Fulfillment Status,” on page 22.
❑	7. (Conditional) Confirm the completion of all fulfillment tasks.

	Checklist Items
❑	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 that allows you to collect and publish. Someone 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 Section 3.3.8, “Managing the Audit Process,” on page 22.
❑	10. (Optional) View run history. For more information, see “Viewing Run History” on page 23

3.3.2 Starting a Review Run

In Identity Governance, you can see all review definitions assigned to you, including the date that the Review Administrator specified the review should be run.

1. In Identity Governance, select **Definitions**.
2. (Optional) Click the gear icon to change column display options. For example, to add the micro certification column to your display drag **Micro-Certifications in progress** to the list of selected columns. You can then view the number of micro certifications and view the run history of the micro certification review.
3. In the Actions column, select **Start Review** on the row of the definition that you want to run.

   NOTE: For micro certification reviews, this step is not required and the Actions column is unavailable. Micro certification reviews are triggered automatically based on remediation setup and do not require manual action.
4. Select **Start and Go Live**.

3.3.3 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, select **Reviews**.

   Identity Governance displays an overview of runs in progress, which indicates progress of completed tasks.
2. (Optional) Click the gear icon to view additional column options and customize column display. For example, you can drag **Started by** to the list of selected columns to view whether a review was started on demand, on schedule, or by micro certification process.
3. To manage a run, select the review.
4. To see a status of each of the review items, select **Review Items**.
5. 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 might include:
   - **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.

6 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.

7 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.

8 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.

3.3.4 Modifying the Settings of a Review Run

As the Review Owner, you can edit the review time frame and escalation timeout; change the Escalation Reviewer, the assigned Auditor, and the Review Owner; and add multiple Review Owners. Depending on your 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, select **Reviews > Reviews**.

2 Select the active review run that you want to modify.

3 To determine whether the number of review tasks can be performed in the specified time frame, complete the following steps:

3a Under the review name, select **more**, and then select the edit icon.

3b Observe the number of review items 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 time frame?

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 time frame 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 time frame 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.

3.3.5 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.

What if I have multiple reviewers?

If the reviewer is listed as **Multiple Reviewers**, then more than one reviewer shares the responsibility for making a decision on the review item. You can see who are members of the shared queue and send reminder emails to all of the members or delegates, if a mapping exists. When a reviewer of a review item in a **Multiple Reviewers** queue is changed, the item is no longer under shared responsibility.

3.3.6 Approving and Completing the 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. The approval process allows the Review Owner to confirm the actions taken by all Reviewers. After approval, a review can be optionally routed to a Review Auditor for legal acceptance.

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 updates the status of the fulfillment items.

3.3.7 Viewing Fulfillment Status

The review and validation process that begins with data collection and publishing concludes with change request reconciliation. Identity Governance can track the status of change requests fulfilled manually or through automatic or workflow-based provisioning. As the Review Owner, you can **View fulfillment status** for review items, with decisions like **Remove** or **Modify**, that generate a change request. You can see the fulfillment status for each review item as soon as the review run is partially or fully approved, and the status continues to be updated until the completion of the fulfillment process.

For more information about the fulfillment process, see the following sections:

- Chapter 5, “Instructions for Fulfillers,” on page 29
- “Understanding Fulfillment Status” in the *NetIQ Identity Governance Administrator Guide*.

3.3.8 Managing the Audit Process

Some review definitions require a Review Auditor to certify the results of the review run. Review Auditors are individuals who have read-only access to a review run. They cannot modify or delete decisions. They can:

- View the review definition used for the review run
- View reviewers and decision statistics
- View review items and related activity
- Accept the review
- Enter comments for rejection and reject the review

NOTE: All decisions and run history are retained even if the review is rejected.

Usually, Identity Governance sends an email notification to the Review Auditor when a review run is waiting for acceptance. The Review Auditor can then log in and can review all details and **Accept** or **Reject** the review. Review Auditor must enter comments when rejecting a review.

3.3.9 Viewing Run History

Identity Governance tracks all the reviews, and maintains a history of previews and review runs associated with a review definition. The run history is searchable and sortable, and displays:

- Start and end date of a review run
- Status including certification percentage
- Review owner
- List of review items and associated actions including change reviewer and modify actions, and remove comments if any
- 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.

---

4 Instructions for Reviewers

This section provides information for individuals assigned the Reviewer authorization for a review run in Identity Governance. Reviewers confirm whether permissions or membership granted to a user or account should be kept or removed or, in some cases, modified. Reviewers can also confirm or request modification of supervisor assignments and user identity attributes such as title, email, and location.

4.1 Understanding Reviews

Identity Governance 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.

4.1.1 Understanding the Steps in a Review Run

In Identity Governance, 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 that the review runs start automatically in live mode based on the schedule. Also, live review runs can start automatically when certification or data policy violation remediation is set to micro certification.

Understanding the Steps in the 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 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 previews the emails notification templates and verifies that appropriate notifications are being sent to the correct recipients.

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 can download all or select review items as a CSV file to review it manually.

Understanding the Steps in the Live Review Run

When the owner initiates a review run in live mode, or when a review run starts by the schedule, or when a micro certification review is automatically started, the following activities occur:

1. Identity Governance generates tasks for the assigned Reviewers and notifies them as specified in the review definition.
2. Reviewers review their assigned set of review items and decide whether the items should be kept, modified, or removed. If a review item is assigned to multiple reviewers, the first reviewer who acts on that item becomes the decision-maker, and the item continues to the next phase of the review. For more information, see Section 4.2, “Performing a Review,” on page 27.
3. (Conditional) If the review definition specifies that a permission requires multiple stages of approval, Identity Governance forwards the affected review items to the next assigned reviewer.

   For example, the application owner, permission owner, or Review Owner might be required to review the permissions and confirm decisions before action is taken to remove any permissions. Reviewers must complete the review in the assigned order.
4. (Conditional) If a Reviewer does not complete tasks in the specified time frame and the review definition specifies an escalation process, Identity Governance forwards the tasks to the assigned Escalation Reviewer or the Review Owner.

   If there are multiple serial reviewers, Identity Governance forwards the task 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: If the review definition specifies it as allowed, Review Owners can override reviewer decisions at any point during a review run. When a Review Owner overrides a decision, the review item is locked and can no longer be modified by the reviewer.
6. Identity Governance initiates the fulfillment process to enable the requested changes.
7. (Conditional) In a manual fulfillment process, Identity Governance generates tasks that the assigned Fulfillers must complete and notifies them by email.
8. (Optional) An Auditor might be required to certify the results of the review run.

4.1.2 Understanding the Reviewer Authorization

Reviewers represent individuals who have the information and authority to determine whether assignments such as assigned permissions, reporting relationships, business role memberships, and user attribute values are correct. You might be assigned to review items in multiple active review runs. Depending on how the review is defined, Identity Governance might send you emails to remind you of incomplete tasks and approaching deadlines.

As a Reviewer, based on the review definition, you can perform any or all of the following tasks:

- Add, remove, or rearrange columns in reviews and review item displays
- Filter the list to show only incomplete review items

- Sort the review items by characteristics such as by user, permission, account, type, attribute, application, roles (technical and business), supervisor, 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 review items
- View activity for a review item
- Change the Reviewer of review items, individually or in a batch, if you do not have the information you need to confirm the assigned permissions
- Change supervisor and also change other identity attributes of an user
- Submit decisions for your tasks in the allotted time frame

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 Section 4.2, “Performing a Review,” on page 27.

4.2 Performing a Review

This section provides the steps required for you to complete Reviewer tasks associated with a review run. Usually, Identity Governance 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 Section 4.1, “Understanding Reviews,” on page 25.

1. In Identity Governance, select **Reviews**.
2. (Optional) Click the gear icon to view additional column options and customize column display. For example, you can drag **Started by** to the list of selected columns to view whether a review was started on demand, on schedule, or by micro certification remediation.
3. Select the review run on which you want to act.
4. (Optional) Adjust display options to help you manage your review items:
   - **4a** (Optional) Select **Include submitted items** to see all review items in the list.
   - **4b** Click **Show all** to see a list of grouping options. The grouping options are especially helpful when you have a long list of review items.
   - **4c** (Optional) Select a grouping option to sort review items by groups and to easily take action on all or selected review items within a group.
   - **4d** Click the gear icon to change display options by adding, removing, or rearranging columns.
5. For each review item, click the review item link to get help with making your decision and then select an action. Or select multiple review items and use **Actions** to select an action.

   NOTE: The review type and definition determines which of the following actions are allowed for a review instance.

   - (Conditional) **Keep** to specify that you believe that the user should have the permission, account, or role

- (Conditional) **Assign**, if there are unmapped accounts, to map the account
- (Conditional) **Modify,** if the review definition allows this option, to change attribute value or to provide modification instructions such as account needs an account custodian.
- (Conditional) **Keep assignment** to specify that the user should have the previously assigned supervisor when reviewing direct reports
- (Conditional) **Change supervisor** to specify that the user should have a different supervisor when reviewing direct reports
- (Conditional) **Remove assignment** to remove the supervisor when reviewing direct reports
- (Conditional) **Remove** to specify that you believe that the user should not have the permission, account, or role
- (Conditional) **Review user profile** to review user attribute values and either modify values and **Save changes** or confirm **No profile changes**

  NOTE: You cannot modify attributes values in bulk.

- **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, Identity Governance will issue a warning and disable the **Change Reviewer** option to prevent cyclical delegation.

6 Look over the changes to ensure accuracy.

7 Select **Submit** to confirm your actions on the review items.

  This action locks your decisions and moves the items out of your queue. Identity Governance then moves the items to the next reviewer's queue if this is a multistage review and you are not the last reviewer. If you are the last reviewer, Identity Governance notifies the Review Owner that the review is ready for certification.

  If one of your review items is in the **Multiple Reviewers** queues, your decision gets locked in when you **Submit** the decision. If you have not yet submitted a decision and another reviewer makes a decision and submits before you, it is the other reviewer's decision that gets locked. You can select **Include submitted items** if not previously selected and see the decision in the **View Activity** option.

4.3 Viewing Completed Reviews

Review Auditors can view the review instance after it is completed and is waiting on acceptance, and after accepting or rejecting the review instance. Reviewers and Review Owners can view the details of a review instance and review items even after the review instance is completed and, if required, accepted.

Select **Show completed reviews** to view a completed, and completed and accepted, or rejected review's start and end date, status including certification percentage, and review items that you submitted. Optionally, sort review items by decision, and select **View Activity** to view actions related to the review item, including change reviewer and modify reasons, if any.

5 Instructions for Fulfillers

This section provides information for individuals assigned the Fulfiller authorization in Identity Governance. Periodically, individuals in your organization participate in a review to determine whether permissions granted to user accounts should be kept or removed, whether user identity attributes should be kept or modified, whether users should be kept or removed as members of business roles, or whether supervisors assignments should be kept or changed. Individuals also calculate policy violations and request changes to mitigate policy violations. For each change, Identity Governance creates a task and routes it to a fulfillment target. When assigned to manually fulfill a change request, a fulfiller reviews the change request details and fulfills the change requests, declines the change request, or reassigns the task to another fulfiller.

5.1 Understanding the Fulfillment Process

Identity Governance collects information from a variety of identity and application data sources in your environment. It allows your organization to periodically review and verify that users have only the level of access that they need to do their jobs. The review process, requests for access, business role definition changes, and remediation of policy violations result in a list of changes, or **changeset**, that are then implemented. Identity Governance refers to the implementation process of a changeset as **fulfillment**.

5.1.1 Managing the Fulfillment Process

Fulfillment target configuration, application setup, and catalog update setup by the Global or Fulfillment Administrator drives how requested changes are fulfilled. The changes can be fulfilled manually, by a help desk service, or sent to Identity Manager, which automatically makes the changes or initiates external workflows. For manual fulfillment processes, the Global or Fulfillment administrator specify individuals or groups as fulfillers responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset.

Fulfillment Administrators also monitor the fulfillment process, and reassign manual fulfillment items if needed. Identity Governance provides the following status conditions for fulfillment items:

- Error or time out
- Fulfilled
- Pending fulfillment
- Verified
- Ignored
- Retry

When the fulfiller confirms the fulfillment activities, Identity Governance updates the status of the fulfillment item. After the administrator collects and publishes application sources, Identity Governance again updates the status of these fulfillment items. Global and Fulfillment Administrators and Auditors can access the Fulfillment Status page to view status of all fulfillment items. For more information about fulfillment targets and fulfillment status, see "Setting up Fulfillment Targets and Fulfilling Changesets" in the *NetIQ Identity Governance Administrator Guide*.

5.1.2 Understanding the Fulfiller Authorization

As part of the review, managers might change the permissions assigned to individuals in your organization. Access requests, business role definition, and user catalog 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 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 an item at the list level, including where the change request originated, and view additional details including potential SoD violations if any, attribute value or supervisor changes, and reason for the request by clicking on the task link
- Reassign your tasks to a different user
- Make the changes to the user account in the affected application
- Declare your tasks complete in Identity Governance

5.2 Performing Manual Fulfillment

Identity Governance sends an email notification when you have tasks in a review run based on your review definition. This section provides the steps required for you to complete Fulfiller tasks associated with a review run after receiving an email to manually fulfill a request.

For more information about your authorization and the review process, see Section 4.1, "Understanding Reviews," on page 25.

1. In Identity Governance, select **Requests** to view the fulfillment requests.
2. Change between tabs to see change requests generated from different actions.
3. (Conditional) If you have the Fulfillment Administrator authorization, access the **Fulfillment Errors** tab to see if there are any fulfillment errors. To resolve the errors:
   - **3a** Click **Fix** to go to the **Fulfillment Configuration** page.
   - **3b** Click **Application Setup**, view the settings for the application producing errors, and adjust the settings.
   - **3c** Go back to the **Fulfillment Requests** > **Fulfillment Errors** tab, and click **Retry** to route the item to the correct fulfiller.
   - **3d** If it is not possible to fix the problem, click **Terminate** to remove the change request item from the **Fulfillment Errors** tab.
4. Click the fulfillment task link on **the Access Request**, **Business Role**, or **Catalog** tab to expand the task description and determine the changes to be made, the reason for the change, and any potential SoD violations.

5 In the application affected by the requested change, modify the permission, user, account, or role according to the fulfillment task. This might impact the SoD policies or uncover unmapped users.

6 Manually fulfill the change request by making the requested changes in the indicated system.

7 Return to Identity Governance to specify one of the following outcomes for the fulfillment task:

- **Fulfilled** to indicate that you successfully completed the requested changes
- **Declined** to indicate that you refused to complete the requested changes
- **Reassign** to assign the fulfillment task to a different user

NOTE: For all of these outcomes, you can also enter comments explaining your action.

8 To complete your tasks, select **Submit**.

Manual fulfillment changes to the fulfillment request do not affect the Review run. Once you specify **Fulfilled** or **Declined** as an outcome, Identity Governance updates the Request status in the Request timeline and when a Review run is complete also updates the fulfillment status of the review item on the Review page.

9 (Conditional) If you have Fulfillment Administrator authorization, you can select **Fulfillment > Status** to view the status of fulfillment requests in the Fulfillment area. For more information, see "Understanding Fulfillment Status" in the *NetIQ Identity Governance Administrator Guide*.