Certifications and Access Reviews

Version: 8.3

Revised: April 2022

Copyright and Trademark Notices

Contents

Introduction to Certifications and Access Reviews

IdentityIQ™ helps you manage compliance by providing an automated way for designated reviewers to view and confirm or remove other users' access privileges, through a process called **certification**. IdentityIQ also lets you certify the contents and membership of roles and groups. Certifications like this are the central focus of compliance activities in an identity and access management program.

IdentityIQ uses certifications (or certification "campaigns") and access reviews to review and manage this user access.

Certifications

In IdentityIQ, the term "certification" or "certification campaign" refers to an overall campaign to review access for a selected set of users – that is, to create and then complete a set of access reviews. The certification campaign is usually the responsibility of a high-level authority on access, such as a compliance officer, administrator, or manager.

A certification defines what is being reviewed and for which users, who the reviewers will be, what the timeline for the reviews is, and other details. For example, a company's compliance officer may set up a quarterly certification campaign to review and certify all the sensitive financial systems the people in the Accounting department have access to, and require each manager in the Accounting department perform the access review for all the members of his or her team.

Access Reviews

The access review part of a certification is when someone who is an authority of some sort – such as a people manager, or someone responsible for an application like a Human Resources system or a financial database - reviews the access that other users have, to verify whether or not it is correct and appropriate, and to make any necessary corrections to revoke inappropriate access.

A certification campaign typically consists of multiple access reviews – for example, a Manager certification can create an individual access review for each department manager, so you have a single certification campaign that consists of a number of access reviews done by different people.

About Certifications

In IdentityIQ, certifications let you automate the review and approval of identity access privileges. In a certification, IdentityIQ collects fine-grained access or entitlement data, and formats the information into interactive reports, which are sent to the appropriate reviewers as access reviews. You can also use certifications to validate things like roles and account groups.

Certifications typically consist of multiple access reviews. For example, when you schedule a Manager Certification, a type of certification that asks managers to review and validate their direct reports' access, it will consist of an individual access review for each of the managers you choose to include as part of the campaign. However, it is possible to configure a certification such that it includes only one access review - for example, you might schedule a Manager Certification for just one specific manager, which means that there would only be one access review making up that certification.

When you configure the certification, you can set it up to annotate each access review with descriptive language that highlights changes, flags anomalies, and highlights where policy violations appear. The access reviews enable reviewers to:

- Approve access for identities
- Approve account group permissions and membership
- Approve role composition and membership
- Take corrective actions, such as revoking entitlements that violate policy
- Forward, reassign, or delegate all or part of the access review to another reviewer

For all corrective actions, IdentityIQ can fulfill certification revocations through automated or manual means, depending on the individual applications' connector configurations. IdentityIQ can also be configured to integrate with ticketing systems or other provisioning systems to fulfill provisioning requests.

The sections below will familiarize you with some terms and concepts related to certifications.

Certification Schedules

Certifications can be scheduled to run on a **periodic** basis; they can also be triggered by an **event**, or run as a **one-off** process.

Periodic Certifications

Periodic certifications are scheduled to run on a recurring basis, such as daily, weekly, monthly, quarterly, or annually. These periodic access reviews provide a snapshot view of the identities, roles, and account groups within your enterprise. Periodic certifications focus on the frequency at which entire entities (identities, roles, or account groups) must be certified.

A periodic certification is considered complete when *all* the access reviews contained within the certification have been completed. The access reviews that make up the certification, in turn, are considered complete when all items, such as roles, entitlements, violations, and application objects, have been acted upon, and those decisions are confirmed by the user to whom that access review was assigned.

Periodic certifications can be created using a multi-level sign-off structure, to allow multiple certifiers to review the access before the review is considered complete.

Event-Based Certifications

Certifications can be configured to run based on "trigger" events that occur within IdentityIQ. For example, you can configure IdentityIQ to automatically generate a certification any time an identity's manager changes. You can also

configure the events that trigger the certifications to meet the needs of your enterprise. See Certification Events for more information.

One-Off Certifications for Identities

One-off certifications can be created from the Identity Risk Score, Identity Search Results, or Policy Violation pages. These one-off access reviews can be run for a single identity, or for multiple identities at once. One-off certifications are most often used in special situations, such as when an access review is required outside of the normal certification cycle. You can also schedule standard IdentityIQ certifications to run on a one-off basis.

Types of Certification

IdentityIQ provides these types of certification:

Targeted Certifications

the most flexible type of certification, designed to meet most organizations' full range of certification needs from a single place. In a Targeted Certification you can certify role, entitlement, and account access for a narrowly defined set of your users. The Targeted Certification gives you a high level of flexibility in choosing which parameters to include in the certification (such as who, what, and when to certify).

Manager Certifications

certify that a manager's direct reports have the right entitlements they need to do their job, and no more than that. You can configure a Manager Certification to include all managers in the company, or only specific managers. You can also configure which applications you want to certify as part of the Manager Certification.

Application Owner Certifications

certify that all identities that have access to *applications* for which the reviewer is responsible have the proper entitlements.

Entitlement Owner Certifications

Certify that all identities that have access to *entitlements* for which the reviewer is responsible are correct.

Advanced Certifications

Certify entitlements and roles for all identities included in a specific population or group.

Account Group Membership Certifications

Certify that all accounts which make up an account group are correct - that is, are the right accounts in the account group. Account groups that do not have owners assigned are certified by the owner of the application on which they reside.

Account Group Permissions Certifications

Certify that all permissions that are granted to an account group for selected application(s) are correct. Account groups that do not have owners assigned are certified by the owner of the application on which they reside.

Role Membership Certifications

Certify that roles for which the reviewer is responsible are assigned to the correct identities.

Role Composition Certifications

Certify that roles for which the reviewer is responsible are composed of the proper permissions and entitlements.

Identity Certifications

This type of certification is used for “one-off” certifications that are launched from the Identity Risk Score, Identity Search Results, or Policy Violation pages. These certifications verify the entitlement information for the identities, typically for at-risk users.

Event-Based Certifications

Certify the entitlement information for the identities selected based on events detected within IdentityIQ.

Contents of a Certification: Policies, Roles, and Entitlements

These are some common terms that are used in certifications.

Policies

Policies govern access and can be defined for your enterprise. You can use certifications to monitor users that are in violation of those policies. For example, a separation-of-duties policy may dictate that one person can not both request and approve purchase orders, or an activity policy might dictate that a user with the Human Resource role should not be able to update the payroll application.

In access reviews, Policy Violations show any violations of policy for an identity. The access reviewer(s) must take action on these violations before the certification can be completed.

There is a Policy Violations page in IdentityIQ that is separate from the access review page. Policy violations can be viewed and acted upon from this page, or as part of another access review.

Decisions made on a violation that come from another page or review are displayed within the access review, below the summary information, or in the revocation dialog.

Roles

Roles are essentially collections of permissions. Through roles, system entitlements can be grouped together and presented as a logical unit, such as a job function, rather than as a detailed and often difficult-to-interpret list of access rights. Within IdentityIQ, users are granted permissions through the roles that are assigned to them, or through roles they inherit through a role hierarchy.

In an access review, only the top-level roles are displayed in the roles section. For example, if a role contains required and permitted roles, only the top-level role is displayed and the required and permitted roles are certified as part of that role. You can click on **Details** (in the three-line menu for the item) to expand the role information and view the role details and hierarchy. Both assigned and detected roles are displayed in the roles section.

If an identity has a role assigned to it multiple times - for example, to grant the same access to multiple accounts the user holds - that role is displayed multiple times, and each one must be reviewed and acted on individually.

Entitlements

Entitlements are either permissions, or specific values for an account attribute (such as group membership). In the context of certifications, entitlements refer to all the entitlements an identity has access to that are not included as part of a role that is assigned to the identity.

Certifications can also include IdentityIQ capabilities and scopes; if the certification includes capabilities and

scopes, these appear as additional entitlements on the IdentityIQ application, as Capabilities and Authorized Scopes attributes. Revoking these entitlements has auto-remediation enabled by default. This means that when the revocation is processed (either when the access review is signed, or immediately, based on the certification configuration) the capabilities and authorized scopes are removed from the identity.

For additional information, see Access Review Pages.

Challenges

When an access reviewer has determined that the user's access should be revoked, you may want to allow the affected user to challenge the decision - for example to share information with the reviewer about why they may need to retain the access in question. To allow users to challenge revocation decisions, you enable a **challenge period** as part of a certification's configuration. During the challenge period, if the certifier has revoked (for example) a user's Financial Reporting access, that user would get an email saying that the entitlement has been revoked; the user can then respond with comments on the item describing why they need to keep access to the Financial Reporting system. The certifier sees that the revocation has been challenged and why, and is able go back in to the access review and reconsider their decision.

For more information, see How to Challenge a Revocation Request.

Revocations

Revocation is when an identity's entitlements are altered in the source application, to remove any entitlements that were marked by the access reviewer as needing to be revoked. Depending on the provisioning features in use, remediations may be processed *manually* or *automatically*. If automatic provisioning is enabled in your system for the relevant application, revocation of access can happen without any further action from the reviewer, as a consequence of an access review decision. If the relevant application does not have automated provisioning enabled, then remediation of that application's entitlements is managed by the creation of manual work items for the Application Revoker or Application Owner, requesting that they change the identity's access or permissions manually. IdentityIQ alerts the Application Revoker or Application Owner about the manual work item via an email message.

A Revocation phase can be enabled for the certification as part of the certification setup. Note that remediation of access occurs as a result of revocations in an access review whether or not a Revocation period is enabled. The difference is that when a Revocation period is enabled, IdentityIQ *monitors* the status of remediation requests; when it is not enabled, remediation requests are submitted for processing but are not tracked.

The purpose of the revocation phase is for the work of revoking access to be done, according to the access revisions that have been made. This means that once a revocation has been processed, an access reviewer can not change their decision for that item.

Configuration settings in the certification setup determine when the revocation is processed.

- **Immediate Revocation**: If the **Process Revokes Immediately** option is selected, then revocation is considered to be processed as soon as a reviewer makes and saves a Revoke decision, and the decision can not be changed. Note that this does not affect Approve decisions; those can be changed even after saving, but if an Approve decision is change to Revoke and saved, it can no longer be changed.
- **Revocation during a revocation phase**: The revocation phase is entered when a certification is signed off, or when the active and challenge phases have ended. Until the certification enters this phase, reviewers can make changes to their approve and revoke decisions (unless the **Process Revokes Immediately** option described above was selected for the certification). **Once the certification is in this phase, reviewers can no longer change their decisions**.

Escalations and Reminders

When a person who has been assigned a manual work item for revoking access does not complete the work in a timely manner, IdentityIQ can send that person email reminders or can even escalate the work to the next level, such as to their manager. Revocation reminders and escalations are used only when revocation is being handled through manual work items assigned to the application's revoker or owner, and not when revocation is processed automatically.

The remediation parameters that are set in the certification configuration tell IdentityIQ what reminders and escalations to perform, and when.

Revocation reminder emails can be automatically sent to the person assigned the revocation work item if the work item is not completed within a specified timeframe. Reminders can configured to be sent once, or at scheduled intervals, beginning a specified number of days before the end of the Revocation period.

Escalations can also be automated to notify and transfer control to someone else (for example, the revoker's manager, or the application owner) if the person originally responsible for the revocation has not completed it, and the end of the Revocation period is near. Escalation triggers, email templates, and rules for determining who the item is escalated to are all part of the Certification configuration.

See Compliance Manager Setup for more information on configuring reminders and escalations.

Phases of a Certification

Certifications progress through phases as they move through their lifecycle. The phases associated with each certification are determined when the certification is set up. Some phases are part of every certification, while others are optional phases that can be configured as needed according to your organization's business processes.

Staging

This is an optional phase you can use to test or validate a certification before sending it to reviewers. The staging phase lets you create a certification and associated access reviews, but not send the access reviews to the certifiers. You can view what the certification schedule definition produces before the certification is activated. If the generated certification does not match your needs, you can cancel the certification and redefine it as needed. If the certification is accurate, you can activate it. If you want to use a staging period, you enable it as part of the certification's configuration parameters at the time you set up the certification.

Active

The active phase is the review period when the reviews are performed - that is, when all decisions that are required for the access review are made. During this phase, reviewers make decisions about access, and changes can be made to these decisions as frequently as required, until the access period expires. The active period lasts either for a scheduled amount of time, or until all the access reviews for the certification have been signed off. You can sign off on the active stage if no roles or entitlements were revoked, or if the optional challenge period has not been enabled. When you sign off on a periodic certification it enters either an end phase, or, if enabled, a revocation phase. To enter the revocation phase, the revocation period must be enabled, and at least one revocation decision must exist.

Challenge

The challenge phase is an optional period when users can challenge all revocation requests if any of their roles, entitlements, or account group access are being removed. When the challenge phase begins, a work item and email are sent to each user affected by a revocation decision. The notifications contain the details of the revocation request and any comments added by the reviewer. The affected user has the duration of the

challenge period to accept the loss of access, or challenge that decision. If you want to allow a challenge period, you enable it as part of the certification's configuration parameters at the time you set up the certification.

You can sign off on a certification in the challenge phase if all challenges are complete and no open decisions remain for the access review. When you sign off on an access review, it enters either the end phase, or, if enabled, the revocation phase. To enter the revocation phase, the revocation period must be enabled, and at least one revocation decision must exist.

Revocation

The revocation phase is the period when all revocation work is completed. When the revocation phase is entered, revocation can be done either automatically or manually. Automatic revocation can happen if your provisioning provider is configured for automatic revocation or if your implementation is configured to work with a help desk solution and a help ticket is generated. If you don't have an automatic revocation process enabled, revocation is done manually via work requests assigned to the relevant users in IdentityIQ. For periodic certifications, the revocation phase starts when a periodic certification is signed off, or when the active and challenge phases have ended.

Revocation activity is monitored to ensure that inappropriate access to roles and entitlements is revoked in a timely manner. Revocation completion status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily. You can view detailed revocation information by clicking the "information" icon in the access review then clicking the **Details** button on the information dialog. Revocation requests that are not acted upon during the revocation phase can be escalated as needed.

End

If a Revocation phase is not enabled for the certification, revocations can be done during the end period. The end period also indicated when the access review is complete.

Automatic Closing of Certifications

Automatic closing is an option you can enable in your certifications to handle access reviews that have not been completed by the time the certification's designated active period has ended. With automatic closing, you can automatically make decisions on the open line items – either to revoke, allow, or mark as an exception – or you can run a rule to perform more complex analyses or other actions.

If you choose to enable automatic closing, there are several configuration options you will set, including the amount of time to allow after the expiration date before automatic closing is invoked, any closing rule that will be run at that time, which action to take on uncompleted Access Review items, and any comment to add to each item for which the automatic action is taken. These can be set as global defaults and also can be set or changed from the global defaults at the individual certification level. See Compliance Manager Setup.

Rules in Certifications

Certifications can use rules to customize certification behavior. Rules enable you to insert your own logic to modify the behavior of the certification; for example, you could write a rule to exclude your executive management team from certifications, or to add an additional level of sign-off approval to an access review. Rules are written using BeanShell, a lightweight Java-based scripting language. IdentityIQ provides a standard set of example rules that you can import to use as starting points for developing your own rules, in an `examplerules.xml` file.

When you set up a certification, there are numerous places where you can choose rules to modify the certification's behavior. Every rule has a type that categorizes it, and in certifications, the rule type determines where and how in the

certification the rule can be used, and what kind of effect or purpose it has. Rules that are applicable to certifications are listed here, in the order in which they would be run in a certification.

Rule Types

User Interface Field Name	Rule Type	How/When Triggered	Effect/Purpose
Exclusion Rule	CertificationExclusion	Run as a part of the certification generation process	Excludes entitlements from the certification based on the rule's logic
Pre-delegation Rule	CertificationPreDelegation	Run as a part of the certification generation process	Automatically delegates access reviews based on the rule's logic
Who Do You Want to Certify Rule (Targeted Certifications Only)	CertificationScheduleEntitySelector	Run as a part of the certification generation process	Select identities to certify in a Targeted certification.
Group Factory: Certifier	Certifier	Run as a part of the Advanced certification generation process for Group Factory certifications	Assigns certifier for each group's access review
Active Period Enter Rule	CertificationPhaseChange	Run at the start of the Active period; the Active period is the period during which certifiers can examine their access reviews and make access decisions	Open-ended; depends on rule logic
Certification Escalation Rule	WorkItemEscalationRule	If the access review has not yet been finished and signed-off by the certifier at the time specified by the Escalation Trigger in the certification definition, this rule is run at that time	Transfers ownership of the access review to a different identity (often the certifier's manager or the certification owner)
Challenge Period Enter Rule	CertificationPhaseChange	Run at the start of the Challenge period (if enabled), which follows immediately	Open-ended; depends on rule logic

User Interface Field Name	Rule Type	How/When Triggered	Effect/Purpose
		after the Active Period ends; If Process Revokes Immediately is selected, Challenge period begins for each entitlement at the moment it is revoked and this rule runs once for each revocation	
Closing Rule	CertificationAutomaticClosing	Run according to the timeframe specified in the Automatic Closing configuration in the certification definition (after the end of the Active phase -- or Challenge phase if enabled)	Open-ended; depends on rule logic
Sign-off Approver Rule	CertificationSignOffApprover	Triggered by certifier sign-off on an access review	Transfers ownership of the access review to a next-level approver who needs to approve the certification decisions made by the certifier; this rule enables two-level (or multi-level) signoff on an access review Exception: When a challenge period is included, the sign-off approver can only override approval decisions; revocation decisions made by the original certifier and seen by the access holder in a challenge work item (whether they challenge the decision or not) will not be changeable in the sign-off approver's certification view.
Revocation Period Enter Rule	CertificationPhaseChange	Run at the start of the Revocation period; the Revocation period immediately follows the Active period (or the Challenge period if it is	Open-ended; depends on rule logic

User Interface Field Name	Rule Type	How/When Triggered	Effect/Purpose
		enabled)	
Revocation Escalation Rule	WorkItemEscalationRule	If the revocation work item has not yet been completed by the assigned revoker at the time specified by the Revocation Escalation Trigger in the certification definition, this rule is run at that time	Transfers ownership of the revocation to a different identity (often the revoker's manager or the application owner)
End Period Enter Rule	CertificationPhaseChange	Run at the beginning of the End period, which starts after all other periods configured for the certification are complete	Open-ended; depends on rule logic

Self-Certification

Self-certification means a user is allowed to be the certifier for his or her own access. Self-certification is often considered a security risk because it allows a user to approve and permit his or her own access, whether or not it is appropriate to his or her job. By default, IdentityIQ does not allow self-certification, other than for System Administrators. However, some organizations have business reasons for allowing self-certification, so there are configuration options to permit it. These can be set at the global level, or at the individual certification level.

Globally, self-certification options are set in the **gear menu > Compliance Manager** page's **Behavior** section. Global settings set the default configuration values for individual certifications, but these defaults can be changed when you configure individual certifications.

At the individual certification level, self-certification options are set on the **Advanced** page of the Certification configuration options for most types of certification; for Targeted certifications this option is set in the **Choose Certifier** section, under **Advanced Options**.

When allowing self-certification, you can choose who is allowed to self-certify: **All certifiers**, **System and Certification Administrators**, or **System Administrators only**. Which users are considered System Administrators or Certification Administrators is determined by the IdentityIQ capabilities the user has. Capabilities can be assigned directly to users, and also to workgroups. The "System Administrator" capability defines who is considered a System Administrator. For Certification Administrators, any IdentityIQ capability that includes the "CertifyAllCertifications" SPRight (such as the out-of-the-box "Certification Administrator" capability) defines the user or workgroup as a Certification Administrator, for purposes of being allowed to self-certify.

You can not configure IdentityIQ to exclude *all* users from self-certification, since excluding even your System Administrators from self-certifying can potentially lead to certifications that are impossible to complete.

When you allow users to self-certify, you can also choose an identity or workgroup to be the **Self Certification Violation Owner**. For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person. If a Self Certification Violation Owner is not chosen, any items that require self-certification will be shown as read-only to the reviewer in the access review.

About Access Reviews

The access review part of a certification is when someone who is an authority of some sort – such as a people manager, or someone responsible for an application like a Human Resources system or a financial database – reviews the access that other users have, to verify whether or not it is correct and appropriate, and to make any necessary corrections to revoke inappropriate access.

Customization of Access Reviews

IdentityIQ provides many ways to customization certifications and the access reviews that comprise them. These options control things like the actions a reviewer can take to correct an action, whether or not reviewers can process access decisions in bulk or only one by one, whether reviewers can delegate reviews to other people, et cetera. Since many access review options can be enabled or disabled when the certification is set up, reviewers may see only some of the features and options described in this section in their own access reviews.

Here are some examples of the customization options for access reviews, that can be set by the person who creates the certification:

- Requiring an electronic signature to close an access review
- Requiring comments when an access item is approved
- Enabling or disabling the option to delegate a review
- Limiting the number of times a review can be reassigned
- Enabling an exception period, to allow a user to retain access for a certain time period but no longer
- Allowing items to approved, revoked, or reassigned in bulk, versus item-by-item only

How Reviewers Are Notified About Access Reviews

Certifications can be configured to send an email notification to reviewers when the access reviews are available. An Access Review tile on the reviewer's home page also shows a count of how many reviews are awaiting the user's attention.

Whether or email notifications are sent, the access reviews themselves appear in the IdentityIQ user interface for the assigned reviewers, and can be accessed from these page or menu option paths:

- In the top navigation menu of IdentityIQ, click the **My Work > My Access Reviews** menu option.
- In the Quicklinks (left sidebar) menu, click the **My Tasks > Access Reviews** option.
- On the home page, click the Access Reviews tile.

How Access Review Items are Displayed: Important, Open, and Complete Tabs

The items for you to review are presented in a tabbed interface.

Important

The **Important** tab lists the access review items that require immediate attention. This includes policy violations, challenge items, and returned items. (Challenge items are items which the certifier revoked and the access holder has challenged the decision; returned items are items which have been delegated to someone else for input and have been rejected by that user and sent back to the certifier.) The Important tab appears only when any of your review items fall into the "important" category.

> If you do not have any review items that fall in the “Important” category, this tab will not appear in your Access Review listing. That means that some of your access reviews may show you an Important tab, and others may not.

Open

The **Open** tab shows access review items awaiting your attention, excluding any items listed on the Important tab.

Complete

The **Complete** tab shows the access review items that you have completed for this certification. You can change decisions from this tab, up until the point the access review has been completed and signed off.

Making Access Decisions

These are the decisions reviewers can make directly on an access review item:

Approve the access

When you approve access, you are indicating that it’s OK for this user to have this access. That means no action will be taken, and the user’s access will remain the same as it is now.

Revoke the access

When the reviewer revokes access, IdentityIQ will remove the access, in whatever way the system is configured to do it. It’s important to note that this revocation doesn’t necessarily happen immediately. This is another option that is configurable by the person who set up the certification. It can be set up so that revocation happens as soon as you make the decision, or it could be set up so that nothing is revoked until the entire certification campaign is complete is complete and signed off. If you’re unsure about when a revocation will take effect, you can check with the owner of the certification – which, remember, is something you can see on the main review page.

Revoke an account

Revoking an account is similar to revoking an individual entitlement or role, but it lets you revoke both the account and all the entitlements associated with the account, at once. This is one of the options that is configurable, so whether you have this option or not will depend on how the certification was set up.

Remediate a policy violation

There is a specific type of revoke option for **Separation of Duties policy violations**. This type of violation occurs when a user has two or more accesses that conflict with each other, in violation of a defined company policy. For example, your company may have a policy that says that one person can’t both approve vendors and make payments to them. For separation of duties policy violations, revoking access involves choosing which of the two conflicting accesses the user will keep, and which will be revoked.

Allow an exception for access

This is another configurable option that you may or may not have. What the “allow” option means is that you don’t want the user to have this access indefinitely, but you do want to allow the access for some particular period of time, after which you’ll revisit the access and potentially revoke it. A typical use case for this is when someone is on a temporary assignment and needs time-limited access to some system, or perhaps is transitioning between job responsibilities and will be losing access to a system or account at some known date in

the future. When you allow access, you're prompted to choose an ending date for the access. Allowing an exception is always an option on policy violation items in an access review, but only appears for other access review items if the certification is configured to include this option.

For separation-of-duties policy violations, allowing an exception marks the item as allowed for a specified duration, so any policy checking during that time will not re-flag the violation.

One of the options that your administrator or certification owner can configure is **sending email notifications when an exception period expires** – so keep in mind that it is up to the certification owner whether or not you will be alerted when an exception period expires.

Automatic Approvals

If you have implemented AI Services, you can enable automatic approvals of access based on recommendations. With this feature enabled, any access review item that has a recommendation of "thumbs up" is automatically moved from the reviewer's **Open** tab to the **Review** tab, with an "Approved" decision. Reviewers retain the option of changing the automated decision, as needed, before signing off on the review. Automated approvals help your reviewers process access reviews quickly and more efficiently by taking easy decisions out of the way so that they can focus on exceptional items. See the **AI Services** documentation for more information.

Item-by-Item versus Bulk Decisions

Review decisions can be made one at a time, or in bulk. The ability to decide on items in bulk is configurable; it can be turned off or on, both per certification, and globally.

If bulk processing is enabled for your review, you will see a **Bulk Decisions** button in the header area of your listing of items. To select the items you want to process in bulk, you can select them one by one using the checkboxes, or you can click in the header row to select either all the items on the current page, or all the items in the entire access review. You can deselect items in the same way.

Once you've chosen your items, click **Bulk Decisions** to approve, revoke, or allow.

Changing Decisions

Until you have signed off on the full review, you have the option to change the decisions you've saved. You can do this immediately when you make a decision, before saving it, by re-clicking the decision button or unchecking the decision from the flyout menu.

Once a decision has been saved, you can still go to the **Complete** tab and make changes there. Click the 3-line menu beside the item, then choose **Undo Decision** from the flyout menu.

Passing Access Reviews to Others

Sometimes you may need someone else's input on an access review, or you may even need someone else to handle the review entirely. There are three ways to pass a review along to someone else, and each involves different levels of ownership or responsibility both for you and for the person you pass it to. These options are all things that the system administrator or certification owner can configure, so your ability to use any of these methods in your review will depend on how the certification has been set up.

Delegating Reviews

When you delegate a review item to someone else, you are allowing that person make the decisions and return the item to you, so that you can review it, accept or change their decision, and then sign off. With delegation, the original reviewer still retains ultimate control of the decision and the sign-off.

When the certification owner sets up the certification, they can configure it so that you can delegate an entire identity, or so that you can delegate individual access items one by one.

When you delegate a review, you choose who to delegate it to, and can enter comments to explain why you have delegated or to give instructions. Delegated items are listed in your Open tab and are labeled as delegated. The 3-line menu gives you options for viewing any decisions made by the person you delegated to, as well as history, details, and comments.

Reassigning Reviews

Reassigning is different from delegating, in that reassigned items are no longer the responsibility of the original reviewer. The person the items are reassigned to assumes complete responsibility for all decisions on those items, and must sign off on those decisions themselves. However, the original owner of the overall access review (that is, the person doing the reassigning) typically still retains responsibility for making sure the person the items were reassigned to completed the review.

Reassigning is done through the **Bulk Decisions** menu, even if you only want to reassign one item. Depending on how the certification was configured, you can reassign the whole identity, a single line item, or a specific set of items in bulk. When you reassign items, they no longer appear in your own list of access review items.

The default behavior for a reassignment is that the person who reassigns the items cannot sign off on their own certification until the reassigned items are completed and signed off by the person you reassigned them to. This means that although you are no longer responsible for the decisions in the certification, you still retain responsibility for making sure the new reviewer completes their review. However, there is a configuration option in the Certification setup that lets you override this requirement, so that the original owner can sign off on his or her own reviews even if some or all of the reassigned items are still pending action.

Forwarding Reviews

Forwarding a review means you relinquish **all** responsibility for the access review. You can not retract it, or even see what activity has occurred in the review – you pass all responsibility to the new owner, including the ability to change any decisions you may have already made.

Forwarding is done at the overall review level, from the main access review listing. That is, you can forward an entire review, but you can't forward individual line items or identities within a review.

Automatic forwarding can be set up for an individual, or at the certification level, and is typically used in an out-of-office scenario. It may also be configured to make sure that certain users never get assigned reviews; for example, executives might forward all their reviews to an administrative assistant.

What Reviewers Can Do With Delegated, Reassigned, or Forwarded Reviews

Delegated Reviews

When you delegate a review item, the user you delegate it to can make decisions about access in the same way as you the original owner can. An important point about delegated items is that they show up for the new reviewer as a **work item** under the **My Work > Work Items** menu rather than in an access review. In the **Manage Work Items** listing, the reviewer clicks on the review to open the review page.

The user can make the same kinds of review decisions in the work items view as a reviewer might make in the Access Reviews view, for example they can approve, revoke, revoke account, and allow exceptions.

The reviewer can choose to decide on only some of the items you have delegated. Once they have made and saved their the decisions, they click **Complete** to save all their changes and enter comments. If the reviewer left any items

undecided when they click Complete, those will revert to you and will appear on your **Open** tab, for you to process. The items the delegated reviewer has decided on will appear in your **Complete** tab.

The person you delegate to also has the option to reject something that has been delegated. If someone rejects items you have delegated to them, those items will come back to you for review, and will revert to you and will appear in your **Important** tab.

The person you delegate can also forward the items to someone else for review. If this happens, you as the original owner will see an update in your review: you will see the name of the new owner as the delegate, rather than the name of the person you originally delegated it to.

Reassigned Reviews

Reassigned items appear to the new reviewer as new **Access Reviews** . The new reviewer can take actions on the review items in the same way as the original owner would have done, including delegating, forwarding, or reassigning the items to someone else. Certifications can be configured to limit the number of times each item can be reassigned. The default behavior for reassignments is that the original owner can not complete the sign-off of the main access review until the person who the items were reassigned to has completed, saved, and signed off on their decisions.

Forwarded Reviews

Forwarded reviews or review items become the full responsibility of the user they were forwarded to. The new owner processes these reviews in the same way as an original owner would, with all the same options. When a review or review items are forwarded, they can no longer be recalled or acted on in any way by the person who forwarded them.

Undoing Delegation and Reassignment of Reviews

Sometimes when you pass a review item or an entire review to someone else, you may need recall it for some reason. To recall a review:

- For **individual delegated items**, click the decision menu for an item and choose **Undo Decision**. When you undo a delegation, any decisions made by the person you delegated to are undone.

  > You can only undo individual line item delegation if the items were delegated individually. In other words, if you delegated an entire identity, you cannot recall items one by one. You will have to undo the delegation of the entire identity.

- If you have **delegated an entire identity**, you can go to the **List** view, and click the Undo arrow beside the identity you have delegated to undo the delegation. When you undo a delegation, any decisions made by the person you delegated to are undone.
- You can recall a **reassigned review**, to take ownership back from the person you reassigned to and return ownership to yourself. To recall a review that have been reassigned, click the **info icon** at the top of the review, then click **Additional Reviews**. This will show you all the items that have been reassigned. To recall the review, click the **Return** button and confirm that you want to return the item to yourself. You can also use the **Email** icon to send an email message to the reassigned reviewer.
- For **reassigned line items**, if the person you reassigned something to has made a decision, you can still undo or change the decision, until the reassignment owner has completely signed off on his or her review.
- **Forwarded items can not be recalled.** Once you forward something, you no longer have access to it, and can not recall it or edit it in any way.

Signing Off on Reviews

When decisions have been made for everything in your review, you can sign off on the review. Sign-off can not occur until *all* items in certification have been decided, including any delegated or reassigned items, unless the certification was specifically configured to allow it. Also, if a challenge period is enabled, sign off cannot occur until that period is complete.

A **blue** Sign-Off button means that all individual reviews for this overall access review are completed, and the entire review can now be marked as complete. A **red** Sign-Off button means that you have finished the items you are responsible for, but subordinate or reassigned reviews have not yet been completed.

Electronic Signatures

In cases when your organization wants to attach a legal significance to the certification sign-off process, the certification can be configured to require the use of electronic signatures. With electronic signatures, the certification owner can associate specific text with the sign off process, such as wording that pertains a regulation like a Sarbanes-Oxley requirement.

As a reviewer, you must re-authenticate using the login process configured for your organization, as part of signing off with an electronic signature.

For more information on configuring electronic signatures, see the **Electronic Signatures** section of the **IdentityIQ System Configuration** documentation.

Access Review Pages

The layout of the access review pages can be customized during the configuration of IdentityIQ. The organization of the pages can vary from the descriptions in this documentation, the function of the product should not be affected.

My Access Reviews

The My Access Reviews page lists all the access reviews assigned to you. How you access this page is determined by how your IdentityIQ instance is configured. It can be accessed through:

- The **Access Reviews** tile on your IdentityIQ home page.
- The **My Work > My Access Reviews** menu.
- The Quicklink (left navigation) menu, through **My Tasks > Access Reviews** or through a custom Quicklink menu your organization has configured.

From this page, you can click **Start** to begin the review; in-process reviews can be reopened by clicking **Continue**. Depending on how IdentityIQ is configured for your organization, you may also have options here to forward the review to another user. See Forwarding Reviews for more details.

This page includes:

- The name of the access review.
- A percentage progress wheel, showong how much of this review has been done so far.
- When the review is due.
- How many individual review items you have, and how many are completed.
- Who requested the review – this is the person who set up the certification.
- The phase the review is in. See Phases of a Certification for more information.

Access Review Details

Starting or opening an access review opens a page with detailed information about access, and options for making decisions. The layout and information will vary depending on the type of access review. See Types of Certification for more information.

Access Review Page Overview

Use this page to review access review requests. The information displayed on this page is dependent on the access review type and options selected at scheduling.

There are five access review types:

- Targeted — used for Targeted certifications
- Identity — used for Manager, Application Owner, and Advanced certifications
- Object — used for Entitlement Owner and Role Member certifications
- Role Composition — used for Role Composition certifications
- Account Group/Application Object — used for Account Group certifications

Only top-level roles are displayed as line items. For example, if a role contains required or permitted roles, those roles are certified as part of the top-level role in the same way that the entitlements that make up a role are certified with the role.

If an identity has a role assigned to it multiple times, that role is displayed multiple times and each one must be reviewed and acted on individually.

All of the access review detail pages include the following information, but it might display differently depending on the access review type:

Access Review Information

Displays the administrative and statistical information for the access review.

Filter

Enables you to filter the information displayed on the page.

Access Review Decision Tab

Displays the list of items that must be certified before this access review is Review. This list can contain entitlements, account groups, roles, or identities based on the access review type and the default settings of IdentityIQ.

See Access Review - Common Information for common terms and detailed information on access reviews.

Access Review - Common Information

This section provides information on the common access review information. This information is displayed differently for the different access review types, if it is available. This section also contains electronic signature information, if that feature is enabled.

This information is displayed on the information panel.

Due

The date on which this access review is due.

Owner

The identity to whom this access review is assigned.

Phase

The phase at this time and the date when this phase ends.

Revocations

This number reflects the fraction of revocation requests completed for this access review a compared to the total number requested. The revocation competition status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily.

Tags

Listed are any tags assigned to the certification when the certification was scheduled. Tags are used to classify certifications for searching and reporting purposes.

Review

You may be able to sign off an access review until all subordinate reviews are complete, based on how this certification was scheduled. Click **Additional Reviews** in the status panel to view the subordinate reviews associated with the one displayed. Click a subordinate access review to display the Access Review Decision page. See Subordinate Access Reviews.

A completion notice displays in the Access Review Information panel when all items and subordinate access reviews are in a complete state. Before IdentityIQ recognizes an access review as complete, you must click **Sign Off** and verify that certification is complete on the Sign off Access Review screen. Additional sign off information is required if your installation is configured to require an electronic signature.

Subordinate Access Reviews

Subordinate access review are any access reviews that must be completed before the top-level certification can be considered completed. Examples of subordinate access reviews can include any groups of identities that you reassign, or any lower-level, subordinate, manager access reviews. Lower-level manager access reviews can be created when Manager Certifications are scheduled and can be required as part of that process.

Subordinate access reviews are not displayed as part of the access review list and do not show as part of the completion status for this access review. When specified, subordinate access reviews must be in a complete state before the top-level certification can be signed off.

The **Access Reviews** link displays with the Access Review Decision page if subordinate access reviews exist. Click **Access Reviews** to expand a table containing the following information:

Column	Description
Name	The name and descriptive information about the top-level certification.
Owner	The current owner of the subordinate access review requests.
Percent Complete	The percentage of the subordinate access review that was acted upon and is in a complete state.
Open	The number of subordinate items that are still in the open state.
Completed	The number of subordinate items that are in the completed state.
Delegated	The number of subordinate items that the current owner delegated to different users.
Action	Click an icon to specify an action to take on the subordinate certification. **Return** — return the subordinate access review items to the review that generated the items and delete the subordinate access review. **Email** — generate an email to send to the owner of the original access review. **Forward** — forward the subordinate access review to a different, qualified certifier.

Targeted Access Reviews

The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined.

For detailed information on certifications and access reviews, see About Certifications.

For detailed information on completing an access review, see About Access Reviews.

Access Review Details - Targeted

This page is comprised of all roles, entitlements and policy violations that are part of this access review.

The page contains three tabs:

- **Important** — Contains items that require immediate attention, such as returned delegations.
- **Open** — All of the other access review items that have yet to be acted upon.
- **Review** — The items on which a decision has been made.

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Targeted Page Features

The following features are available for all of the tabs:

- List icon —click the icon to display a list of the identities that make up the access review.
- Download to CSV icon — click the icon to download the access review list to a CSV file.
- Information icon —click the information icon to get details about the access review, including due date, phase, and subordinate access reviews.
- Columns —add, remove, or rearrange the columns displayed on the page.
- Group By — rearrange the sort order of items on the page.
- Filter —use a filter to limit the items displayed.

> The recommendations icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ. See the **AI Services** documentation for more information.

- Recommendations — display the Decision Recommendation popup
- Bulk Decision button —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- Bulk select/deselect — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

> The Important tab is not displayed if no urgent issues exist.

Targeted - Important Tab

Column	Description
Policy Name	Name of the policy being violated.
Policy Description	Description of the policy being violated.
Rule	Specific rule that is being broken to cause the violation of the policy.
Owner	Owner of the policy.
Identity	Identity that is in violation.
Account Name	The account name for the application with which the item is associated and the account status, enabled or disabled.
Application	The application with which the item is associated.
Compensating Control	Any compensating controls associated the policy. For example, in some cases managers may be exempt for certain separation of duty policies.
Conflict	For separation of duties policy violations, the conflict that is causing the violation of the policy.
Description	Description of the violation from the Policy Configuration page.
Remediation Advice	Any correction advice associated with the policy. This advice is added when the policy is created.
Rule Description	The description of the rule that has been broken.
Changes Detected	This column flags any changes made to this access item for this identity, since the last time it was included in a certification *of this type*. For example, changes can be detected in an identity between one Manager certification and the next, but are not detected between a Manager certification and an Advanced certification for the same identity. Values can be: **No**: the item has been certified before. Once an identity has been certified, any item that was previously certified will show as No each time a subsequent certification *of this same type* is generated **Yes**: the item has not been certified. Once an identity has been certified, any new items that are detected the next time a certification *of this same type* is generated will have a **Yes** value. **New User**: this identity has never been certified, in a certification *of this type.*

Use the Decision column to **Allow** the violation, or click the menu icon to display additional options; Delegate, Comment, History, Details.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information by default. You can configure which columns appear on the Open tab by clicking the Columns button and adding, removing, or rearranging columns as needed.

Column	Description
Type	Role, entitlement, or account.
Display Name	The item name as it appears throughout the product.
Description	The description associated with the item.
Classifications	This column appears only if “Show Classifications” was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Application	The application with which the item is associated.
Account Name	The account name for the application with which the item is associated and the account status, enabled or disabled.
Identity	The identity associated with the role, entitlement, or account.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Click the recommendation icon for details about the recommendation. The recommendations icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ. See the AI Services documentation for more information.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the **Decision** column to change or undo a decision.

Click the automatic approval icon for details about the approval. The the automatic approval icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ.

See the **AI Services** documentation for more information.

How To Perform a Targeted Access Review

> The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

> Use Bulk Decisions to reassign items to another decision maker.

1. Access the targeted access review from the My Access Reviews page or directly from your Home page.
2. Select items individually and select an action in the Decision column.

   — OR —

   Select multiple items and select an action from Bulk Decision list.
3. Click **Save Decisions** to move the completed items to the Review tab.

   > Automatically approved items are displayed on the Review tab where you can accept the approval or change the decision as needed.
4. Review your decisions on the Review tab and make any required changes.
5. When all decisions have been made, click Sign-Off Decision to display the Sign Off on Certification dialog.

Manager, Application Owner, and Advanced Access Reviews

Access reviews for Manager, Application Owner, and Advanced Access Certifications share a common user interface. The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all identity list - type certifications.

For detailed information on certifications and access reviews, see About Certifications.

For detailed information on completing an access review, see Access Review Decisions/Operations.

Access Review Details - Identity List

The identity list is composed of all identities containing roles, entitlements and policy violations that are part of this access review.

The identity list page contains three tabs:

- **Important** — Contains items that require immediate attention, such as returned delegations.
- **Open** — All of the other access review items that have yet to be acted upon.
- **Review** — The items on which a decision has been made.

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Identity List Page Features

- The following features are available for all of the tabs:
- Identity list icon —click the icon to display a list of the identities that make up the access review.
- Download to CSV icon — click the icon to download the access review list to a CSV file.
- Information icon —click the information icon to get details about the access review, including due date, phase, and subordinate access reviews.
- Columns —Add, remove, or rearrange the columns displayed on the page.
- Group By —Rearrange the sort order of items on the page.
- Filter —Use a filter to limit the items displayed.

> The recommendations icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ. See the **AI Services** documentation for more information.

- Recommendations — display the Decision Recommendation popup
- Bulk Decision button —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- Bulk select/deselect — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

> The Important tab is not displayed if no violations exist.

Identity List - Important Tab

Column	Description
First Name	The first name associated with the identity that requires access review.
Last Name	The last name associated with the identity that requires access review.
Policy Name	The policy in violation.
Policy Description	Description of the policy.
Rule	The rule from the policy in violation.
Owner	The owner of the policy.
Account Name	The account name for the application with which the item is associated and the account status, enabled or disabled.
Application	The application with which the item is associated.
Compensating Control	Any compensating controls associated the policy. For example, in some cases managers may be exempt for certain separation of duty policies.
Conflict	For separation of duties policy violations, the conflict that is causing the violation of the policy.
Description	Description of the violation from the Policy Configuration page.
Remediation Advice	Any correction advice associated with the policy. This advice is added when the policy is created.
Rule Description	The description of the rule that has been broken.
Changes Detected	This column flags any changes made to this access item for this identity, since the last time it was included in a certification *of this type*. For example, changes can be detected in an identity between one Manager certification and the next, but are not detected between a Manager certification and an Advanced certification for the same identity. Values can be: **No**: the item has been certified before. Once an identity has been certified, any item that was previously certified will show as No each time a subsequent certification *of this same type* is generated **Yes**: the item has not been certified. Once an identity has been certified, any new items that are detected the next time a certification *of this same type* is generated will have a **Yes** value. **New User**: this identity has never been certified, in a certification *of this type.*

Use the Decision column to **Allow** the violation, or click the menu icon to display additional options; Delegate, Comment, History, Details.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Identity List - Open Tab

Column	Description
First Name	The first name associated with the identity that requires access review.
Last Name	The last name associated with the identity that requires access review.
Type	The type of item being certified, Role or Entitlement.
Display Name	The item name as it appears throughout the product.
Description	The description associated with the item.
Classifications	This column appears only if “Show Classifications” was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Application	The application with which the item is associated.
Account Name	The account name for the application with which the item is associated and the account status, enabled or disabled.
Account ID	The login ID of this identity on the application.
Risk Score	The risk score associated with this role or entitlement, for this identity.
Role Account Name	For roles, the name of the account.
Role Application	For roles, the application this role applies to.
Changes Detected	This column flags any changes made to this access item for this identity, since the last time it was included in a certification *of this type*. For example, changes can be detected in an identity between one Manager certification and the next, but are not detected between a Manager certification and an Advanced certification for the same identity. Values can be: **No**: the item has been certified before. Once an identity has been certified, any item that was previously certified will show as No each time a subsequent certification *of this same type* is generated **Yes**: the item has not been certified. Once an identity has been certified, any new items that are detected the next time a certification *of this same type* is generated will have a **Yes** value. **New User**: this identity has never been certified, in a certification *of this type.*

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Click the recommendation icon for details about the recommendation. The recommendations icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ.

See the **AI Services** documentation for more information.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

Click the automatic approval icon for details about the approval. The the automatic approval icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ.

See the **AI Services** documentation for more information.

How To Perform an Identity List Access Review

> The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

> Use Bulk Decisions to reassign items to another decision maker.

1. Access the identity list access review from the My Access Reviews page or directly from your Home page.
2. Select items individually and select an action in the Decision column.

   — OR —

   Select multiple items and select an action from Bulk Decision list.
3. Click **Save Decisions** to move the completed items to the Review tab.

   > Automatically approved items are displayed on the Review tab where you can accept the approval or change the decision as needed.
4. Review your decisions on the Review tab and make any required changes.
5. When all decisions have been made, click Sign-Off Decision to display the Sign Off on Certification dialog.

Role Membership and Entitlement Owner Access Reviews

Role Membership and Entitlement Owner access reviews share a common user interface. The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all object list - type certifications.

For detailed information on certifications and access reviews, see About Certifications.

For detailed information on completing an access review, see Access Review Decisions/Operations.

Access Review Details - Object List

The object list is composed of all roles or entitlements that are part of this access review.

The object list page contains three tabs:

- **Important** — Contains items that require immediate attention, such as returned delegations.
- **Open** — All of the other access review items that have yet to be acted upon.
- **Review** — The items on which a decision has been made.

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Object List Page Features

The following features are available for all of the tabs:

- **Object list icon** —click the icon to display a list of the items that make up the access review.
- **Download to CSV icon** — click the icon to download the access review list to a CSV file.
- **Information icon** —click the information icon to get details about the access review, including due date, owner, phase, number of completed items and revocations.
- **Columns** —Add, remove, or rearrange the columns displayed on the page.
- **Group By** —Rearrange the sort order of items on the page.
- **Filter** —Use a filter to limit the items displayed.
- **Bulk Decision button** —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- **Bulk select/deselect** — click the box on the header line and choose to select or deselect multiple items.

The recommendations icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ. Recommendations are not available on Entitlement Owner Certifications. See the **AI Services** documentation for more information.

- **Recommendations** — display the Decision Recommendation popup

Important Tab

The Important tab contains the following information:

> The Important tab is not displayed if no urgent issues exist.

Entitlement List - Important Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Display Name	The entitlement named used throughout IdentityIQ" />.
Attribute	The attribute with which the entitlement is associated.
Account Name	The name of the account with which the entitlement is associated.
Description	Description of the entitlement.
Return Comment	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated, or by the user from whom it was revoked.

Role Membership List - Important Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Role	The name of the role.
Description	Description of the role.
Classifications	For Role Membership reviews only. This column appears if “Show Classifications” was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Return Comment	Comments from the reviewer to whom the decision was delegated.
Role Application	The application with which the role is associated.
Decision	The decision made by the reviewer to whom the decision was delegated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Entitlement List - Open Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Display Name	The entitlement named used throughout IdentityIQ" />.
Attribute	The attribute with which the entitlement is associated.
Account Name	The name of the account with which the entitlement is associated.
Description	Description of the entitlement.

Role Membership List - Open Tab

Column	Description
First Name	The first name associated with the item that requires access review.
Last Name	The last name associated with the item that requires access review.
Role	The name of the role.
Description	Description of the role.
Classifications	For Role Membership reviews only. This column appears if “Show Classifications” was enabled for the certification. If an entitlement has classification data associated with it, to flag that the permission gives access to potentially sensitive or otherwise protected data, a classification icon appears in this column. Click the icon to see details about the classification.
Return Comment	Comments from the reviewer to whom the decision was delegated.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Click the recommendation icon for details about the recommendation. The recommendations icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ. Recommendations are not available on Entitlement Owner certifications.

See the **AI Services** documentation for more information.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

Click the automatic approval icon for details about the approval. The the automatic approval icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ.

See the **AI Services** documentation for more information.

How to Perform an Object List Access Review

> The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

> Use Bulk Decisions to reassign items to another decision maker.

1. Access the object list details from the My Access Reviews page or directly from your Home page.
2. Select items individually and select an action in the Decision column.

   — OR —

   Select multiple items and select an action from Bulk Decision list.
3. Click **Save Decisions** to move the completed items to the Review tab.

   > Automatically approved items are displayed on the Review tab where you can accept the approval or change the decision as needed.
4. Review your decisions on the Review tab and make any required changes.
5. When all decisions have been made, click Sign-Off Decision to display the Sign Off on Certification dialog.

Role Composition Access Reviews

The list is composed of all of the roles that make up this access review. This list is only available for Role Composition access reviews. The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all role composition list - type certifications.

For detailed information on certifications and access reviews, see About Certifications.

For detailed information on completing an access review, see Access Review Decisions/Operations.

Access Review Details - Role Composition List

The role composition list is composed of all roles that are part of this access review.

The object list page contains three tabs:

- **Important** — Contains items that require immediate attention, such as returned delegations.
- **Open** — All of the other access review items that have yet to be acted upon.
- **Review** — The items on which a decision has been made.

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Object List Page Features

The following features are available for all of the tabs:

- **Object list icon** —click the icon to display a list of the items that make up the access review.
- **Download to CSV icon** — click the icon to download the access review list to a CSV file.
- **Information icon** —click the information icon to get details about the access review, including due date, owner, phase, number of completed items and revocations.
- **Columns** —Add, remove, or rearrange the columns displayed on the page.
- **Group By** —Rearrange the sort order of items on the page.
- **Filter** —Use a filter to limit the items displayed.
- **Bulk Decision button** —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- **Bulk select/deselect** — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

> The Important tab is not displayed if no urgent issues exist.

Role Composition List - Important Tab

Column	Description
Role	The name of the role with which this item is associated.
Name	The name of the line item being reviewed.
Type	The type of role or entitlement profile.
Description	Description of the role.
Application	The application associated with this item, if appropriate.
Return Comments	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Column	Description
Name	The name of the role or the individual line items contained within.
Type	The type of role or entitlement profile.
Description	Description of the role.
Application	The application associated with this item, if appropriate.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

How to Perform a Role Composition Access Review

> The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

> Use Bulk Decisions to reassign items to another decision maker.

1. Access the access review details page from the My Access Reviews page or directly from your Home page.
2. Click an item to display the detailed role information.
3. Take action on individual items.

   — OR —

   Use the select boxes and select an action from Bulk Decision list.

4. Click **Save Decisions**.
5. When all decisions have been made, click **Sign-Off Decisions** to display the Sign Off on Certification dialog.

Account Group Membership and Account Group Permission Access Reviews

The access review might look different in your instance of IdentityIQ depending on the configuration and the options selected when the certification was defined. These are all account group list - type certifications.

For detailed information on certifications and access reviews, see About Certifications.

For detailed information on completing an access review, see Access Review Decisions/Operations.

Access Review Details - Account Group List

The list is composed of all of the account groups, application objects, that make up this access review.

The object list page contains three tabs:

- **Important** — Contains items that require immediate attention, such as returned delegations.
- **Open** — All of the other access review items that have yet to be acted upon.
- **Review** — The items on which a decision has been made.

By default the page opens with the Important tab displayed, if there are issues that require immediate action.

Object List Page Features

The following features are available for all of the tabs:

- **Object list icon** —click the icon to display a list of the items that make up the access review.
- **Download to CSV icon** — click the icon to download the access review list to a CSV file.
- **Information icon** —click the information icon to get details about the access review, including due date, owner, phase, number of completed items and revocations.
- **Columns** —Add, remove, or rearrange the columns displayed on the page.
- **Group By** —Rearrange the sort order of items on the page.
- **Filter** —Use a filter to limit the items displayed.
- **Bulk Decision button** —make the same decision for multiple items. If only one action is applicable, that action appears on the button.
- **Bulk select/deselect** — click the box on the header line and choose to select or deselect multiple items.

Important Tab

The Important tab contains the following information:

> The Important tab is not displayed if no urgent issues exist.

Account Group Permissions List - Important Tab

Column	Description
Account Group	The account group name.

Column	Description
Type	The type of the account group.
Description	Description of the account group.
Attribute	The attribute associated with this account group.
Entitlements	Any entitlements associated with the account group.
Return Comment	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated.

Account Group Membership List - Important Tab

Column	Description
First Name	The first name of the account group member.
Last Name	The last name of the account group member.
Type	The type of the account group.
Description	Description of the account group.
Return Comments	Any comments associated with this item.
Decision	The decision made by the reviewer to whom this item was delegated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use **Reassign** to reassign the policy violation decision to another user.

The Open Tab

The Open tab contains the following information:

Account Group Permissions List - Open Tab

Column	Description
Account Group	The account group name.
Type	The type of the account group.
Description	Description of the account group.
Attribute	The attribute associated with this account group.
Entitlements	Any entitlements associated with the account group.

Account Group Membership List - Open Tab

Column	Description
First Name	The first name of the account group member.

Column	Description
Last Name	The last name of the account group member.
Type	The type of the account group.
Account	The name of the account associated with this member.
Description	Description of the account group.

Use the Decision column to **Approve** or **Revoke** the item, or click the menu icon to display additional options; Allow, Delegate, Revoke Account, Comment, History, Account Details.

Revoking an account affects all role or entitlements with which it is associated.

Delegated items are still part of this access review and must be acted upon before it is complete.

Use the **Bulk Decisions** to make decision for multiple items or reassign items to another decision maker.

Review Tab

The Review tab contains all of the items upon which a decision has been made. Click the menu icon in the Decision column to change or undo a decision.

How to Perform an Account Group Access Review

> The options available in an access review are dependent on the configuration of IdentityIQ and the option defined when the certification was scheduled.

> Use Bulk Decisions to reassign items to another decision maker.

1. Access the access review details page from the My Access Reviews page or directly from your Home page.
2. Take action on individual items.

   — OR —

   Use the select boxes and select an action from Bulk Decision list.
3. Click **Save Decisions**.
4. When all decisions have been made, click **Sign-Off** Decision to display the Sign Off on Certification dialog.

Access Review Decisions/Operations

> The terms account group and application object are use interchangeably in this document but have the same meaning. Some applications can have multiple application objects. An account group can be the name of one of those objects.

There are many ways to move through the IdentityIQ application. As you become familiar with IdentityIQ, you can configure the product to fit the functions of your job. To take action, you must be the owner or delegated approver of an access review. You might be able to view another user's access review; however, the reviews are read-only files.

> System Administrators and Certification Administrators can take action on all access review items whether they own the certification or not.

Basic Access Review Procedure

Access Reviews are performed from the Access Review Page Overview page.

1. Go to your My Access Review page.
2. Perform one of the following actions on each item included in the Access Review Request:

   > Not all of the decision options are available at all times.

   - Reassign — See Reassign Access Reviews.
   - Approve — Approve Access Reviews
   - Delegate — Delegate Access Reviews
   - Allow Exception — Allow Exceptions on Access Reviews
   - Revoke or Edit Access — Revoke or Edit Access From Access Reviews
   - Revoke Account — Revoke an Account on Access Reviews
   - Allow Violation — Allow Policy Violations on Access Reviews
3. Save your changes. Any decision made on the Access Review Details page or the Decisions tab must be saved before to moving to a different page. A warning prompts for any unsaved changes.

   Decisions are not committed at this point, however, and can still be changed before the access review is signed off on.

   > Changing the decisions might revoke one or more line item delegations. Any changes made during the delegation will be lost.
4. Sign off a periodic certification task before it is overdue.

   > All items must be in the complete state before the sign off option is available.

   You must sign off a periodic certification before it is considered complete. Click **Sign Off** on the Access Review Details page and select **Finish** on the Sign Off Access Review screen.

If the challenge period for revocations is active, you cannot sign off an access review until one of the following conditions is met:

- All items are complete and the challenge period is not active or no revocation decisions were made.
- The access review is in the challenge phase and all items are completed and any revocation decisions have progressed through the challenge procedure.
- The challenge period has expired.

5. OPTIONAL: If an electronic signature is required, you must authenticate in order to complete the electronic signature. Electronic signature requirements are configured when the certification is scheduled. Use the same credentials for the electronic signature that you use to sign in to IdentityIQ.

Access Review Decisions

Perform one of the following actions on each item included in the Access Review Request:

> Not all of the decision options are available at all times.

- Reassign — See Reassign Access Reviews
- Approve — See Approve Access Reviews
- Delegate — See Delegate Access Reviews
- Allow Exception — See Allow Exceptions on Access Reviews
- Revoke or Edit Access — See Revoke or Edit Access From Access Reviews
- Revoke Account — See Revoke an Account on Access Reviews
- Allow Violation — See Allow Policy Violations on Access Reviews

Reassign Access Reviews

You can reassign items individually or use:

- Bulk reassignment to reduce access review lists. For example, if you are the assigned approver of an application with thousands of identities, you can use this feature to reassign identities by department or manager.
- Automatic reassignment or forwarding of all access reviews assigned to you. You can use the Forwarding User field on the Edit Preferences page. If you select a forwarding user, all work items including access review requests are sent to that user.

When you choose to reassign you will see the Reassign Items dialog.

Enter the following information in the reassignment dialog.

Recipient

Type the full name of the approver to whom you are reassigning this work item. The recipient can be an identity or a workgroup. Typing the first few letters of a name displays a pop-up menu of IdentityIQ users and workgroups with names containing that letter string. Click the arrow next to the field to display all users.

— OR —

Select an assignee from the drop-down menu. The drop-down menu can contain options such as assign to self, assign to manager, or assign to application owner.

Description

(optional) A brief description of the item being reassigned.

Comment

(optional) Any additional information needed.

Click **Reassign** to reassign the item and return to the Access Review Details page.

The Percentage complete bar is updated to show the changes and the selected items are removed from the list and do not show as part of the completion status for this access review. If configured, all reassigned items must be acted upon before you can sign-off a periodic certification.

Approve Access Reviews

You cannot approve policy violations. Warning messages are displayed if you attempt to include policy violations when performing an approval.

If provisioning is enabled from the access review pages and you approve a role that contains required roles to which the identity does not have access, a dialog displays enabling you to request provisioning for those roles. If you perform a bulk approval, this function is overwritten and the roles are approved in their current state.

If you perform bulk approval and the access review has missing roles, you do not have the option to provision required roles. The provisioning function is only available if you approve roles individually and provisioning is enabled for this access review.

If the provisioning dialog displays, review the missing information and make a provisioning decision.

If you choose to request that the missing roles be added, you must select a recipient for the request and click **Provision Required Roles** again. The recipient you specify is used if automatic provisioning is not configured or there is no default remediator for the application. Or click **Do Not Provision** and return to the access review page.

When you perform an approve at the top level you are approving all of the items that are included in the identity, role, entitlement, or account group/application object. Access Reviews performed at this level are logged for auditing purposes.

Delegate Access Reviews

Delegation can be performed automatically based on rules specified when the certification request is generated. Items delegated automatically display in the access review details and behave exactly like items delegated manually.

The Enable Line Item Delegation option must be selected when the certification was created to delegate certification items from the Access Review Details page.

Type the following information in the **Delegate Access Review** dialog.

Recipient

Type the full name of the approver to whom you are delegating this work item. The recipient can be an identity or a workgroup. Typing the first few letters of a name displays a pop-up menu of IdentityIQ users and workgroups with names containing that letter string.

Description

A description of the work item being delegated. You can edit the description as required.

Comment

(optional) any additional information needed for this delegation.

Changing the decisions may revoke one or more line item delegations. Any changes made during the delegation that be lost.

You cannot delegate account groups from the account group list.

When you delegate at the top level you are also delegating all of the items that are included in the identity or role.

Allow Exceptions on Access Reviews

> This option is only available if it was turned on in the global settings at the time of your configuration.

Use **Allow Exception** to put an expiration date on access to a particular entitlement, role, or account group. For example, if one employee must temporarily assume the duties of another during a vacation, you can allow them access to that role for the length of the vacation.

Decisions made in access reviews are shown on the Policy Violations page for the affected policy violation.

Allow exceptions on individual items that make up the identity.

Type the following information in the **Allow Exception** dialog.

Expiration

Manually type an expiration date, or click the icon and select a date.
A 4-digit year is required if you type the date manually. For example, mm/dd/yyyy.

Comment

(Optional) Any additional information needed for this exception.

Revoke or Edit Access From Access Reviews

This section information on the follow:

- Request the removal of an identity access to a specified role or entitlement
- Remove a permission of member from an account group
- Remove access to a managed entitlement from an identity
- Remove a profile or included role from a role
- Edit the values of specific entitlement attributes or permission on identity-type access reviews

> Entitlements must be configured on the application to enable editing from the access review pages.

For revocation on individual roles, if a role contains required or permitted roles that are not used in any other roles for this identity, a dialog displays enabling you to make revocation decision on each of those included roles. By default all included roles, that are not used in other roles for this identity, are marked for removal. If you perform bulk revocation this function is overwritten.

On periodic access reviews, by default, no action is taken on a revocation request until the access review containing this item is signed off or the challenge period expires, if the challenge period is active. This is done to ensure that no entitlement is removed until final confirmation is received from the requestor. This default behavior can be overwritten when the access review schedule is created.

Revocation is done automatically if your provisioning provider is configured for automatic revocation through help ticket generation or if your implementation is configured to work with a help desk solution. Without the automatic configurations, revocations are done manually using a work request assigned to a IdentityIQ user or workgroup. If an access review requires that multiple revocation requests be sent to the same IdentityIQ user or workgroup they are rolled up into one work item.

For identity-type access reviews, the revocation process can also include the challenge and revocation periods. The challenge phase is the period during which all revocation requests can be challenged by the user from whom the role or entitlement is being removed or modified. The revocation phase is the period during which all revocation work must be completed. The revocation phase is entered when an access review is signed off or when the active and challenge phases have ended.

Type the following information in the revocation dialog and click **Revoke**.

> This dialog is not displayed if a default revoker was specified as part of the IdentityIQ configuration.

Recipient

Type the full name of the revoker to whom you are assigning this work item. The recipient can be an identity or a workgroup. Typing the first few letters of a name displays a pop-up menu of IdentityIQ users and workgroups with names containing that letter string.
If automatic remediation is enabled or a default revoker was specified for the application to which the entitlements are associated, the recipient specified here is overwritten.

Comment

(Optional) Any additional information needed for this revocation.

Edit Revocation Details

Only available if the entitlement is configured for modification. One line displays for each entitlement contained in this revocation request.
Operation — select the operation to perform, Remove or Modify.
Attribute — attribute name that the attribute or permission is associated.
Value — if are modifying the entitlement, select or type the new value.
Application — application to which the entitlement is associated.
Account ID — login ID of this identity on the application specified.

Revoke an Account on Access Reviews

When you select **Revoke Account** for one entitlement, all other entitlements associated with the same account for the item being certified are marked for revocation.

On periodic certifications, by default, no action is taken on a revocation request until the certification containing the account is signed off or the challenge period expires, if the challenge period is active. This is done to ensure that no account is removed until final confirmation is received from the requestor. When the certification schedule is created, this default behavior can be overwritten allowing revocation requests to be processed immediately.

Revocation is done automatically if your provisioning provider is configured for automatic revocation through help ticket generation or if your implementation is configured to work with a help desk solution. Without the automatic configurations, revocations are done manually using a work request assigned to a IdentityIQ user or workgroup. If a certification requires that multiple revocation requests be sent to the same IdentityIQ user or workgroup they are rolled up into one work item.

For identity-type certifications, the revocation process can also include the challenge and revocation periods. The challenge phase is the period during which all revocation requests can be challenged by the user from which the account is being removed. The revocation phase is the period during which all revocation work must be completed. The revocation phase is entered when a certification is signed off or when the active and challenge phases have ended.

Respond to a Challenged Revocation

For identity- type certifications, the revocation process can include the challenge and revocation periods. The challenge phase is the period when a user whose role or entitlements are being removed can challenge those revocation requests.

When a revocation request is challenged, the status of the item associated with the revocation request displays as **Challenged**. You must take action on all challenged revocations before a certification is complete.

From the **Challenge Decision** drop-down menu select either **Accept** or **Reject**.

All comments are kept with the certification item and can be viewed below the certification decision information for that item. Click **comments** to view the comments added by the challenger and **accepted/rejected** to view the comments associated with the decision.

Based on your decision one of the following occurs:

Reject

The revocation process proceeds as normal when the certification is signed off or the challenge period ends.

Accept

The item is moved to the open status and you must make another certification decision.

Allow Policy Violations on Access Reviews

Do this to allow an identity to retain conflicting roles, accounts, or entitlements for a specific period of time. For example, if one employee must temporarily assume the duties of another, you can allow them access to a role that creates a policy violation for the length of the vacation.

To display detailed information about the policy, click the violation name on the Decisions tab.

Type the following information in the **Allow Violation** dialog.

Expiration

Manually type an expiration date, or click the **"..."** icon and select a date.
A 4-digit year is required if you type the date manually. For example, mm/dd/yyyy.

Comment

(Optional) Any additional information needed for this exception.

How to Complete Access Review Work Items

The following procedures list the steps to complete Access Review work items that were originally assigned to a different approver, but now require you, as a member of the workgroup, or the other members of a workgroup to take action. Access review work items include items that were delegated, reassigned, forwarded, require your approval, or require you to take revocation actions.

How to Complete Delegated Access Reviews

You can complete delegated access reviews items from access reviews that were assigned to a different certifier that the original approver delegated to you. For example, if an employee does work for you but reports to a different manager, that manager might not be familiar with all of the entitlements or roles listed in the employee's Identity Cube.

To display the Manage Work Item page, click a delegation work item.

Required Authorization

To take action on a delegated work item, you must be the owner of that work item.

> A System Administrator or Certification Administrator can also take action on work items.

Complete Delegated Access Reviews

1. Open a delegated work item.
2. Review the work item information in the Summary section.
3. Review the Comments section for any information associated with this work item. Use the **Add Comment** button to add additional information to the work item.
4. Make an access review decision on each item listed for the identity. See Making Access Decisions for detailed information.
5. Click **Complete** to display the **Completion Comments** dialog and mark the work item as complete.

> If your deployment is configured to require a decision on each item in the work item before it is marked complete and you do not take action on all items in the work item, an alert displays when you attempt to complete a work item.

Delegation Review - Optional

If the access review was originally configured to require a delegation review, you can perform this review after the delegate completes their portion of the access review. The items awaiting review are listed on the **Important** tab of the access review.

1. In the access review, click the **Important** tab. Delegated items that have been completed and are awaiting review are listed in the **Returned Items** section.
2. To view the comments of the delegated decision maker, click the three-line menu and choose **History**,

3. Click **Agree** to accept the delegated decision; if you don't accept the delegated decision, you can override the delegated decision with any of the available options (Revoke, Revoke Account, Allow, etc.). You can also delegate the line item again.

> If the identity who originally delegated the work item overrides a delegated decision, an audit shows the delegation of the work item was never assigned.

How to Complete Revocation Work Items

You can confirm that you have completed the requested revocation. Revocation requests are sent after the access review for the associated item is completed and signed off or when the access review enters the challenge phase, if the challenge period feature is active. This process ensures that nothing is removed until the final decision is made on the access review. When you click **Complete** on this work item, you are stating that you acted on the revocation request.

Required Authorization

You must have authorization on the specified application to perform the required revocation.

> A System Administrator or Certification Administrator can also take action on work items.

Complete Revocation Work Items

1. Select a revocation work item to display the Manage Work Item page.
2. Review the work item information in the Summary section.
3. Review the Comments section for any information associated with this work item.

   Use the **Add Comment** button to add additional information to the work item if necessary.
4. Review and perform the operations necessary to revoke the privileges specified.

   Click a line item to view the details of the revocation request for that item.
   The revocation of application privileges is not performed as part of IdentityIQ. The revocation is performed on the specific application from which the entitlements are to be removed. For information on how to remove entitlements, refer to the documentation associated with the specific application
5. If this work item was assigned to a workgroup, use the **Assign Selected Items** button to assign specific revocation requests to members of that workgroup. The name of the workgroup member is displayed in the Assignee column.
   Any member of the workgroup can change the assignee status.
6. Click **Complete** to display the **Completion Comments** dialog and mark the work item as complete.
   — OR —
   If there are multiple revocation requests in the work item, you can select multiple revocations and use the **Mark Revocation Complete** button to mark complete. Alternatively, you can click on the revocation item and complete each item individually.

How to Complete Reassigned or Forwarded Access Reviews

You can reassign or forward access reviews. Reassigned work items are designated as reassigned in the Description columns on pages on which they are displayed. Forwarded work item descriptions maintain the name of the original owner or the name of the application to which the access review applies.

You use the same procedure to complete access reviews that were reassigned or forwarded to you that you use for access reviews that were originally assigned to you. See Access Review Decisions/Operations.

How to Perform Multi-Level Sign Off on Access Reviews

You can perform multi-level sign-off access reviews that require more than one person to review before sign off. Multi-level sign-off access reviews are access reviews that an assigned certifier completed and signed off and require other users to review before the access reviews are complete. When an access review is assigned to you for additional sign off, you receive an email notification and the access review request is sent to you.

You can access the access review request the same way as any other access review, make changes or add comments as required, and click **Sign Off** when you are finished.

After you sign off, the multi-level sign off rule runs again to determine if the access review is complete or if additional sign off actions are required. This process is repeated until the rule determines that no further sign-off actions are required for the access review.

How to Challenge a Revocation Request

The challenge phase is the period when the user whose role or entitlement is being removed, can challenge all revocation requests.

For identity-type access reviews, the revocation process can include the challenge and revocation periods.

If a role or entitlement is removed from your Identity Cube, you are assigned a work item that enables you to accept or challenge the revocation.

To accept the revocation, do not respond to this challenge work item.

To challenge the revocation request, type your reasons for the challenge in the **Reason for Challenge** field and click **Challenge**. Or click **Cancel** to close the work item without taking action.

Certification Events

Certifications can be configured to run based on events that occur within IdentityIQ. For example, an event-based certification might be configured to run when a manager change is detected for an identity and for that certification request to be sent to the newly assigned manager. The events that trigger the certifications can be configured to meet the needs of your enterprise.

Use the Certification Event tab to configure events within your enterprise to trigger the creation and assignment of certification requests. Event-based certifications are launched when changes are detected during an identity refresh.

To access the Certification Events panel, click the **Setup** tab and select **Certifications.** On the Certifications page click the **Certification Events** tab. Click an existing certification event to view the details defined when it was created. Click **New Certification Event** to display the certification event configuration panel. See Define a Certification Event.

The Certifications Events tab contains the following information:

Column	Description
Name	The name assigned when the certification event was created. This name is used to identify the certification event. This name is not displayed in the certifications that are created when this event is triggered.
Type	The event type associated with this certification event.
Attribute Name	The attribute specified in attribute change type certification events.
Owner	The user that created the event certification.
Disabled	Indicates whether or not the certification event is enabled.

Define a Certification Event

To schedule a certification from a certifying event, you make decisions on the Basic, Lifecycle, Notifications, and Advanced tabs. The left panel provides a summary and descriptions of the tabs. To move through the scheduling process, select a tab in the Summary panel or click **Next** at the bottom of the page. You do not have to move through the tabs in order.

When a Certification Event is set up, all certifications for that event are listed in the same certification group on the Setup > Certifications page.

> Event certifications are generated as Identity certifications and are displayed as such. To separate Event certifications from other Identity certifications use the Custom Name and Custom Short name options on the Advanced panel.

To schedule a non-event certification, see the Certification Schedules Tab.

These are fields on the Event Certification panels:

Field Name	Description
Basic These options specify what and when to certify and who is responsible for performing the access reviews.	
Name	Assign a descriptive name for the event certification. This name is used to identify the event certification. This name is not displayed in the certification requests that are created when an event is triggered.
Description	Add a brief description of the certification event.
Event Type	Specify an event-type or rule to associate with the certification. **Create** - launch a certification when a new identity is discovered. **Manager Transfer** - launch a certification when an identity's manager changes. **Attribute Change** - launch a certification when a change is detected for the specified attribute. **Rule** - use a rule to determine when certifications are launched. **Native Change** - launch a certification when a change is detected on a native application. **Alert** - launch a certification when an alert is triggered within your enterprise
Previous Manager Filter	For Manager Transfer event certification types only: Certifications are launched if identities are transferred from the specified manager. If no manager is specified, all managers are included.
New Manager Filter	For Manager Transfer event certification types only: Certifications are launched if identities are transferred to the specified manager. If no manager is specified, all managers are included.
Attribute	For Attribute Change event certifications types only: Select the identity attribute to associate with the event certification. The attribute drop-down list contains all of the standard and extended identity attributes configured in your deployment of IdentityIQ.
Previous Value Filter	For Attribute Change event certification types only: Certifications are launched if the attribute value specified has changed. If no value is specified, all values are included.
New Value Filter	For Attribute Change event certification event types only: Certifications are launched if the attribute value specified was newly assigned. If no value is specified, all values are included.

Field Name	Description
Rule	For Rule event certification types only: Select the event certification rule used to launch certifications. Rules are created as part of the configuration process of IdentityIQ.
Disabled	Select to specify that a lifecycle event should not be processed.
Included Identities	Specifies which identities to include when detecting this lifecycle event. Select one of the following filter types to narrow your selection: **Match List** — a list of attributes and permissions on selected applications. **Filter** — a custom database query for role creation. **Script** — a custom script for role creation. **Rule** — select an existing rule from the drop-down list. Click the "..." icon to launch the Rule Editor to make changes to your rules if needed. **Population** — select an existing population of identities to include.
Threshold Type	To use an Identity Processing Threshold to stop lifecycle events before they are fully processed, in case of accidentally-triggered workflows, choose from **Fixed** or **Percentage**. For more information, see **Identity Processing Thresholds** in the **Rapid Setup** documentation.
Threshold	Enter a value to use in conjunction with the Threshold Type, for Identity Processing Thresholds.
Certification Name	Specify the name of the certification associated with the certification event.
Certification Owner	Specify the owner of the certification.
Certifiers	Specify the full name of the person or people to be assigned the certification. To display a list of all valid certifiers in the system, type the first few letters of the name and then select a name from the displayed list. **Assign to Manager(s)** - assign to the manager(s) of the identities for whom the certifications are created. You must also enter a default certifier in case some of the identities do not have a manager assigned. **Select Certifier(s) Manually** - manually specify certifiers to whom these event certifications will be assigned.
Included Applications	Specify the applications with the roles and entitlements that should be discovered when generating this certification. If no applications are specified, then all of the applications are included.

Field Name	Description
Included Access	Include entitlements or Accounts in the certification that are assigned to an identity but are not contained within a defined role.
Include Policy Violations	Include policy violations for each identity in the certification report. If this field is deactivated no policy violations are included.
Include Roles	Include roles assigned to the identity in the certification.
Tags	Specify one or more tags for the certifications. Tags can be used to classify certifications for searching and reporting.
Lifecycle These options define the lifecycle of the certification.	
Active Period Enter Rule	Select a rule to run when the certification enters its active period.
Active Period Duration	Specify the length of the review period during when all decisions required within this certification should be made. During this phase changes can be made to decisions as frequently as needed. You can sign off on a certification in the active stage if no roles or entitlements were revoked or if the challenge period is not active. When you sign off on a certification, it enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.
Enable Challenge Period	Specify the period when all revocation requests can be challenged by the user whose role or entitlement is being removed. When the challenge phase begins, a work item and email are sent to each user in the certification that the revocation decision affects. The work items contain the details of the revocation request and any comments the requestor adds. The affected user has the duration of the challenge period to accept the loss of access or challenge that decision. You can sign off on a certification in the challenge phase if all challenges are completed and there is no open decision on the certification. When you sign off on a certification, it enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.
Enable Revocation Period	If the revocation period is disabled, the certification is not scanned for completed revocations and revocation status might not be accurately reflected throughout the product. Specify the period when all revocation work should be completed. Revocations can be done automatically or manually. Your provisioning provider must be configured for automatic revocation. Manual revocations use a work request assigned to a IdentityIQ user with the proper authority on the specified application. The revocation phase begins when a certification is signed off or when the active and challenge phases have ended. Revocation activity is monitored to ensure that inappropriate access to roles and entitlements is revoked in a timely manner. Revocation completion status

Field Name	Description
	is updated at an interval specified during the deployment of IdentityIQ. By default this task is performed daily. Click **Details** to see view detailed revocation information. Revocation requests that are not acted upon during the revocation phase can be escalated as needed.
End Period Enter Rule	Select a rule to run when the certification begins its end period.
Process Revokes Immediately	Select this option to specify that revocation requests are processed as soon as a revocation decision is saved. If this field is not selected, revocation requests are not sent until the certification is signed off. If the challenge period is active, the revocation request is not sent until the revocation is accepted or the challenge period expires.
Enable Automatic closing	Select this option to automatically close the review after the specified parameters are met. This option closes unfinished reviews.
Notifications: **These options specify when reminders and escalations occur for certification and revocations.**	
Suppress Initial Notifications	Prevent the sending of an initial notification.
Initial Notifications Email Template	Set the default email template for initial certification notifications.
Notify Before Certification Expires	Send email reminders before certification expires. Send the first reminder: The number of days before the certification expiration date that the first reminder is sent. Reminder Frequency: The frequency with which email reminders are sent until the request is completed or expires. Reminder Email Template: The IdentityIQ notification template used for the reminders.
Escalate Before Certification Expires	Send an escalation notice and change the owner of the certification to the escalation recipient. **Escalation Trigger**: The number of days after which a certification is assigned, or the number of email reminders that are sent to the certification owner, before the first escalation notice is sent. **Escalation Rule**: The escalation rule to apply when escalating a certification request.
Send Revocation Reminder	Send email reminders before the revocation period expires. Send the first reminder: The number of days before the revocation expiration date that the first reminder is sent. **Reminder Frequency**: The frequency with which email reminders are sent

Field Name	Description
	until the request is completed or expires. **Reminder Email Template**: The IdentityIQ notification template used for the reminders.
Escalate Revocation	Send an escalation notice and change the owner of the revocation request to the escalation recipient. **Escalation Trigger**: The number of days after which a revocation request is assigned, or the number of email reminders that are sent to the revocation request owner, before the first escalation notice is sent. **Escalation Rule**: The escalation rule to apply when escalating a revocation request.
Notify Users Of Revocations	Set the default email template for initial certification notifications.
Bulk Reassignment Modification Notices	Set the default email template for bulk reassignment notifications.
Behavior: **These advanced options specify items that can change the presentation and behavior of the certification.**	
Require Electronic Signature	Enable this option to require an electronic signature as part of the Sign-off procedure. Select the electronic signature meaning from the Electronic Signature Meaning drop-down list. An electronic signature performs the same authorization checking as the IdentityIQ login page.
Require Subordinate Completion	Enable this option to require that all subordinate access reviews be completed before the parent report can be completed.
Automatically Sign Off When Nothing to Certify	Enable this option to automatically sign off an access certification, with the assignee's credentials, if the access review contains no items, even if there are subordinate access reviews present. Access reviews containing no items and having no subordinate access reviews are always automatically signed off on using the certification initiator's credentials.
Suppress Notification When Nothing to Certify	Do not send notification email when the assignee has nothing to certify.
Require Reassignment Completion	Enable this option to require that all reassignment access reviews be completed before the parent report can be completed.

Field Name	Description
Return Reassignments to Original Access Review	Enable this option to cause the contents of reassignment access reviews to revert to the original access review when the reassigned access review is signed.
Automatically Sign Off When All Items Are Reassigned	Enable this option for an access review to be automatically signed off when all items in the access review are reassigned. The Require Reassignment Completion and Return Reassignments to Original Access Review options must not be enabled for this option to be available.
Require Delegation Review	Enable this option to require the original access review owner to review all delegated access reviews.
Require Comments For Approval	Enable this option to require the certifier to include comments when an access review item is approved.
Require Comments When Allowing Exceptions	Enable this option to require the certifier to include comments when an exception is allowed.
Require Comments for Revocation	Require the certifier to include comments when a certification item is revoked.
Disable Delegation Forwarding	Select to disallow the forwarding of a work item that was delegated by a different user.
Limit Reassignments	Limit the number of times an item can be reassigned with a certification champaign.
Show Classifications	Show classification information. When enabled, classifications provide additional information about roles, managed attributes and policy violations.
Enable Line Item Delegation	Enable this option to allow certifiers to delegate individual items from an access review.
Enable Identity Delegation	Enable this option to allow certifiers to delegate entire identities in an access review.
Enable Account Revocation	Enable this option to allow the certifier to revoke an account, when its associated entitlements are also revoked. Note that disabling this option does not prevent the reviewer from revoking accounts directly - it only enables or disables the "revoke account" option when entitlements are being certified.
Enable Allow Exceptions (applies only to non-policy viol-	Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.

Field Name	Description
ation items)	
Deprovision Items When Exception Expires (applies only to non-policy violation items)	Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations. This option is available only when the **Enable Allow Exceptions** option is also enabled.
Enable Allow Exception Popup	Enable this option to allow certifiers to view the Allow Exception popup and manually set expiration dates and allow comments. This applies to both violation and non-violation items.
Default Duration for Exceptions	Set a default time period in which exceptions are allowed during the access review.
Enable Bulk Approval	Enable this option to allow users to bulk approve access review items.
Enable Bulk Revocation	Enable this option to allow users to bulk revoke access review items.
Enable Bulk Allow Exceptions	Enable this option to allow users to allow exceptions in bulk.
Enable Bulk Reassignment	Enable this option to allow users to bulk reassign access review items.
Enable Bulk Account Revocation	Enable this option to allow users to revoke all entitlements for a specific account in bulk. This option is not available for Entitlement Owner certifications.
Enable Bulk Clear Decisions	Enable certifiers to cancel all decisions currently made on the access review.
Advanced: **These advanced options specify items that can change the contents and behavior of the certification.**	
Custom Name	Specify the custom name template used to name certifications. The name can contain parameterized content that is merged into the name when the certification is generated.
Custom Short Name	Specify the custom short name template used to give certifications short names. The name can contain parameterized content that is merged into the short name when the certification is generated.
Exclusion Rule	Select the rule to run to exclude specific entitlements from the certification. For example, if you have an entitlement that is assigned to every user in your enterprise, you generally do not need to include it in certifications.
Save Exclusions	Select this option to save any entitlements that are discovered, but excluded from the certification enabling them to be used in reports.

Field Name	Description
Exclude Inactive Identities	Select this option to exclude inactive identities from new certifications and remove identities that become inactive from existing certifications.
Exclude Logical Tier Entitlements	Select this option to exclude entitlements on tier application accounts from the certification. This option applies to composite applications.
Filter Logical Application Entitlements	Select this option to allow logical entitlements defined on the logical application's managed entitlement list to be included in the certification. Any logical application entitlements are filtered from the tier application entitlements
Include IdentityIQ Capabilities	Select this option to include IdentityIQ capabilities of the identity for certification.
Update Entitlement Assignments	Select this option to update assignments after entitlement decisions are made.
Pre-delegation Rule	Automated pre-delegation and pre-reassignment rules are not meant to be run in conjunction with the Fallback Forwarding User rule. Specify the rule to use to determine if portions of the certifications that this schedule generates need be pre-delegated to specific certifiers.
Sign Off Approver Rule	Specify the rule that is used to determine if additional review is need on the sign off decision. After the certifier's initial sign off, this rule is run to determine if another approver need to review the decisions need to be reviewed. If additional review is needed, the certification request is sent to that user's inbox and they receive an email notification. This process is repeated until no more reviewers are discovered by the rule.
Allow Self Certification For	Choose which users may self-certify (that is, be the certifier for their own access), either by forwarding or reassigning an access review: All certifiers, Certification and System Administrators, System Administrators only
Self Certification Violation Owner	For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person.

Manage and Schedule Certifications

> The term account group can be replaced by the term application object for some applications. Some application can have multiple application objects. An account group can be the name of one of those objects.

IdentityIQ automates and optimizes the review and approval of:

- Identity access privileges
- Account group permissions and membership
- Role composition and membership

Use the Certifications page to view and create the scheduled certifications that are required to maintain compliance in your enterprise. You can also use this page to create one-time certifications when required. From this page, you can create certifications for your entire enterprise or for one approver or one item.

Certifications include multiple access reviews. When a certification schedule is created the work item arrives labeled as an access review request.

The Certification Page contains the following areas:

- Certifications Tab
- Certification Events
- Scheduling a New Certification

Certifications Tab

Use the Certifications tab to view certification requests that are complete or in the process of running.

Column	Description
Name	The type of certification scheduled and the date and time when it was first launched.
Owner	The user that started the certification request
Status	Current status of the certification request. Pending, Active, or Staged.
Percent Complete	Percentage of certification completion based on the number of access reviews in the certification.
Create Date	The date and time when the certification request was generated.
Tags	Assigned labels that are used to classify certifications for searching and reporting.

The detailed results page contains all of the information that is available for the scheduled certifications.

Click a certification to display the detailed results page for that certification. Right-click and select **Change Owner** to assign a new owner for this certification or select **Use as Template** to use this certification as a template to schedule a new certification.

> A change to the owner does not reassign or forward this certification to the new owner and no notification is sent to the new owner upon the change. The new owner name is associated with the certification throughout IdentityIQ.

The Certification Results page displays the name and owner of the certification, the date it was created, and status bars to track completion of the reviews, including the information described in the table below. For each access review, a description of the access review, including additional information, is described in the Access Reviews section of the table.

Access Review Information

Item	Description
View Certification Options	Click to view all of the certification parameters.
Exclusions	Click to view which items were not included in the certification.
completed	The date and time when the certification request was completed. The completed status is based on the completion of all certification components.
Decision Statistics	
Roles	Pie chart with statistical data for open, approved and remediated business role items for the access reviews within the certification. This pie chart is only visible if Include Roles was enabled in the Basic section of the certification schedule creation.
Additional Entitlements	Pie chart with statistical data for open, approved and remediated entitlement items for the access reviews within the certification. This pie chart is only visible if Include Additional Entitlements was enabled in the Basic section of the certification schedule creation.
Policy Violations	Pie chart with statistical data for open, allowed and remediated policy violations for the access reviews within the certification. This pie chart is only visible if Include Policy Violations was enabled in the Basic section of the certification schedule creation.
Access Reviews	
Description	The type of certification.
Percent Complete	The percentage of the certification that is complete. For example, 46% (6 of 13) means 6 of the 13 users on the list, or 46% of the total number, have been acted upon.
Phase	The current phase of the certification process.

Item	Description
	The challenge and revocation phases are only active if those functions were activated when the certification request was scheduled. **Active** — the time period when the certifier must make all decisions required to complete the certification. **Challenge** — the time period when the affected user can challenge the decisions to revoke roles or entitlements. **Revocation** — the time period when all revocation work is expected to be completed for roles or entitlements that were revoked. Reminder notifications and escalations can be set based on these completion expectations. **End** — the certification is complete.
Phase End	The date and time when the current phase ends and the next phase begins. The length of each phase is specified when the certification request is scheduled.
Tags	Tags are used to classify certifications for searching and reporting. Tags are assigned when certifications are scheduled.
Certifiers	The name of the person responsible for acting on the access review.
Due	The date and time when the access review decision is required.
E-signed	A check-mark icon indicates that an electronic signature exists. An electronic signature performs the same authorization checking as the IdentityIQ login page.

The information displayed for each certification varies based on the type of certification and the parameters specified when the schedule is created.

For example, a manager certification results page can contain the number of access reviews that were generated, the managers who were assigned the requests, and the active period for this schedule.

Certification Schedules Tab

Use the Certification Schedules tab to view and edit information about pending and periodic.

> Certifications that are scheduled to run one time are considered to be pending and are removed from the list of scheduled certifications after the scheduled run time.

Periodic certifications are scheduled to run on a periodic basis, such as hourly, daily, weekly, monthly, quarterly, and annually. Periodic access reviews provide a snapshot view of the identities, roles, and account groups in your enterprise. Periodic certifications focus on the frequency that entire entities (identities, roles, account groups) must be certified.

Periodic certifications are not complete until all access reviews included in the certification are complete. An access review is not complete until all actions are complete and the user who is assigned the access review confirms the decisions.

Periodic certifications can be created using a multi-level sign-off structure which enables multiple certifiers to review access reviews before they are considered complete. For example, a certification can be created for the direct reports of a team leader who knows his employees, but is not authorized to make final certification decisions. When the team leader makes his decisions and signs off on the access review, it can be forwarded to the department manager to review the decisions and make changes if necessary.

The Certifications Schedule tab contains the following information:

Column	Description
Name	The type of certification scheduled and the date and time when it was launched.
Task	The task that was performed.
Next Execution	The next date and time when the certification runs.
Last Execution	The date and time when the certification ran last.
Result	Result status of the last run of the certification, for example Success or Failed.
Owner	The user who started the certification request

Click an existing certification to view the details defined for the certification when it was created. Certifications can be modified for future certifications. Actions that were taken on the access reviews included in the certification and the current phase of the certification determine which items can be modified.

Scheduling a New Certification

> Identity certifications are special cases and are scheduled from the Identities or Advanced Identity Search Results pages. Any IdentityIQ user with access to those pages can schedule an identity certification.

Use the **New Certification** drop-down list to schedule certifications.

> Identity Certifications are not scheduled from the Certifications page, they are requested from the Identity Risk Scores, Identity Search Results or Policy Violations pages.

> Automatic approvals are not dismissed in the access reviews if you turn off the automatic approval feature and then activate a staged certification. To remove automatic approvals access reviews generated by a staged certification, you must delete and redefine the certification.

To generate a preview of a certification, enable the staging feature on the Lifecycle panel on the Schedule Certification page for non-targeted certifications or on the Schedule panel for targeted certifications. When the staging feature is enabled, a certification and associated access reviews are created, but the access reviews are not sent to the certifiers. You can view what the certification schedule definition produces before the schedule is activated. If the generated certification does not match your needs, you can cancel the certification and redefine it as needed. If the certification is accurate, activate the schedule.

For more information on the contents of certifications, see:

- Scheduling a Non-Targeted Certification
- Scheduling a Targeted Certification

Creating a New Certification from an Existing One

New certifications can be created from existing certification definitions so the existing certification definition provides a starting point for configuring the new one.

To do this, right-click a certification on the **Setup > Certifications** page, Certifications tab, and click **Use Certification as a Template**. Then modify the certification details as needed for the new certification.

Scheduling a Non-Targeted Certification

A non-targeted certification refers to any of the types of certification you can schedule in IdentityIQ other than the Targeted certification: Manager, Application Owner, Entitlement Owner, Advanced, Account Group Membership, Account Group Permissions, Role Membership, Role Composition, and Identity. For more details, see Types of Certification

The sections below describe all fields included in any non-targeted certification. Fields or options that are available for a specific type of certification are listed in a separate column.

Basic Fields

The **Basic** page includes general information about the certification including the name, owner, and various controls about when and how often to run it. This page also includes a number of fields that are specific to a limited set of certification types.

The **When to Certify** section of this page determines the scheduling and frequency of each certification. Certifications can be run once or on an hourly, weekly, monthly, quarterly or annual basis. They can be kicked off immediately or scheduled to start at a later date or time. Each subsequent certification run, if any, will repeat at the same time of day as the first run, after the specified time interval has passed. (Certifications scheduled to run hourly will run once an hour at the same minute of each hour.)

> Certification start times must be at least one minute later than the current time. For example, if it is currently 11:41, the certification start time must be 11:42 or later.

> Certifications that run across time zones run at the time scheduled, relative to the time zone in which they are scheduled. For example, a certification scheduled to run at 1:00 PDT will run at 4:00 EDT.

Field Name	Certification Type	Description
Certification Name	All	Specify a name and date parameter that identifies the certification.
Certification Owner	All	Specify an owner of the certification.
Recipient	Manager	The full name of a specific manager being assigned a certification. To display a list of all of the manager names in the system, type the first few letters of the name. You can select a name from the displayed list.
All Managers	Manager	Schedule a certification for all managers configured in the IdentityIQ application.
Application(s)	Application Owner	Select the applications to certify. Use the Ctrl or Shift keys to select multiple applications or select **All Applications**.

Field Name	Certification Type	Description
	Entitlement Owner Account Group	
All Applications	Application Owner Entitlement Owner Account Group	Include all applications in the certification.
Populations to Certify	Advanced	**Population** — All available populations IdentityIQ. Includes all public populations and populations you created.
		Certifier(s) — The identities who are requested to complete the certification request. Certifiers can be individual identities or workgroups. To display a list of all of the manager names in the system, type the first few letters of the name. You can select a name from the displayed list. A separate certification request is sent for each population specified, even if the certifier of each is the same.
Group Factories to Certify	Advanced	**Group Factory** — All available groups created by group factories and includes all identity attributes designated as group factories.
		Certifier Rule — Select the rule used to designate certifiers for the groups selected.
Certifiers	Identity	Select the person or people to review the certification. Options include assigning managers or manually selecting certifiers.
Identities	Identity	Lists each identity included in the certification. To remove identities, select an identity and click **Remove Selected Users**. To add identities type a name in the field and click **Add User**.
Included Applications	Manager Identity	The applications included when generating this certification. If no applications are specified, all of the applications are included.
Select Role(s)	Role Membership Role Composition	To specify roles to certify, select a role from the list. To specify a role type to certify, click the **Certify by Role Type** radio button and select the role type from the list. When you include business roles, all assigned business roles

Field Name	Certification Type	Description
		are displayed in the certification.
Certify All Roles	Role Membership Role Composition	Schedule a certification on all roles defined in your enterprise.
Include Role Hierarchy	Role Composition	Create certification items for each role that is included in the roles selected for certification.
Included Access	Manager Application Owner Identity	Select Entitlements to include entitlement access in the certification. You can also choose to include Additional Entitlements, Roles and Accounts With No Entitlements in the certification. You must select Accounts to include from accounts in the certification. The Include Roles option is enabled by default and all assigned business roles are displayed in the certification.
Include Policy Violations	All	Include policy violations for each identity in the certification report.
Include Unowned Data	Entitlement Owner	Select this option to include managed entitlements and permissions that have no owner in the access review.
Unowned Entitlement Reviewer	Entitlement Owner	Select this option to assign ownership of unowned entitlements to the application owner or an identity you select from the drop-down list.

Lifecycle Fields

The **Lifecycle** page determines which phases of the complete certification process will be included for the specific certification's access reviews and which rules will be run at the start of each phase. Parameters on this page impact details of the different certification phases. See Phases of a Certification.

Examples of these parameters include:

- Rules run at the beginning of the access reviews' various phases
- Duration of the Active period
- Inclusion of a Challenge period
- Inclusion of a Revocation period
- Timing of revocation request submission
- Closing of incomplete certifications after expiration

Field Name	Description
Enable Staging Period	Use to generate a test certification that is used to verify functionality and configuration of the parameters before the certification is generated. The test certification displays in the Certifications tab with the status set to Staged. Click the certification to view it is contents and either activate or cancel it. You might experience a short delay between scheduling the test certification and seeing it on the Certifications tab with all of the data displayed. Automatic approvals are not dismissed in the access reviews if you turn off the automatic approval feature and then activate a staged certification. To remove automatic approvals access reviews generated by a staged certification, you must delete and redefine the certification.
Active Period Enter Rule	Select a rule from the drop-down list to apply when the certification enters its active period.
Active Period Duration	Specify the review period when all decisions required within this certification must be made. During this phase changes can be made to decisions as often as needed. You can sign off on a certification in the active period only if no roles or entitlements were revoked or if the challenge period is not active. When you sign off on a certification, the certification enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.
Enable Challenge Period	Specify the period when all revocation requests can be challenged by the user from which the role or entitlement is being removed. When the challenge phase begins, a work item and email are sent to each user in the certification that the revocation decision affects. The work items include the details of the revocation request and any comments the requestor added. The affected user has the duration of the challenge period to accept the loss of access or challenge that decision. You can sign off on a certification in the challenge phase if all challenges were completed and no open decisions remain on the certification. When you sign off on a certification, it enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist. This option is not available for Role Composition and Role Membership certifications.
Challenge Period Enter Rule	Select a rule from the drop-down list to apply when the certification enters its challenge period.
Challenge Period Duration	Specify the period of time when items remain in the challenge period.
Challenge Email Templates	Choose the email templates used for a variety of challenge period notifications.

Field Name	Description
Enable Revocation Period	If the revocation period is disabled, the certification is not scanned for completed revocations and revocation status might not be accurately reflected throughout the product. Specify the period when all revocation work must be completed. When the revocation phase is entered, revocation is done automatically if your provisioning provider is configured for automatic revocation or manually using a work request assigned to an IdentityIQ user with the proper authority on the specified application. The revocation phase is entered when a certification is signed off or when the active and challenge phases have ended. Revocation activity is monitored to ensure that inappropriate access to roles and entitlements is revoked in a timely manner. Revocation completion status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily. Click **Details** to view detailed revocation information. Revocation requests that are not acted upon during the revocation phase can be escalated as required.
Revocation Period Enter Rule	Select a rule from the drop-down list to apply when the certification enters its revocation period.
Revocation Period Duration	The period of time when items remain in the revocation period.
End Period Enter Rule	Select rule to run when the certification enters the end period.
Process Revokes Immediately	Specifies that revocation requests must be processed as soon as a revocation decision is saved. If this field is not activated, revocation requests are not sent until the certification is signed off. If the challenge period is active, the revocation request is not sent until the revocation is accepted or the challenge period expires.
Enable Automatic Closing	Specifies that decisions not made by the certifier during the active phase are made automatically. Use the following options to configure the details of this process. **Time After Certification Expiration** - Select the amount of time following this access review's expiration date that IdentityIQ must wait before attempting to automatically close it. **Closing Rule** - Select the rule that IdentityIQ runs at the beginning of the automatic closing process. **Action Taken On Undecided Items** - The action that IdentityIQ assigns to any undecided items when automatically closing this access review. Choose from Approve, Revoke, or Allow Exception.

Field Name	Description
	Comments - Input the comments that IdentityIQ adds to any undecided items when automatically closing this access review.

Notifications Field Descriptions

The **Notifications** page controls whether and when certifiers and revokers are sent email notices and reminders to complete the required tasks. By default, email notification is sent to certifier(s) when the access reviews are ready to review. Options selected on this page determine whether and how frequently additional email reminders are sent; they can also trigger escalations when certifications are nearing their expiration and have not been completed. Similarly, revocation reminder emails and automatic escalations can be configured for revocation requests created from the access reviews.

> Some of these options are not available on Identity, Application Owner, and Advanced certifications.

Field Name	Description
Suppress Initial Notifications	Select this option to prevent the sending of initial certification notification emails.
Initial Notification Email Template	Choose the email template used for initial certification notifications.
Notify Before Certification Expires	Send email reminders before certification expires.
Send Revocation Reminders	Send email reminders before the revocation period expires. Includes when the first reminder is sent, how often reminders are sent, and which template to use for the reminders.
Escalate Revocations	Send an escalation notice and change the owner of the revocation request to the escalation recipient. Includes settings for: • Number of reminders to send to the revocation request owner before the first escalation occurs • Escalation rule to apply when escalating an uncompleted revocation request • Email template to use for the escalation notice
Notify Users Of Revocations	Send an email notification to identities whose access was revoked. This option is not available for Account Group Permissions or Role Composition certifications.
Bulk Reassignment Modification Notices	Choose the email template to use to send bulk reassignment notices

Behavior Fields

The **Behavior** page is used to configure how certifiers view and interact with the access reviews. It determines the default display characteristics of the access reviews. It also enables or disables options such as reassignment and delegation of identities or individual line-items, provisioning of missing role requirements, permitting of policy violation exceptions, and application of bulk actions to multiple certification records at a time.

Field Name	Description
Prompt for Signoff	Enable this option to display a pop-up reminder to indicate when an access review is complete and ready for sign-off.
Require Electronic Signature	Enable this option to require an electronic signature as part of the Sign-off procedure. Select the electronic signature meaning from the Electronic Signature Meaning drop-down list. An electronic signature performs the same authorization checking as the IdentityIQ login page.
Require Subordinate Completion	Enable this option to require that all subordinate access reviews be completed before the parent report can be completed.
Automatically Sign Off When Nothing to Certify	Enable this option to automatically Sign Off an access certification, with the assignee's credentials, if the access review contains no items, even if there are subordinate access reviews present. Access reviews containing no items and having no subordinate access reviews are always automatically signed off using the certification initiator's credentials.
Suppress Notification When Nothing to Certify	Do not send notification email when the assignee has nothing to certify.
Require Reassignment Completion	Enable this option to require that all reassignment access reviews be completed before the parent report can be completed.
Return Reassignments to Original Access Review	Enable this option to cause the contents of reassignment access reviews to revert to the original access review when the reassigned access review is signed.
Automatically Sign Off When All Items Are Reassigned	Enable this option for an access review to be automatically signed off when all items in the access review are reassigned. The Require Reassignment Completion and Return Reassignments to Original Access Review options must not be enabled for this option to be available.
Require Delegation Review	Enable this option to require the original access review owner to review all delegated access reviews.
Require Comments For Approval	Enable this option to require the certifier to include comments when an access review item is approved.
Require Comments When Allowing Excep-	Enable this option to require the certifier to include comments when an exception is allowed.

Field Name	Description
tions	
Require Comments for Revocation	Require the certifier to include comments when a certification item is revoked.
Disable Delegation Forwarding	Select to disallow the forwarding of a work item that was delegated by a different user.
Limit Reassignments	Enable this option to allow users to limit the number of reassignment of certification item.
Show Classifications	Show classification information in identity-based access reviews. When enabled, classifications provide additional information about roles, managed attributes and policy violations. Note that this option is available only in identity-based certifications.
Enable Line Item Delegation	Enable this option to allow certifiers to delegate individual items from an access review.
Enable Identity Delegation	Enable this option to allow certifiers to delegate entire identities in an access review.
Enable Account Revocation	Enable this option to allow users to bulk revoke all entitlements for a specific account.
Enable Allow Exceptions (applies only to non-policy violation items)	Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.
Deprovision Items When Exception Expires (applies only to non-policy violation items)	Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations. This option is available only when the **Enable Allow Exceptions** option is also enabled.
Enable Allow Exception Popup	Enable this option to allow certifiers to view the Allow Exception popup and manually set expiration dates and allow comments. This applies to both violation and non-violation items.
Default Duration for Exceptions	Set a default time period in which exceptions are allowed during the access review.
Show Recommendations	This option is only visible if you have purchased and activated the SailPoint AI Services product This feature is only available on Manager, Application Owner, Advanced, and Role Membership certifications. Enable recommendations from AI Services to display in access reviews.
Automatically	This option is only visible if you have purchased and activated the SailPoint AI Services product

Field Name	Description
Approve Recommended Items	This feature is only available on Manager, Application Owner, Advanced, and Role Membership certifications. Automatically mark access review items as approved and move them from the Open to the Review tab of the access review.
Enable Bulk Approval	Enable this option to allow users to bulk approve access review items.
Enable Bulk Revocation	Enable this option to allow users to bulk revoke access review items.
Enable Bulk Allow Exceptions	Enable this option to allow users to allow exceptions in bulk.
Enable Bulk Reassignment	Enable this option to allow users to bulk reassign access review items.
Enable Bulk Account Revocation	Enable this option to allow users to revoke all entitlements for a specific account in bulk. This option is not available for Entitlement Owner certifications.
Enable Bulk Clear Decisions	Enable certifiers to cancel all decisions currently made on the access review.

Advanced Fields

The **Advanced** page allows for additional customizations of the certification. This includes selection of an Exclusion Rule for excluding identities or entitlements from the certification. Depending on the certification type, the options may also include other parameters for excluding identities or entitlements, and inclusion of IdentityIQ capabilities and scopes, among other options. For most certification types, this is also where the certifier can be assigned.

Field Name	Certification Type	Description
Custom Name	All	The custom name used to name certifications. You can combine free text and parameterized text by selecting parameters from the drop-down list on the right.
Custom Short Name	All	You can combine free text and parameterized text by selecting parameters from the drop-down list on the right.
Certifiers	Role Membership Role Composition	**Assign to Manager (Role Membership Only)—** assign the certification request to the role member's manager. If the role members do not share a common manager, a separate certification request will be created for each manager with at least one direct report in the role under certification. If a manager is not found for an identity, the certification is assigned to the role owner for that identity. **Assign to Role Owner —** assign the certification to the owner

Field Name	Certification Type	Description
		of the role under certification. If multiple roles have been selected, separate certifications will be created if the given roles do not share a common owner. If no role owner is discovered, a warning is attached to the task results with a list of the items that could not be assigned for certification. **Select Certifier Manually —** enter the full name of a specific certifier or certifiers being assigned this certification. Certifiers can be individual identities or workgroups. A name entered here overrides the default certifier for the type of certification requested. Typing the first few letters of the name displays a list of all of the authorized certifier names in the system containing that letter combination. You can select from the displayed list.
Certifiers	Application Owner Account Group Membership Account Group Permissions	The full name of a specific certifier or certifiers being assigned to this certification. A name entered here overrides the account group owner as certifier for this certification request. Certifiers can be individual identities or workgroups.
Generate Certifications	Manager Identity	Select whether to generate a certification request for the specified managers, or for the specified managers and all of their subordinate managers. If you select **For the specified manager(s) only**, the **Flatten Hierarchy** option is displayed. Select the **Flatten Hierarchy** option to include everyone below the manager in the reporting hierarchy on the certification request.
Exclusion Rule	All	Select the rule that should be run to exclude certain entitlements from the certification. For example, if you have an entitlement that is assigned to every user in your enterprise, you probably do not need to include it in certifications.
Save Exclusions	All	Activate to save any entitlements that are discovered, but excluded from the certification so that they can be used in reports.
Exclude Inactive Identities	All except Role Composition, Account Group Permissions, and Entitlement Owner	Exclude inactive identities from new certifications and remove identities that become inactive from existing certifications.

Field Name	Certification Type	Description
Include Roles Required By Other Roles	Role Membership	Include roles that are required by other roles in the certification. Note that revoking a required role in an access review will not remove it.
Filter Logical Application Entitlements	All except Entitlement Owner	Only logical entitlements defined on the logical application's managed entitlement list will be included in the certification. Additionally any logical application entitlements will be filtered from the tier application entitlements.
Include IdentityIQ Capabilities	All except Entitlement Owner	Include IdentityIQ capabilities of the identity for certification.
Update Entitlement Assignments	All except Entitlement Owner	Enable to have decisions made on entitlement values in the access review apply to the entitlement assignment model. When enabled, approvals create assignments and revocations remove assignments.
Pre-delegation Rule	All	Specify the rule to use to determine if portions of the certifications generated by this schedule should be pre-delegated or reassigned to specific certifiers.
	All except Role Composition	The rule used to determine if additional review is needed on the Sign Off decision. After the initial Sign Off by the certifier, this rule is run to determine if the decisions need to be reviewed by another approver. If they do, the certification request is sent to that user's inbox and they receive an email notification. This process is repeated until no more reviewers are discovered by the rule. You must also select the email template used for Sign Off approvers.
Allow Self Certification For	All except Role Composition and Account Group Permissions	Choose which users may self-certify (that is, be the certifier for their own access), either by forwarding or reassigning an access review: All certifiers, Certification and System Administrators, System Administrators only
Self Certification Violation Owner	All except Role Composition and Account Group Permissions	For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person. If a Self Certification Violation Owner is not specified, any items that require self-certification will be read-only to the reviewer.
Enable Partitioning	Manager	Enable the use of multiple threads to schedule the certification

Scheduling a Targeted Certification

Targeted Certifications are the most flexible type of certification. In a Targeted Certification you can certify role, entitlement, and account access for a narrowly defined set of identities. The Targeted Certification gives you a high level of flexibility in choosing which parameters to include in the certification (such as who, what, and when to certify).

- Targeted Certification: Who to Certify
- Targeted Certification: What to Certify
- Targeted Certification: Choose Certifier
- Targeted Certification: Schedule
- Targeted Certification: Additional Settings

Targeted Certification: Who to Certify

To narrow down the identities to certify, choose an option for selecting identities. To certify all identities in your system, do not define any selection criteria.

Filter Identities

Use filters to define the identity list for the certification. You can filter identities by attribute, using operations like Equals, Not Equals, or Starts With. You can choose the values for the filter from a list, or type them in. You can only type in valid values.

You can choose more than one value for any one filter. When you do this, the criteria works as an “or” operation, so the certification will include all identities meeting any of the criteria. For example, filtering on Department Equals and entering two departments will select identities from both those departments.

Add more filters if you want to filter on more than one attribute using an “and” condition. With multiple filters, identities have to meet each of the sets of filter criteria in order to be included. For example, filtering on Department Equals Accounting and Location Equals Berlin will select only identities that are in the Accounting department in Berlin.

Access reviews for Service or RPA/Bot identities are sent to the certifier specified during your configuration process.

Population

Choose from the populations that have been defined in your IdentityIQ system. Populations are saved queries based on searches run from the Identity Search feature of Advanced Analytics. For more information see the **Advanced Analytics** documentation.

Rule

Choose a rule that will select identities. The Targeted Certification does not include a rule editor, so you are limited to choosing existing rules from the list. Only rules with a rule type of **CertificationScheduleEntitySelector** are included in this list.

Exclude Inactive Identities

Check this to omit identities flagged as Inactive at the time the certification is generated. For recurring certifications, future occurrences will reflect any changes that have happened since the last certification was generated, including identities that have become inactive.

Targeted Certification: What to Certify

This section lets you narrow the focus of the certification by defining which elements of accounts, roles, entitlements, and target permissions to include.

For **Roles / Entitlements**, you can add more criteria that is specific to entitlements:

- Check **Additional Entitlements** to include entitlements that are not contained in a role. If you check this option, you can also add filtering criteria to choose the entitlements to include.
- Check **Include Accounts without Entitlements** to include accounts that have no entitlement attributes.
- Check **Target Permissions** to include the actions a user can perform on an Unstructured Target such as a file share or folder.

Adding Filters

You can filter the Roles/Entitlements or Accounts to include in the certification, using operations like Equals, Not Equals, or Starts With. You can choose the values for the filter from a list, or type them in. You can only type in valid values.

You can choose more than one value for any one filter. When you do this, the criteria works as an “or” operation, so the certification will include all entities meeting any of the criteria. For example, filtering on Owner Equals and entering two identities will select roles/accounts owned by *either* of those identities.

Add more filters if you want to filter on more than one attribute using an “and” condition. With multiple filters, entities have to meet each of the sets of filter criteria in order to be included. For example, filtering accounts on Service Account Equals True and Application Equals Active_Directory will select only service accounts on the Active Directory application

Select Attribute

Select a role\entitlement attribute from the drop-down list.

Operator

Select an operator from the drop-down list for this attribute.

Value

Select a value from the drop-down list. The values available are dependent on the attribute and operator selected. You can enter text in the value field for some types of attributes, to help find the value you want; only valid values are supported.

Other Options

Include Policy Violations

Policies are rules that enforce your enterprise's business policies on separation of duty, activity, and risk. Violations of those policies can be included in the access reviews generated by the certification.

Exclude Logical Tier Entitlements

Logical applications are applications formed by the detection of accounts from other applications, called "tier" applications, in existing Identity Cubes. Use this option to exclude entitlements on tier application accounts from the certification. This applies only to logical applications, which are applications formed by the detection of accounts from other applications, called "tier" applications, in existing Identity Cubes.

Filter Logical Application Entitlements

Allow logical entitlements defined on the logical application's managed entitlement list to be included in the certification. Any logical application entitlements are filtered from the tier application entitlements.

Include IdentityIQ Capabilities

Capabilities control access to pages, tabs, and fields within IdentityIQ. Use this option to include IdentityIQ capabilities in the certification.

Include IdentityIQ Scopes

Scopes are used to restrict access to objects in IdentityIQ. If scoping is enabled in your implementation, use this option to include scopes in the certification

Targeted Certification: Choose Certifier

Use the **Choose Certifier** section to configure who will perform the certification by reviewing and deciding on access.

Targeted certifications are designed to enable you to get very specific on the certification scheduling page to select exactly who should be the certifier for the certification. Tools are provide that eliminate the need to reassign certifications. This design provides the flexibility of rules from the user interface so that you can schedule certifications without having to write rules.

If required, reassignment can be performed by specifying a Certifier type rule in the Primary Certifier field. For example, if the certifier should be a manager except if the target identity is a manager herself or has no manager, a Certifier type rule can contain the following:

```
import sailpoint.object.Identity;
     Identity target = entity.getIdentity(context);
     if (target.getManagerStatus() || (target.getManager() == null)) {
         return "spadmin";
     }
     return target.getManager().getName();
```

Pre-delegation rules can still be used to support the Delegation and Forwarding of access reviews, but any reassignment components are ignored. Pre-delegation rules are set in the Targeted Certification: Additional Settings section.

Primary Certifier

Choose the **Primary Certifier** for the access reviews.

Manager

The manager of each identity will act as the primary certifier for that identity. A backup certifier is also required.

Owner

For **Roles**, the role owner always acts as the primary certifier. For **Additional Entitlements**, you can choose from the **Application Owner** or the **Entitlement Owner** as the primary certifier. A backup certifier is also required. Pre-delegation rules do not support reassignments in the Targeted Certification. Use the Primary Certification field in a Certifier type rule for reassignment

Rule

Choose the certifier using a rule. The Targeted Certification does not include a rule editor, so you are limited to choosing existing rules from the list. Only rules with a rule type of “Certifier” are included in this list. A backup certifier is also required. If you want to use a rule to manage **reassignments**, use a Certifier Rule here to control reassignments rather than a pre-delegation rule; pre-delegation rules do not support reassignments in the Targeted Certification.

Single Certifier

Choose an identity or workgroup who will be responsible for the access review. You have the option to add a backup certifier, but a backup certifier is not required.

Backup Certifier

A Backup Certifier is required for all types of Primary Certifier except single certifier. The Backup Certifier is the user or workgroup that will be assigned the review if the Primary Certifier can not be identified (for example, in a manager certification when an identity does not have a manager assigned).

Advanced Options

Reassignments

With reassignment, you can pass individual line items or an entire identity to another user to review. The person the items are reassigned to assumes complete responsibility for all decisions on those items, and must sign off on those decisions themselves.

Enable Bulk Reassignment

Allow reviewers to reassign multiple items simultaneously within an access review.

Limit Reassignments/ Reassignment Limit

Limit the number of times reviewers can reassign an item in the access review. If you opt to limit reassignments, include the number of reassignments allowed.

Require Reassignment Completion

Require the completion of all reassigned reviews before the parent review can be completed.

Return Reassignments to Original Access Review

When a reassigned review is signed off, return the reassigned review to the original access review owner. When items are returned, the original owner can modify the decisions the reassigned reviewer has made.

Automatically Sign Off When All Items Are Reassigned

Allow the access review to be automatically signed off when all items in the access review are reassigned. This option can only be enabled if the Require Reassignment Completion and Return Reassignments to Original Access Review options are not enabled.

Self Certification

Allow self certification for

Choose which users may self-certify - that is, be the certifier for their own access, either by forwarding or reassigning an access review: All certifiers, Certification and System Administrators, or System Administrators only

Self Certification Violation Owner

For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person. If a Self Certification Violation Owner is not specified, any items that require self-certification will be read-only to the reviewer.

Other

Prompt for Sign Off

Display an overlay prompting reviewers to sign off, when the access review is complete.

Require Electronic Signature

Require an electronic signature as part of the sign-off process. Reviewers use their IdentityIQ login as authorization for the electronic signature.

Electronic Signature Meaning

If you choose to require electronic signature, choose the meaning (the text that goes with the electronic signature) from the list. Electronic signature meanings are defined in **Global Settings > Electronic Signatures**.

Automatically Sign Off When Nothing to Certify

If the access review contains no items, allow the review to be signed off automatically with the assigned reviewer's credentials. This sign-off occurs even if there are subordinate access reviews.

Suppress Notification When Nothing to Certify

Do not send a notification email when the assignee has nothing to certify.

Sign Off Approval Rule

A rule can determine if any additional review is needed on the Sign-Off decision. If you enable this option, you also choose the rule to run after initial sign-off by the reviewer, and a **Sign Off Approval Notice Email Template**. The rule determines if the decisions need to be reviewed by another approver. If so, the user is notified via email using the email template, and the certification request is sent to that user's inbox. This process is repeated until no more reviewers are discovered by the rule. The Targeted Certification does not include a rule editor, so you are limited to choosing existing rules from the list. Only rules with a rule type of "CertificationSignOffApprover" are included in this list.

Bulk Reassignment Modification Notices

Choose the email template to use to send bulk reassignment notices.

Targeted Certification: Schedule

Use the **Schedule** section to configure when and how frequently this certification should run.

Start

Execution Frequency

If you want the certification to run on a recurring basis, choose the frequency.

Start Date

The date the certification will be launched.

Start Time:

The time the certification will be launched. Certification start times must be at least one minute later than the current time. For example, if it is currently 11:41, the certification start time must be 11:42 or later. Certifications that run across time zones run at the time scheduled, relative to the time zone in which they are scheduled. For example, a certification scheduled to run at 1:00 PDT will run at 4:00 EDT.

Run Now

Start the certification immediately after Schedule Certification is clicked. If this is a recurring certification, the subsequent certifications are scheduled accordingly.

Enable Staging Period

A staging period is when the access reviews have been created but are not yet visible to certifiers, allowing the owner to review the certification before making it active. You can view what the certification definition produces before the certification is activated. If the generated certification does not match your needs, you can cancel the certification and redefine it as needed. If the certification is accurate, activate the schedule.

Initial Notification Email Template:

The default email template to use for sending initial certification notices to certifiers.

Suppress Initial Notification

Check this option if you do not want send initial notification emails to certifiers.

> Automatic approvals are not dismissed in the access reviews if you turn off the automatic approval feature and then activate a staged certification. To remove automatic approvals access reviews generated by a staged certification, you must delete and redefine the certification.

Active

Active Period Duration

The review period when all decisions required within this certification must be made. During this phase changes can be made to decisions as often as needed. You can sign off a certification in the active period only if no roles or entitlements were revoked, or if a challenge period is not active. When you sign off a certification, the certification enters the end phase or the revocation phase. To enter the revocation phase, the revocation period must be active and a revocation decision must exist.

Active Period Enter Rule

A rule to run when the certification enters its active period. Rules of type “CertificationPhaseChange” are included in the list.

Notifications and Reminders

Reminders can be sent to the certifiers during the Active period if they have not yet completed and signed off on their access reviews. Escalations can be used to transfer responsibility to someone else (such as the certifier’s manager or the certification owner) when a certifier has not completed the access review and the end of the Active phase is near.

Click **Add** to create a reminder or escalation.

Create a Reminder

Send First Reminder Notification

When to send the first reminder email. **After Start** means days after the certification's scheduled start date. **Before Expiration** means days before the Active or Challenge (if enabled) period ends.

Reminder Frequency

How frequently email reminders are sent, until the request is completed or expires.

Reminder Email Template

The email template to use for reminder notifications.

Additional Email Recipients

Activate this option to add more email recipients. Then choose how the additional recipients are defined:

- **Recipient Rule**: To use a rule to add more email recipients, choose from the list. Rules of type "EmailRecipient" are included in this list.
- **Select Additional Recipients**: Add identities or workgroups who should receive email notifications for reminders. You can choose multiple recipients.

Create Another

Check this box then click **Add** to create additional reminders.

Create an Escalation

Escalate

When to trigger an escalation. You can only choose **After Sending Reminders** if at least one reminder has been created. **Day(s) After Start** means days after the certification's scheduled start date. **Day(s) Before Expiration** means days before the Active or Challenge (if enabled) period ends.

Escalation Rule

This rule transfers ownership of the access review to a different identity. Choose a rule from the list; rules of type "WorkItemEscalationRule" are included in this list. The rule is run if the access review has not yet been finished and signed off by the certifier at the time specified in the **Escalate** section above.

Escalation Email Template

The email template to use for escalation notifications.

Additional Email Recipients

Activate this option to add more email recipients. Then choose how the additional recipients are defined:

- **Recipient Rule**: To use a rule to add more email recipients, choose from the list. Rules of type "EmailRecipient" are included in this list.
- **Select Additional Recipients**: Add identities or workgroups who should receive email notifications for escalations. You can choose multiple recipients.

Create Another

Check this box then click **Add** to create more escalations.

End

Enable Revocation Period

Enabling a revocation period makes IdentityIQ periodically scan identities to determine whether the requested remediations have been carried out. Remediation occurs whether or not a Revocation period is enabled, but when the Revocation period is enabled, IdentityIQ monitors the status of remediation requests; when it is not enabled, remediation requests are processed but are not tracked.

When the revocation phase is entered, revocation is done automatically if your provisioning provider is configured for automatic revocation, or manually using a work request assigned to an IdentityIQ user with the proper authority on the specified application. The revocation phase is entered when a certification is signed off, or when any Active and Challenge phases have ended.

Revocation completion status is updated at an interval specified during the deployment of IdentityIQ. By default this is performed daily. Revocation requests that are not acted upon during the revocation phase can be escalated as required.

If the revocation period is disabled, the certification is not scanned for completed revocations and revocation status might not be accurately reflected throughout the product.

Revocation Period Duration

The length of the revocation period.

Revocation Period Enter Rule

A rule to run when the certification enters the revocation period. Rules of type “CertificationPhaseChange” are included in this list.

Process Revokes Immediately

Select this option to indicate that revocations should happen immediately when a decision is made. Otherwise, revocations are not launched until the certification is signed off.

Revocation Notifications

Use this option to send email reminders or escalations before the revocation period expires. Reminders send emails as the end of the revocation period approaches. Escalations use rules to determine how the work item for the revocation is escalated (for example, by transferring responsibility to the certifier's manager). You can only add revocation notifications if Enable Revocation Period is selected. Click Add to create a reminder or escalation.

Create Revocation Reminder

Days Before Expiration to Send First Reminder Notification

When to send the first reminder email.

Reminder Frequency

How frequently email reminders are sent, until the request is completed or expires.

Reminder Email Template

The email template to use for reminder notifications.

Additional Email Recipients

Activate this option to add more email recipients. Then choose how the additional recipients are defined:

- **Recipient Rule**: To use a rule to add more email recipients, choose from the list. Rules of type “EmailRecipient” are included in this list.
- **Select Additional Recipients**: Add identities or workgroups who should receive email notifications for revocations. You can choose multiple recipients.

Create Another

Check this box then click **Add** to create additional reminders.

Create Revocation Escalation

Escalate

When to trigger an escalation. You can only choose **After Sending Reminders** if at least one reminder has been created. **Day(s) Before Expiration** means days before the Active or Challenge (if enabled) period ends.

Escalation Rule

This rule transfers ownership of the access review to a different identity. Choose a rule from the list; rules of type “WorkItemEscalationRule” are included in this list. The rule is run if the access review has not yet been finished and signed off by the certifier at the time specified in the Escalate section above.

Escalation Email Template

The email template to use for escalation notifications.

Additional Email Recipients

Activate this option to add more email recipients. Then choose how the additional recipients are defined:

- **Recipient Rule**: To use a rule to add more email recipients, choose from the list. Rules of type “EmailRecipient” are included in this list.
- **Select Additional Recipients**: Add identities or workgroups who should receive email notifications for revocation escalationss. You can choose multiple recipients.

Create Another

Check this box then click **Add** to create additional notifications.

Notify Users of Revocation

Send an email notification to identities whose access was revoked.

End Period Enter Rule

A rule to run when the certification begins its end period. Rules of type “CertificationPhaseChange” are included in this list.

Enable Challenge Period

A challenge period allows users to be notified of revocation decisions affecting their access. The affected user has the duration of the challenge period to accept the loss of access, or to challenge the decision with a justification for

continued access. The Challenge period begins when the Active Period ends. The certifier can consider a challenger's justification and can change decisions based on the challenge.

Challenge Period Duration

The length of the challenge period.

Challenge Period Enter Rule

A rule to run when the certification enters the challenge period. Rules of type "CertificationPhaseChange" are included in this list.

Email Notifications

- **Challenge Period Start Notices to Certifiers**: Email template for notifying certifiers when the challenge period will start.
- **Challenge Period End Notices To Certifiers**: Email template for notifying certifiers when the challenge period will end.
- **Challenged Decision Notices To Certifiers**: Email template for notifying certifiers when a decision has been challenged.
- **Challenge Decision Expiration Notices To Challengers And Certifiers**: Email template for sending challenge decision expiration notices to challengers and certifiers.
- **Challenge Creation Notices To Challengers**: Email template for notifying challengers that a challenge has been created.
- **Challenge Expiration Notices To Challengers**: Email template for sending challenge expiration notices to challengers.
- **Challenge Accepted Notices To Challengers**: Email template for notifying challengers that a challenge has been accepted and agreed to by the certifier.
- **Challenge Rejected Notices To Challengers**: Email template for notifying challengers that their challenge has been rejected by the certifier.

Enable Automatic Closing

Automatic closing enables IdentityIQ to automatically complete and sign off access reviews that are unsigned by the access review's expiration date. Automatic closing occurs after all the other phases that have been enabled for the certification are complete.

Closing Rule

A rule to run at the beginning of the automatic closing process. Rules of type "CertificationAutomaticClosing" are included in the list.

Action Taken On Undecided Items

The action IdentityIQ will take on any undecided items when automatically closing the access review.

Automatic Closing Signer

An identity or workgroup to add as the signer of the access review when it is automatically closed.

Time After Certification Expiration

The amount of time following this certification's expiration date that IdentityIQ should wait before attempting to automatically close it.

Comments

Include any comments to add to undecided items when automatically closing this access review.

Targeted Certification: Additional Settings

Use the **Additional Settings** section to configure general information and reviewer options for the certification.

Certification Name

A name to identify the certification to certification owners. You can use free text as well as parameterized dates such as creation day, quarter, or year.

Certification Owner

The identity or workgroup responsible for the certification.

Advanced Options

Enable Bulk Clear Decisions

Allow certifiers to cancel multiple decisions simultaneously in the access review.

Update Entitlement Assignments

Enable this to cause decisions made on entitlement values in the access review to apply to the entitlement assignment model. When this is enabled, approvals create assignments, and revocations remove assignments.

Enable Partitioning

Partitioning aids the performance of certification scheduling, by subdividing activity across multiple threads, to increase processing throughput and speed. If you enable partitioning, you also set the **Number of Partitions**.If you do not enter a number, IdentityIQ will calculate an optimal number.

Show Recommendations

Enable recommendations from AI Services to appear in access reviews. This option is visible only if you have implemented SailPoint AI Services.

Automatically Approve Recommended Items

Automatically mark access review items that are recommended for approval as Approved, and move them from the Open to the Review tab of the access review. This option is visible only if you have implemented SailPoint AI Services.

Show Classifications

Show classification information in the access reviews. When enabled, classifications provide additional information about roles, managed attributes and policy violations.

Show Elevated Access

When enabled, this will show roles or entitlements that have elevated access.

Delegation Options

Require Delegation Review

Enable this option to require the original access review owner to review all delegated access reviews.

Line Item Delegation

Enable this option to allow certifiers to delegate individual items from an access review.

Identity Delegation

Enable this option to allow certifiers to delegate entire identities in an access review.

Disable Delegation Forwarding

Select to disallow the forwarding of a work item that was delegated by a different user.

Pre-Delegation Rule

Select a pre-delegation rule from the drop-down list. Pre-delegation rules do not support reassignments in the Targeted Certification. Use the Primary Certification field in a Certifier type rule for reassignment.

Email Owner on Pre-Delegation Completion

Send a email to the owner of the original certification upon completion of the certification by the delegates

Approve Options

Require Comments For Approval

Enable this option to require the certifier to include comments when an access review item is approved.

Enable Bulk Approval

Enable this option to allow users to bulk approve access review items.

Revoke Options

Enable Bulk Revocation

Enable this option to allow users to bulk revoke access review items.

Enable Account Revocation

Enable this option to allow users to bulk revoke all entitlements for a specific account.

Enable Bulk Account Revocation

Enable this option to allow users to revoke all entitlements for a specific account in bulk.

Require Comments for Revocation

Require the certifier to include comments when a certification item is revoked.

Allow Options

Enable Allow Exceptions (applies only to non-policy violation items)

Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.

Deprovision Items When Exception Expires (applies only to non-policy violation items)

Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations. This option is available only when the **Enable Allow Exceptions** option is also enabled.

Enable Bulk Allow Exceptions

Enable this option to allow users to allow exceptions in bulk.

Enable Allow Exception Popup

Enable this option to allow certifiers to view the Allow Exception popup and manually set expiration dates and allow comments. This applies to both violation and non-violation items.

Require Comments When Allowing Exceptions

Enable this option to require the certifier to include comments when an exception is allowed.

Default Duration for Exceptions

Set a default time period for which exceptions are allowed during the access review.

Access Review Properties

Custom Name

The name of the access review(s). If you do not enter a name here, IdentityIQ will use a default name that includes the type of the certification and the date it was generated. You can use free text as well as parameterized dates such as creation day, quarter, or year.

Custom Short Name

A shorter name for the access review(s). You can use free text as well as parameterized dates such as creation day, quarter, or year.

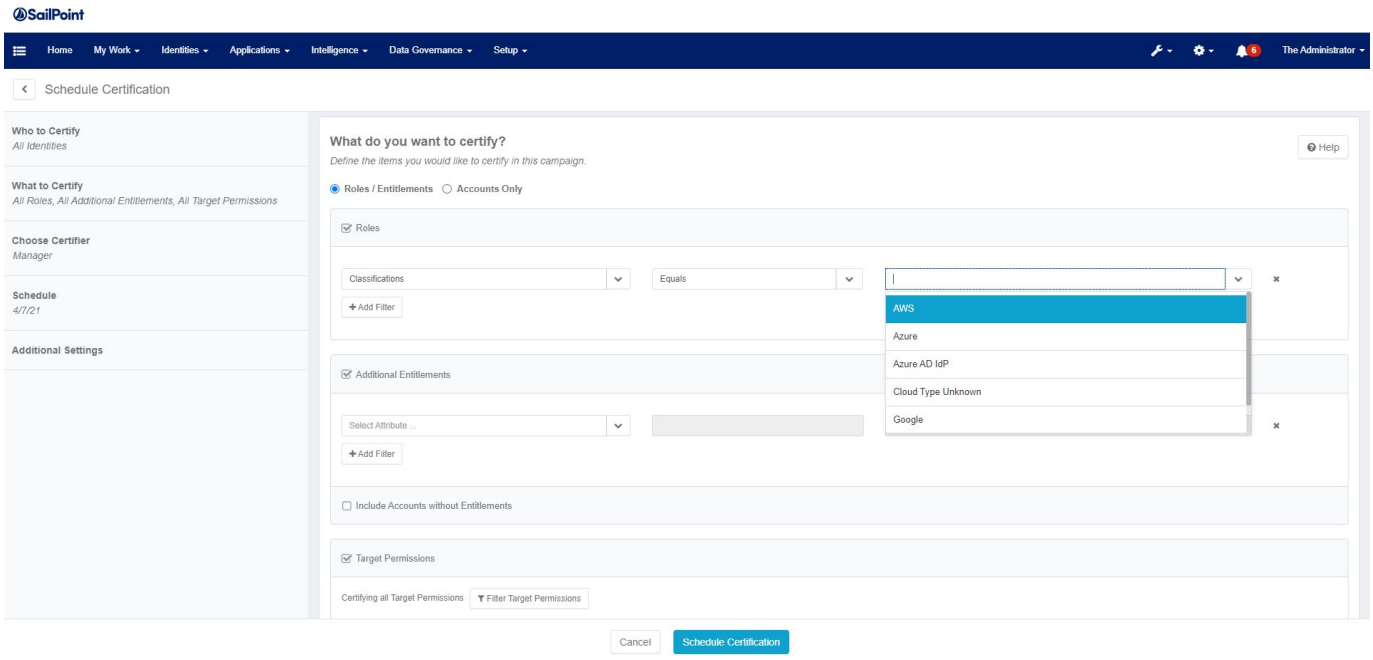
Tags

Labels that are used to classify certifications for searching and reporting.

Targeted Certifications Cloud Filtering

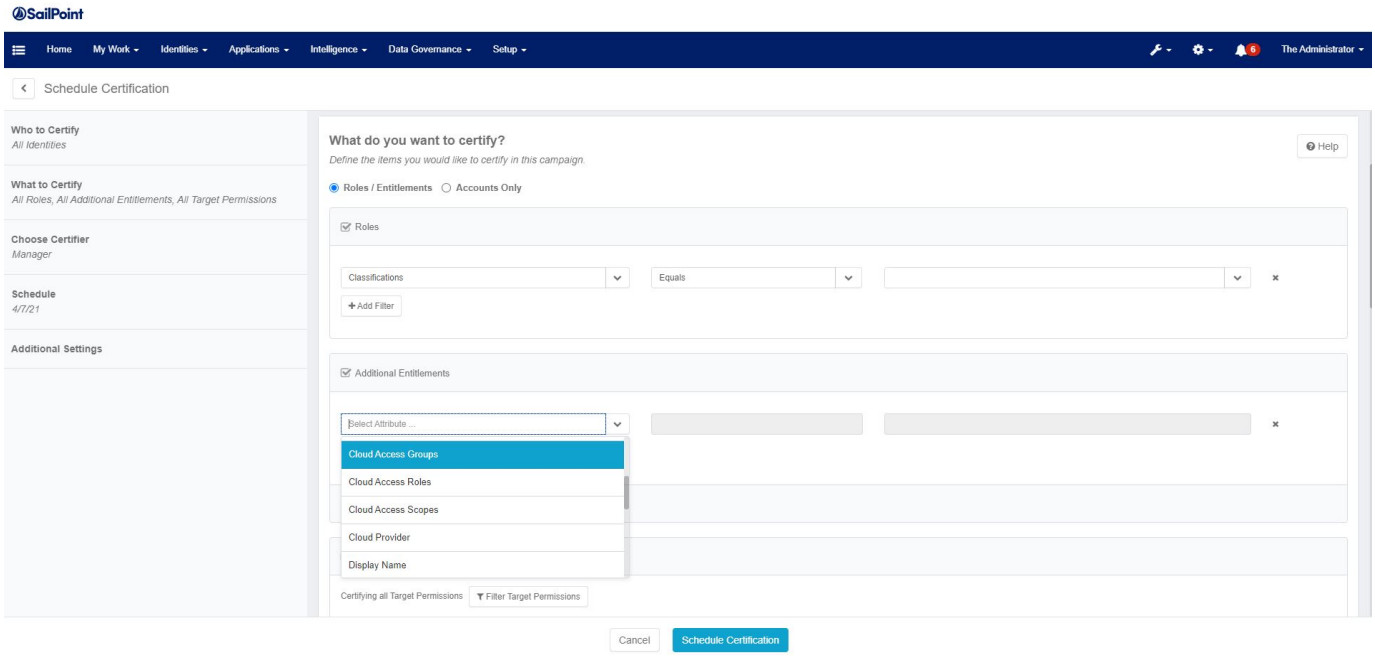
When integrated with IdentityIQ, Cloud Access Management allows the user to define a Targeted Certification to specify cloud specific selection criteria for Roles and Additional Entitlements.

The selection criteria for Targeted Certifications is used to decide which entitlements and/or roles will be included as certifiables when the certification is generated.



New search criteria have been added for Additional Entitlements. All new search criteria will appear as a pull-down option. They will only appear if Cloud Access Management is enabled.

- Cloud Access Scopes – Matches ManagedAttributes which have *any* of the given scopes indirectly from their Cloud Access Manager groups or roles.
- Cloud Access Roles – Matches ManagedAttributes which map to *any* of the given roles directly or indirectly from their Cloud Access Manager groups.
- Cloud Access Groups – Matches ManagedAttributes which map to *any* of the given groups.
- Cloud Provider – Matches ManagedAttributes which have a Cloud Access Manager group or (indirectly) a Cloud Access Manager role with *any* of the given clouds set directly.


SailPoint
Home
My Work
Identities
Applications
Intelligence
Data Governance
Setup
The Administrator
Schedule Certification
Who to Certify
All Identities
What to Certify
All Roles, All Additional Entitlements, All Target Permissions
Choose Certifier
Manager
Schedule
4/7/21
Additional Settings
What do you want to certify?
Define the items you would like to certify in this campaign.
Help
Roles / Entitlements
Accounts Only
Roles
Classifications
Equals
Add Filter
Additional Entitlements
Select Attribute ...
Cloud Access Groups
Cloud Access Roles
Cloud Access Scopes
Cloud Provider
Display Name
Certifying all Target Permissions
Filter Target Permissions
Cancel
Schedule Certification

Compliance Manager Setup

You can set global defaults for all your certifications and access reviews, in the Compliance Manager global configuration. Global settings include things like challenge and revocation periods, the options and requirements for access reviewers, which bulk actions are enabled, and email templates.

The Compliance Manager global settings determine the *default* behavior for certifications and access reviews, which can be changed at the individual certification level when the certification is scheduled. Any fields that behave differently, that is, that can not be changed by an individual certification scheduler, are noted as such in the field descriptions below.

Because configuration options are based on your deployment, your available options may not include all the options described in this document.

To access the Compliance Manager setup options, click the **gear** icon on the Navigation menu bar and choose **Compliance Manager**.

> Do not open multiple tabs or browsers when setting global configurations. Working in multiple tabs might cause changes made in one tab to overwrite changes made in the other.

Lifecycle

Lifecycle:

Notify Users of Revocations	Enabling this option will send email notifications to users that have access revoked.
Certification Escalation Rule	To apply rule-based behavior when certifications are escalated, select a rule from the drop-down. This will be default rule that the system uses when an access review is escalated.
When Exceptions Expire	Select the action performed on an exception when it expires: Do Nothing, or Notify Certifier.
Active Period Duration	The Active Period is the period when all decisions in the access reviews are made by the reviewers. Set the number and type of units (hours, days, weeks or months) to use as the default active period duration.
Enable Challenge Period	A Challenge Period is an optional period when users can challenge decisions from reviewers to remove their access privileges. If you want to enable a challenge period as your certifications' default behavior, select the option and set its default duration.
Enable Revocation Period	The Revocation Period is when all revocation work is completed. The revocation period places a limit on the amount of time a revoker has to act on a revocation request before that request work item is escalated. Select this option to enable the default revocation period and its default duration. If the revocation period is disabled, the certification will not be scanned for completed revocations, and revocation status might not be accurately reflected throughout the product.

Default Revoker	If you enable Bulk Revocations (see the Bulk Actions section below), you can choose a default user to whom all bulk remediation requests will be sent. Bulk revocation requests are made during the certification process. You can select an item from the **Select Bulk Action** drop-down list on the Certification Report worksheet view or click **Revoke All** on the Certifications Decision tab. If this field is left blank, the remediator is specified as part of the request process.
Enable Automatic Closing	Specifies that the remediation period should be enabled, during which IdentityIQ periodically scans users to determine whether the requested remediations have been carried out. Use the following options to configure the details of this process. **Time After Certification Expiration** — Select the amount of time following this access review expiration date that IdentityIQ should wait before attempting to automatically close it. **Closing Rule** — Select the rule that IdentityIQ runs at the beginning of the automatic closing process. **Action Taken On Undecided Items** — The action that IdentityIQ assigns to any undecided items when automatically closing this access review. Choose from Approve, Revoke, or Allow Exception. **Comments** — Input the comments that IdentityIQ adds to any undecided items when automatically closing this access review. **Signer** — Select the identity who signs off on automatically closed access reviews. This setting is only configurable at the system setup level. Individuals who are scheduling certifications cannot define the signer.

Behavior

Behavior:

Selection Count Requiring Bulk Revoke Confirmation	Input the number of selected items which require additional confirmation for bulk revocations.
Prompt for Sign Off	Select to display a pop-up window when an access review is complete and ready for sign off.
Require Electronic Signature	Select to require that, by default, all certifications require an electronic signature. For more information on configuring electronic signatures, see the **Electronic Signatures** section of the **IdentityIQ System Configuration** documentation.
Require Subordinate Completion	Require that, by default, all subordinate access reviews be completed before the parent access review can be completed.
Automatically Sign Off When	Automatically sign off the certification when assignee has nothing to certify.

Nothing to Certify	
Suppress Notification When Nothing to Certify	Suppress notification of certification when assignee has nothing to certify.
Require Reassignment Completion	Require that, by default, all reassigned access review items be completed before the parent access review can be completed.
Return Reassignments to Original Access Review	Specify that, by default, the content of reassigned access reviews be returned to the parent access review upon sign off. Use this option to ensure that the original content of an access review request is preserved for tracking and reporting purposes.
Automatically Sign Off When All Items Are Reassigned	Specify that an access review be automatically signed off on when all items in that access review are reassigned. This item is not available if the Required Reassignment Completion or the Return Reassignments to Original Access Review options are selected.
Require Comments for Approval	Require that all certifiers enter comments for each item they approve in an access review request.
Require Comments When Allowing Exceptions	Require the certifier to include comments when a certification decision is made.
Require Comments for Revocation	Require the certifier to include comments when a certification item is revoked.
Require a review on delegated certification items	Select to require that all access review approvers review the decision made on any user, role, entitlement, or policy violation that they delegated to another approver before they can complete the access review containing that delegation.
Require delegated certification items to be completed	Select to require that all items in a delegation work item have a decision associated with them before the work item can be marked as complete. This setting is only configurable at the system setup level. Individuals cannot change the value of this setting for a single certification.
Disable Delegation Forwarding	Select to disallow the forwarding of a work item that a different user delegated.
Allow Self Certification For	Choose which users may self-certify - that is, be the certifier for their own access, either by forwarding or reassigning an access review: All certifiers, Certification and System Administrators, System Administrators only
Self Certification Violation Owner	For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person.

	If a Self Certification Violation Owner is not specified, any items that require self-certification will be read-only to the reviewer.
Limit Reassignments	The limit reassignment feature allows you to limit the number of times the users within the certification campaign can reassign a certificate item.
Reassignment Limit	Set the number of reassignments allowed. Certification is not forwarded or reassigned when the reassignment limit is reached.
Show Classifications	Classifications can be shown in Manager, Application Owner, Advanced, Role Membership, and Targeted certifications. This setting also determines whether classification information is shown in Separation of Duties (SOD) policy violations, in the dialog for correcting violations by revoking access.
Show Elevated Access	Displays elevated access on roles and entitlements in access reviews.

Decisions

Decisions:

Enable Provisioning Missing Role Requirements	Enable the certifier to provision missing role requirements from within an access review.
Enable Line Item Delegation	Enables certifiers to delegate individual access review items, such as a single role or entitlement, rather than the entire identity to be reviewed. This option also enables the delegation of policy violations, either from inside an access certification or from the Manage -> Policy Violations page.
Enable Account Revocation	Allows the certifier to revoke an account, when its associated entitlements are also revoked. Note that disabling this option does not prevent the reviewer from revoking accounts directly - it only enables or disables the "revoke account" option when entitlements are being certified..
Enable Identity Delegation	Enable certifiers to delegate entire identities from a certification request.
Enable Allow Exceptions (applies only to non-policy violation items)	Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.
Deprovision Items When Exception Expires (applies only to non-policy violation items)	Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations.

Enable Allow Exception Popup	Enables certifiers to view the Allow Exception pop-up and manually set expiration dates.
Default Duration for Exceptions	Set the time period during which exceptions should be allowed. Input the number of units and unit type (hours, days, weeks or months) to use as the exception duration.
Default Operation for Remediation Modifiable Attributes	Set the default operation shown on the revocation dialog for remediation-modifiable attributes.
Show Recommendations	This option is only visible if you have purchased and activated the SailPoint AI Services product. Enable recommendations from AI Services to display in access reviews.
Automatically Approve Recommended Items	This option is only visible if you have purchased and activated the SailPoint AI Services product. Enable access review items to be automatically marked as approved by AI Services and move to the Access Certification Review tab for final approval.

Bulk Actions

Bulk Actions:

Select the actions to enable from the Worksheet/Identity view and the Detail view. The actions include the following:

- Enable Bulk Approve
- Enable Bulk Revocation
- Enable Bulk Allow Exceptions
- Enable Bulk Reassignment
- Enable Bulk Account Revocation
- Enable Bulk Clear Decisions

Certification Contents

Certification Contents:

Additional Entitlement Granularity	The default granularity at which additional entitlements are listed in the access review. For example, if you select **Attribute/Permission**, each permission associated with each attribute is listed, and must be acted upon, separately.
Exclude Logical Tier Entitlements	Exclude entitlements on tier application accounts from the access review. This only applies to logical applications. Tier applications are those application that make up a logical application.

Generate Certification(s)	Specify whether, by default, access review requests should generate an access review request for the specified managers, or for the specified managers and all employees below them in the reporting hierarchy. If you select **For the specified manager(s) only**, the **Flatten Hierarchy** option is displayed. Select the **Flatten Hierarchy** option to include all of the employees that report directory to the selected managers and the employees that report to their subordinate managers on the access review request.

Email Templates

Email Templates:
Much of the communication performed during the access review process is done through email notifications sent automatically by IdentityIQ as an access review proceeds through its life cycle. Use this section to specify the template to use for each certification-related notice.