

Lifecycle of a Certification

IdentityIQ Versions: 5.5, 6.0, 6.1, 6.2, 6.3, 6.4

This document guides the reader through the Lifecycle of a Certification and its associated Access Reviews. It describes how various Rules and Tasks affect the progression of an Access Review from generation to its end phase. It also explains how specific parameters in the certification specification affect its progression through the lifecycle phases. Though many details are included here that are important for the creation of a Certification, this is not a step-by-step instruction guide for certification creation. Instructions for creating a certification through the user interface are available in the User Guide or through the online context-sensitive help.

Document Revision History

| Revision Date | Written/Edited By | Comments |
|---------------|-------------------|--|
| Jan 27, 2012 | Jennifer Mitchell | Initial Creation |
| July 2013 | Jennifer Mitchell | Corrected error: cert does not bypass revocation period if no revokes requested |
| Feb 2014 | Jennifer Mitchell | Updated for version 6.2; added partitioned manager certification configuration details; also added info on staging period and existing-cert-as-template functionality (both added in 6.0) |
| Nov 2014 | Jennifer Mitchell | Fixed broken cross-reference links in doc |
| April 2015 | Jennifer Mitchell | Updated to reflect compatibility with version 6.3 and 6.4; added details on changes to reminder/escalations configuration options made in 6.0 and made small verbiage changes for clarity in other areas |

© Copyright 2014 SailPoint Technologies, Inc., All Rights Reserved.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Restricted Rights Legend. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and reexport of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or reexport outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Entities List; a party prohibited from participation in export or reexport transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Trademark Notices. Copyright © 2014 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo, SailPoint IdentityIQ, and SailPoint Identity Analyzer are trademarks of SailPoint Technologies, Inc. and may not be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

Table of Contents

| | |
|---|----|
| Lifecycle Overview | 5 |
| Terminology | 5 |
| Certification Generation | 6 |
| Specification | 6 |
| Types of Certifications | 6 |
| Basic | 7 |
| Lifecycle | 8 |
| Notifications | 9 |
| Behavior | 9 |
| Advanced | 10 |
| Creating a New Certification from an Existing One | 10 |
| Execution | 11 |
| Exclusion Rule | 12 |
| Pre-Delegation Rule | 12 |
| Partitioned Certification | 13 |
| Partitioning Configuration | 13 |
| Staging Period | 14 |
| Notification | 15 |
| Active Phase | 16 |
| Certification Reminders and Escalations | 16 |
| Challenge Phase | 18 |
| Sign-Off | 19 |
| Remediation and the Revocation Phase | 19 |
| Revocation Reminders and Escalations | 20 |
| End Phase | 21 |
| Automatic Closing | 22 |
| Continuous Certifications | 22 |
| Certification Events | 25 |
| Summary of Rules Triggered by Certifications | 27 |
| Rules Configured during Certification Specification | 27 |
| Other Certification-Related Rules | 28 |

| | |
|---|----|
| Summary of Tasks affecting Certifications | 29 |
| Setting Certification Defaults | 30 |

Lifecycle Overview

The certification process in IdentityIQ allows Identities' access privileges to be reviewed and managed by designated reviewers through system-generated Access Reviews. All certifications proceed through several phases from initial generation to completion. The diagram below illustrates the complete certification progression when all phases are enabled.

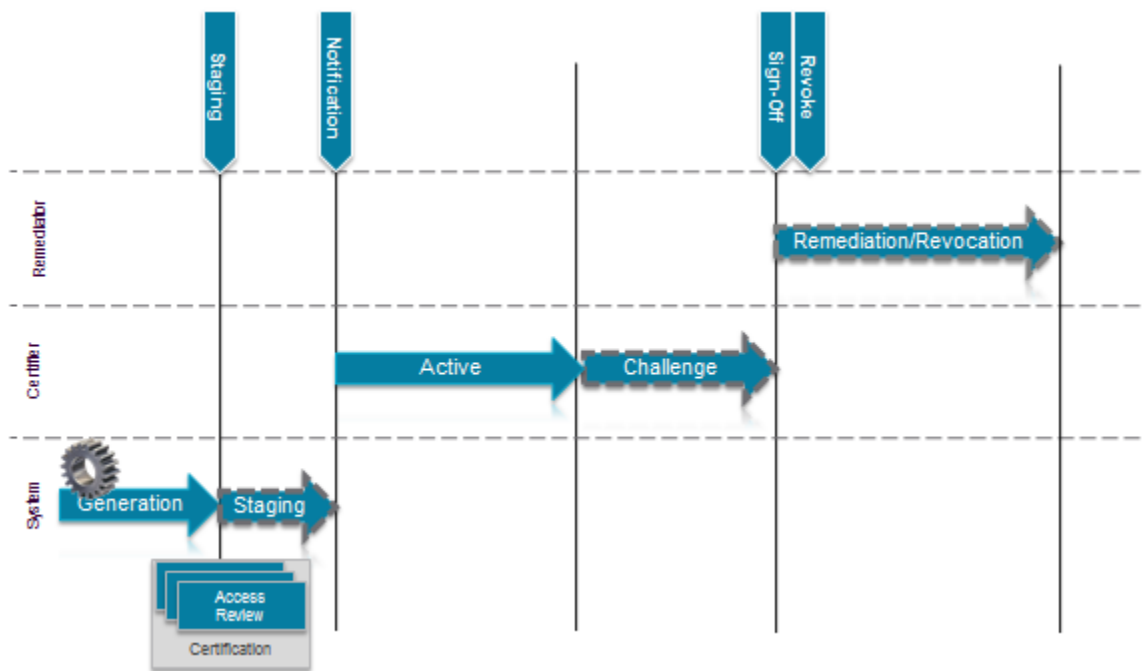


Figure 1: Certification and Access Review Lifecycle

All certifications include Generation, the Active Phase, Sign-Off, and the End Phase. Each certification can be configured to include some or all of the other available phases and events.

This document describes the lifecycle of a certification. It includes discussions of how to configure the required and optional phases, what rules can be created that affect the certification at different phases, and what built-in tasks impact the progression of a certification through its phases.

Terminology

IdentityIQ currently uses two distinct constructs in the certification process that often get confused with each other. These are:

- Certification
- Access Review

In IdentityIQ releases prior to 5.1, only the concept of a "Certification" existed, and it was a set of data to be reviewed and approved (or revoked) by a single reviewer, or certifier. Beginning with Release 5.1, the capabilities of certifications expanded so that a single certification specification could create more than one set

of data for review and could designate separate certifiers for each. From that point forward, the individual datasets were referred to as “Access Reviews” while the larger grouping was called the “Certification”. Now, an authorized user specifies the parameters for a certification, which then creates one or more Access Reviews for review by the appropriate certifier(s).

Certification Generation

The certification generation process is divided into two parts:

- Specification: configuration of the certification parameters
- Execution: creation of the Access Review dataset(s) at the scheduled time based on the parameters

Specification

The first step in creating a certification is the specification. The parameters specified for the certification identify the data to be included in the Access Reviews and dictates which phases will be applied to the certification.

Each individual certification specification can set up a different phase progression. For example, the organization may want to include a Challenge period in a manager certification but may choose not to select that for an application owner certification. In fact, it is permissible to enable a phase (like a Challenge period) for one manager certification and not for another. The specifications selected for one certification are completely independent from those selected for the next.

Types of Certifications

The certification type must be selected before any of the parameters can be set. Click the **New Certification** list on the **Monitor** -> **Certifications** window to choose the certification type.

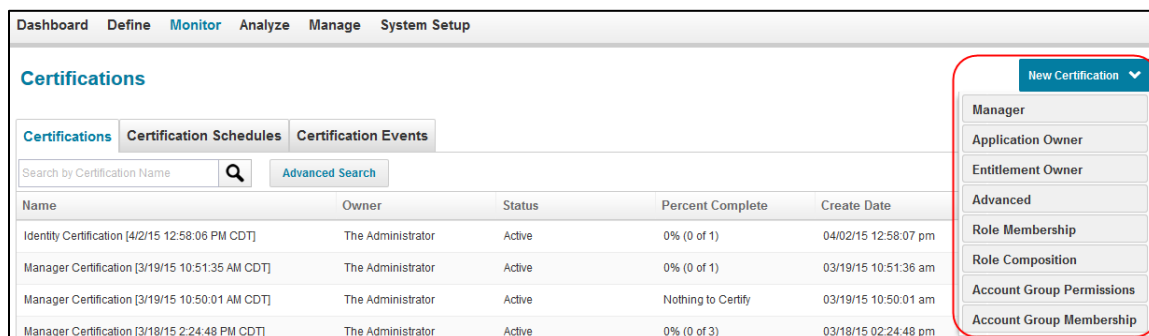


Figure 2: New certification List

The table below identifies each of the available certification types in IdentityIQ and briefly describes their usage. The details reported in each of these certification types vary, but the overall certification process is the same for all types.

| Certification Type | Description/Usage |
|--------------------|--|
| Manager | Shows a manager the access granted to direct reports to confirm that they have the entitlements they need to do their job but no more than |

| | |
|---------------------------|---|
| | they need |
| Application Owner | Lists all identities and their entitlements related to a specific application so the owner of that application can confirm that all entitlements to the application are appropriate |
| Entitlement Owner | Most useful for managed entitlements owned by an individual; Lists identities with a specific entitlement for the entitlement owner to certify |
| Advanced | Allows for creation of custom certifications based on Groups or Populations |
| Role Membership | Lists identities connected to specified Role(s) |
| Role Composition | Shows assignments or Entitlements that are encapsulated within Roles (Role set reported can be filtered) |
| Account Group Permissions | List the permissions that constitute an Account Group for selected application(s) |
| Account Group Membership | Lists identities assigned to one or more Account Groups |

The specification for any certification, regardless of type, is divided into 5 pages in the IdentityIQ user interface:

- Basic
- Lifecycle
- Notifications
- Behavior
- Advanced

Each of these pages is described more fully in the sections to follow.

Basic

The Basic page allows the administrator to name and assign ownership of the certification, specify filters that are applied to the certification data, and set the frequency and timing of the certification execution.

The specific parameters available for filtering the certification vary based on the type of certification selected. For example, in a Manager certification, the Manager and the Applications to certify can be specified as filter criteria; for a Role Membership or Role Composition certification, the filter options include the Roles that will be certified.

The **When to Certify** section of this page determines the scheduling and frequency of each certification. See the *Execution* section for more details.

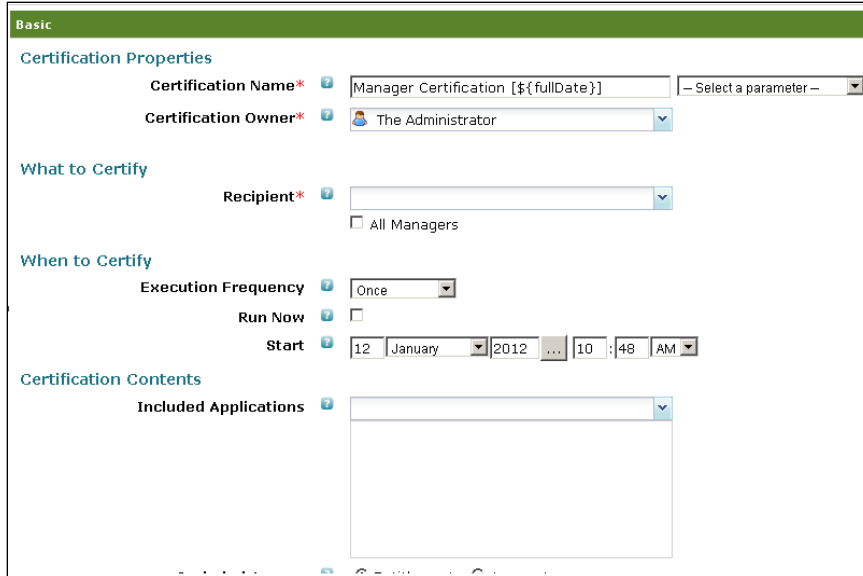


Figure 3: Basic Page for a Manager Certification

Lifecycle

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:

- The Rules run at the beginning of the Access Reviews' various phases
- The duration of the Active period (see Active)
- The inclusion of a Challenge period (see *Challenge Phase*)
- The inclusion of a Revocation period (see *Remediation and the Revocation Phase*)
- The timing of revocation request submission
- The closing of incomplete certifications after expiration (see *Automatic Closing*)

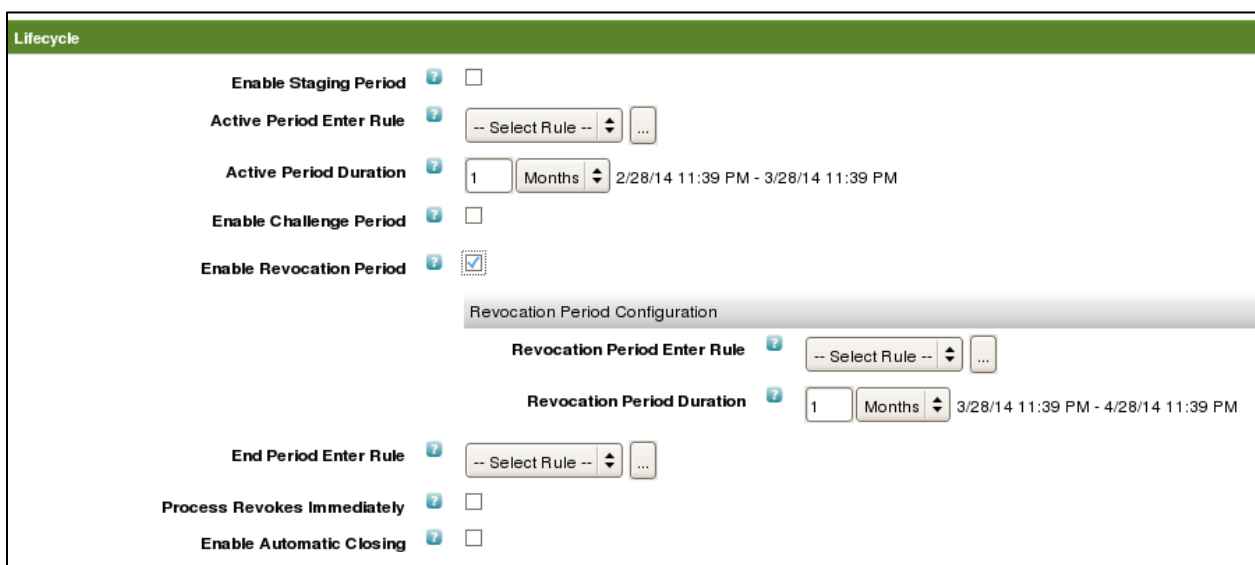


Figure 4: Lifecycle Page for a Manager Certification

Some Lifecycle options are not applicable to all certification types and are therefore not shown on all certifications' Lifecycle pages. For example, Role Membership and Role Composition certifications do not include a Challenge Period option and Account Group Membership and Permissions certifications do not include a Revocation Period option.

Notifications

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.

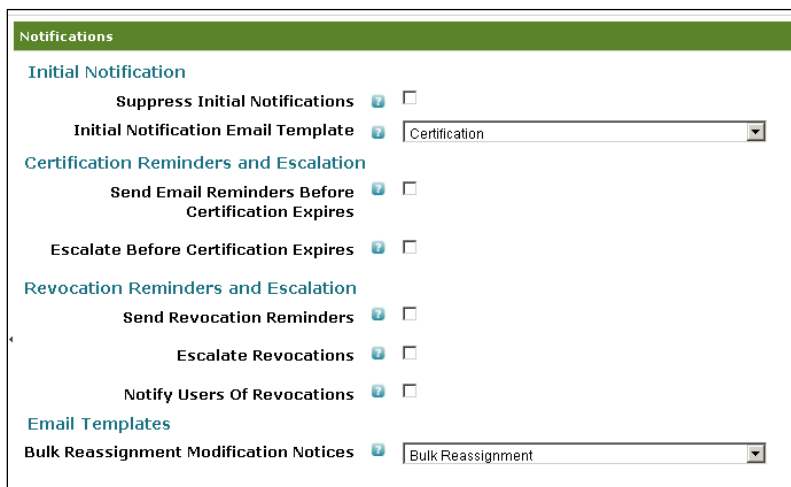


Figure 5: Notifications Page for a Role Membership Certification

The various notification types are described in more detail in this document in the sections related to the phases in which each notification should occur (see *Notification*, *Certification Reminders and Escalations*, and *Revocation Reminders and Escalations*).

Behavior

The Behavior tab is used to specify how certifiers view and can 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.

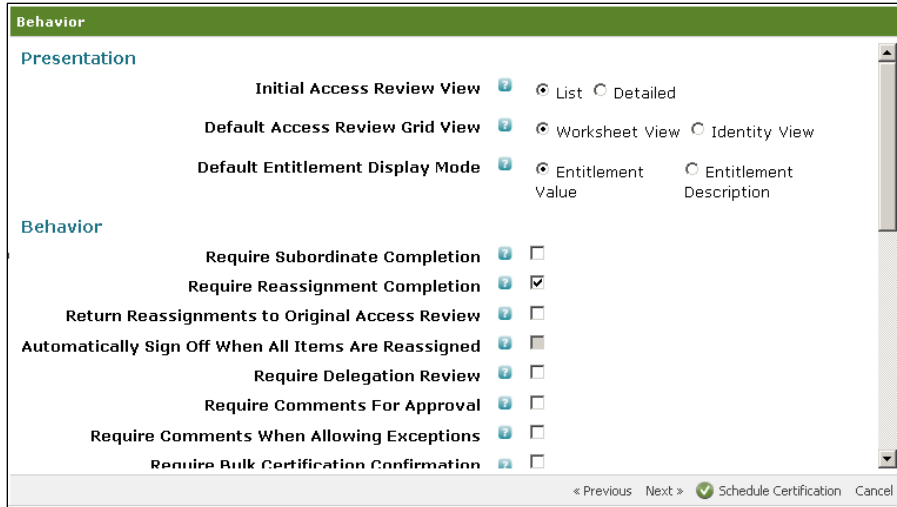


Figure 6: Behavior Page for a Manager Certification

Advanced

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 specification of 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. Finally, the certification's Pre-delegation and Sign-Off Approver Rules can be specified on this page, if applicable. (See *Pre-Delegation Rule* and *Sign-Off* for details on those rules.)

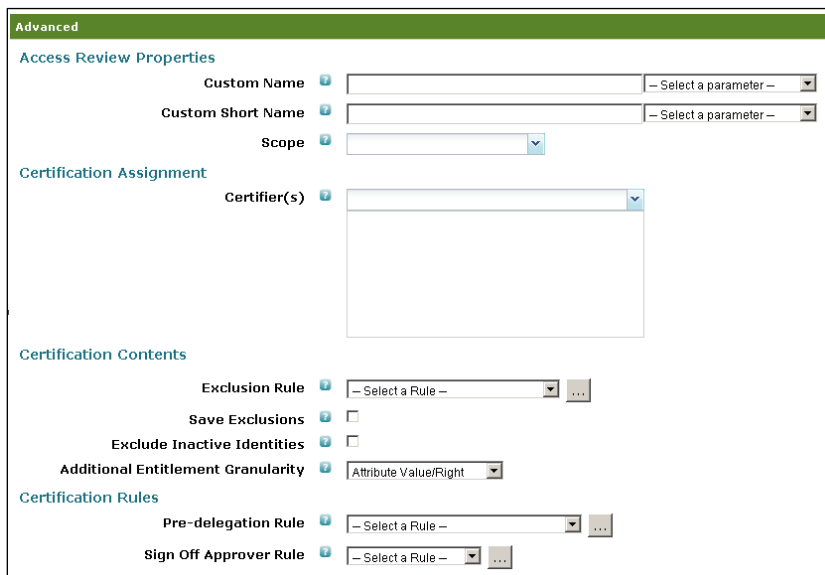


Figure 7: Advanced Page for Application Owner Certification

Creating a New Certification from an Existing One

Beginning with IdentityIQ Version 6.0, new certifications can be created from existing certification definitions so the existing certification definition provides a starting point for configuring the new certification. To do this, right-click a certification on the **Manage -> Certifications** page and click **Use Certification as a Template**.

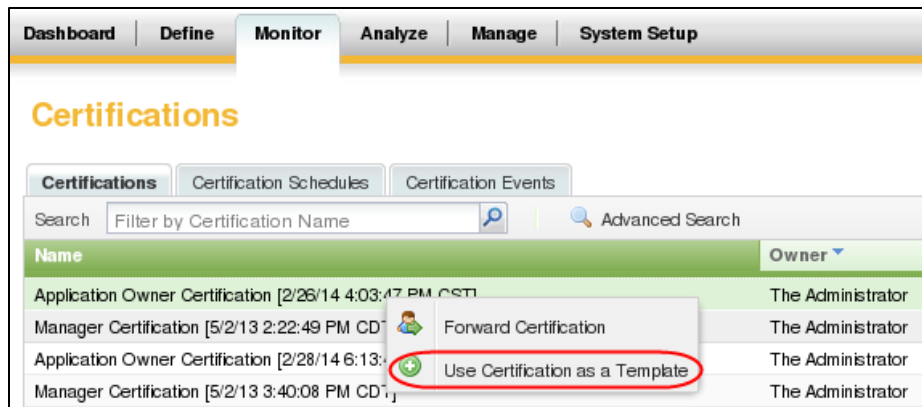


Figure 8: Using a Certification as a Template

Then modify the certification specification as needed for the new certification.

Execution

Once the certification parameters have all been specified, clicking **Schedule Certification** schedules it for execution. The certification will be executed according to the parameters specified in the **When to Certify** section.

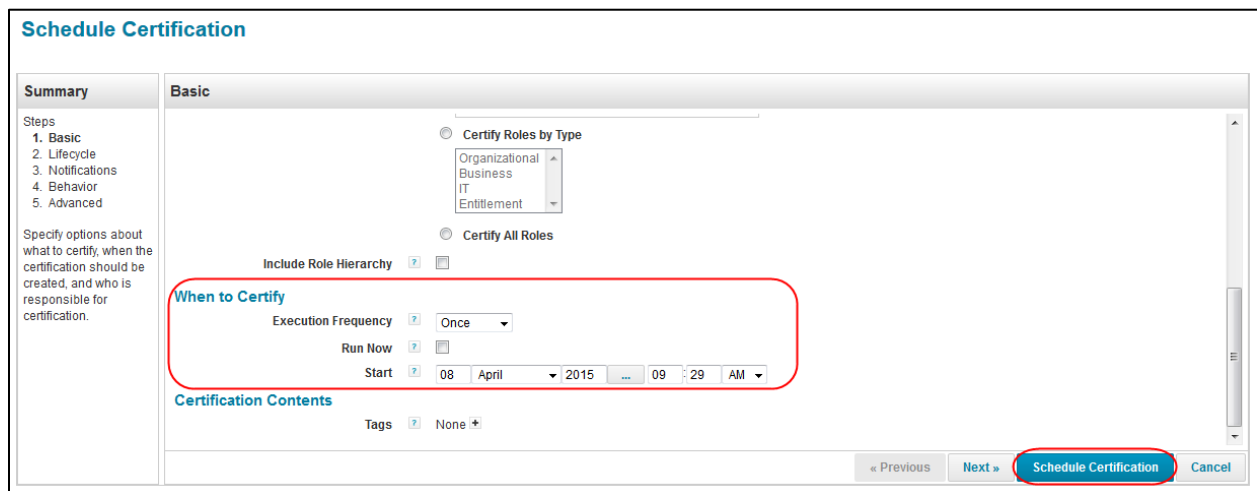


Figure 9: Scheduling Certification Execution

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.)

During Execution, two Rules are run if they were written and selected for the certification:

- Exclusion Rule: excludes Identities or Entitlements from Access Reviews
- Pre-Delegation Rule: delegates review of Identities or line-items to someone other than the certifier before the certifier must review and approve them

Exclusion Rule

The Exclusion Rule applies logic to the list of items being certified to exclude entities or Entitlements from the certification's Access Reviews. Any attribute of the Entity or Items (see rule arguments below) can be evaluated and used to exclude them from the Access Reviews.

Arguments for an Exclusion Rule are:

| Type | Argument | Description |
|--------|----------------|---|
| Input | Log | Log4j object used for debugging |
| | Context | SailPointContext object that can be used to query the database or execute other SailPointContext services |
| | Entity | The AbstractCertifiableEntity to potentially exclude. Currently, this is either an Identity, an AccountGroup, or a Bundle (role object). |
| | Certification | The Access Review being created. |
| | CertContext | The CertificationContext that is being used to generate the certification. |
| | Items | List of Certifiable items that are currently part of the certification for this identity. Any items that should be excluded from the certification should be deleted from this list and added to the itemsToExclude list by the Rule's logic. |
| | ItemsToExclude | A List of Certifiable items that should not be included in the certification. This list will be empty when the rule is executed. Any items that should not be part of the certification should be moved from the items list to the itemsToExclude list in the Rule's logic. |
| Return | Explanation | An optional explanation describing why the items were excluded. |

These are some examples of exclusions that could be applied with an Exclusion rule:

- Exclude "inactive" Identities from a Manager certification
- Exclude specific Account Groups from an Account Group Membership certification
- Exclude accounts that are part of a Composite Account from a certification
- Exclude certain Roles from an Application Owner certification
- Exclude items from a certification when they have already been included in another active certification

Pre-Delegation Rule

A Pre-Delegation Rule can be written to automatically delegate some entities to other reviewers before the certifier even sees them. Depending on the options selected on the certification's Behavior page, certifiers can usually manually delegate Identities or line-items to other reviewers during their review process. This rule automates that delegation without requiring the certifier's direct involvement, which can streamline the Access Review when review of the items by someone other than the certifier is part of the organization's standard process.

For example, in some organizations, the Manager might be responsible for the access review but team Leads are charged with reviewing their group's Entitlements before they are sent to the Manager. A pre-delegation rule can be written to pre-delegate items to the Leads. When the Leads' reviews are complete, the items are returned to the Manager for final approval and sign-off.

Any Entity attribute can be used to identify items for pre-delegation.

Arguments for a Pre-Delegation Rule are:

| Type | Argument | Description |
|--------|-------------------|--|
| Input | Log | Log4j object used for debugging |
| | Context | SailPointContext object that can be used to query the database or execute other SailPointContext services |
| | Entity | The AbstractCertifiableEntity to potentially delegate. Currently, this is either an Identity, an AccountGroup, or a Bundle (role object). |
| | Certification | The Access Review being created. |
| | CertContext | The CertificationContext that is being used to generate the certification. |
| Return | RecipientName | The name of the Identity that should certify this entity. Either this or 'recipient' should be non-null if pre-delegation should be performed. |
| | Recipient | The Identity that should certify this entity. Either this or 'recipientName' should be non-null if pre-delegation should be performed. |
| | Description | Optional description to set on the delegation WorkItem. If null, a default description of "Certify [entity name]" is used. |
| | Comments | Optional comments to set on the delegation WorkItems. |
| | Reassign | Optional Boolean value to specify that the item should be reassigned, rather than delegated. |
| | CertificationName | Optional string to specify the name for the reassignment Access Review if creating a new Access Review for reassignment. This field is ignored for delegations (when Reassign is False). |

Partitioned Certification

IdentityIQ Version 6.2 introduced the option of partitioning manager certifications across multiple processing threads. This is particularly useful for global manager certifications which are generating certifications for all managers in the organization and are thus processing large volumes of data.

To turn on partitioning for a Manager certification, go to the **Advanced** page of the certification specification and choose **Enable Partitioning**.



Sign Off Approver Rule ? -- Select Rule -- ...

Partitioning Options

Enable Partitioning ? ☒

Figure 10: Partitioning Configuration Option

Partitioning Configuration

Partitioning for manager certifications is configured through values in these objects:

| Configuration Object/Location | Usage/Purpose |
|-------------------------------|---|
| RequestDefinition object: | maxThreads attribute specifies the maximum number of threads to use for |

| | |
|---|--|
| Manager Certification Generation Partition | certification generation on each request host |
| ServiceDefinition object: <i>Request</i> (or iiq.properties file) | Specifies which hosts are request hosts, which causes IdentityIQ to start the request service on those hosts |
| Server objects: all | <p>Created for each host that connects to the IdentityIQ database; each host is examined to verify whether the request service has been started on it (and thus whether the host is a request server that can be used for certification generation)</p> <p>Also specify maxRequestThreads values that indicate the number of available request threads on each server, which may constrain the number of partitions if this value is lower than the RequestDefinition maxThreads value</p> |

The number of partitions is calculated like this:

$$\text{Partitions} = \text{RequestDefinition MaxThreads} * \text{number of request hosts}$$

The total number of managers in the certification is then divided evenly across the partitions for processing.

NOTE: Individual servers can be constrained to process fewer threads by specifying a maxRequestThreads value in the Server object for that server. In that case, the calculated number of partitions is reduced by the difference between the RequestDefinition maxThreads and Server maxRequestThreads values.

If the number of partitions calculated for the certification exceeds the number of available processing threads at the time the certification is launched (e.g. because other processes are consuming some of the available threads), the extra partitions will be queued and processed as threads become available.

Refer to the Partitioning Best Practices white paper for more details on partitioning configuration.

Staging Period

IdentityIQ Version 6.0 introduced the concept of a Staging period to the certification lifecycle. This period allows certification administrators a time period in which they can examine the certification after it is generated but before notifications are sent to certifiers to begin their review processes.

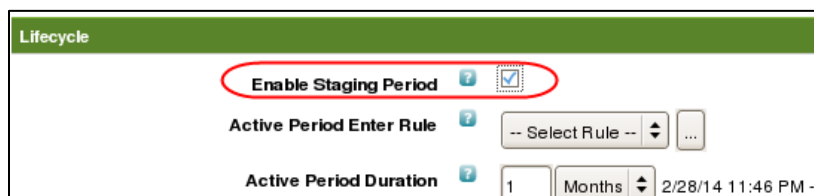


Figure 11: Specification of a Staging Period

The staging period is most useful when a new certification campaign is being defined and executed for the first time; the results of the certification specification can be examined to confirm that the reviews generated match the intentions and that no configuration errors were made. Without this staging period, certifiers would be notified to begin their reviews immediately, and some might even complete their reviews before a configuration error is discovered that might require the entire campaign to be discarded and recreated. All of the confusion

and frustration resulting from a mistake like that can be avoided by implementing the staging period. When the certification is examined and found to be correct, it can be activated; if errors are found, it can be canceled and recreated.

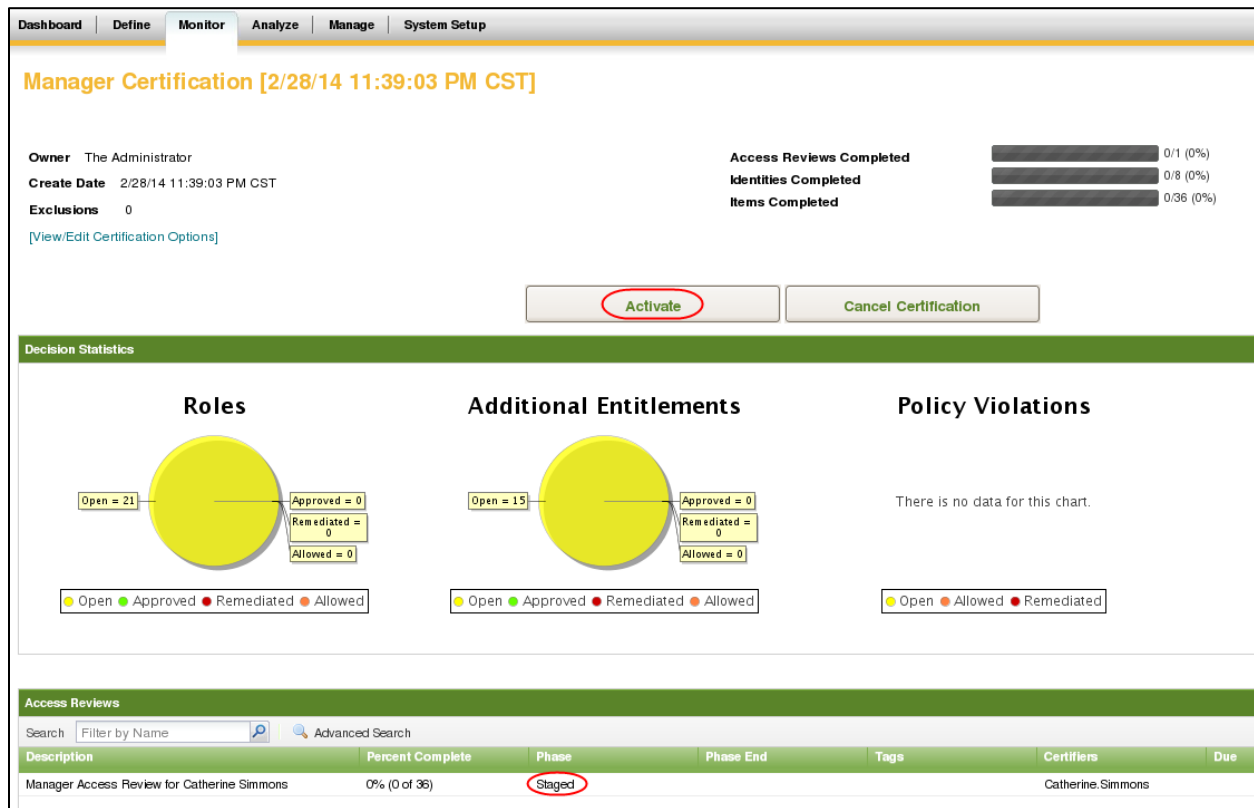
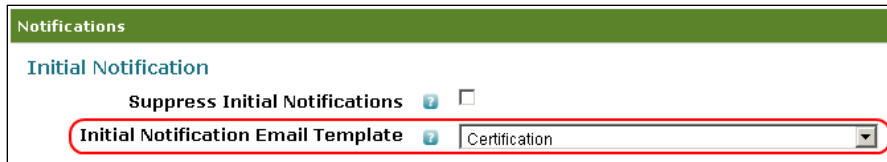


Figure 12: Staged Certification Ready for Activation (or Cancellation)

NOTE: Administrators who discover an error in a staged certification may want to use the staged certification as a template, especially if the changes they need to make to it are fairly minor. This can be done as described in the *Creating a New Certification from an Existing One* section above, but this must be done *before* clicking **Cancel Certification** inside the staged certification because canceling the certification deletes the whole certification from the system.

Notification


Once the certification has been generated (and activated, in the case of one where the Staging Period was enabled), the default behavior in IdentityIQ is to send an email to the certifiers to notify them of their awaiting Access Reviews. The email text is created in a template, selected as the **Initial Notification Email Template** on the Notifications page of the certification specification. The template can use attributes of the certification, Recipient, and Sender objects in building the email text.



The screenshot shows the 'Notifications' section with the 'Initial Notification' sub-section. The 'Initial Notification Email Template' dropdown menu is highlighted with a red box and set to 'Certification'. The 'Suppress Initial Notifications' checkbox is unchecked.

Figure 13: Notification Template Selection

This Notification step can be bypassed in the Access Review process by selecting **Suppress Initial Notifications** on the Notifications page of the certification specification. This is generally only done when an alternate process for notifying certifiers is being used. For example, if a single Manager certification process generated Access Reviews for 2000 managers, the organization might choose to send notifications to the managers over a period of several days to limit the number of people trying to complete reviews at one time, thereby minimizing the risk of overloading the system and creating performance problems.

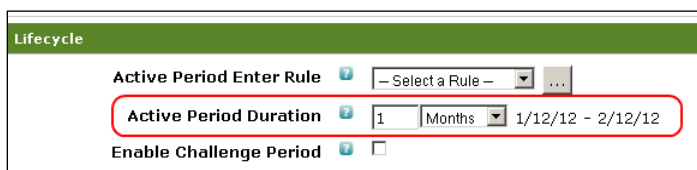


The screenshot shows the 'Notifications' section with the 'Initial Notification' sub-section. The 'Suppress Initial Notifications' checkbox is checked and highlighted with a red box. The 'Initial Notification Email Template' dropdown menu is set to 'Certification'.

Figure 14: Bypassing Initial Certification Notification

Active Phase

The Active Phase is the timeframe during which certifiers are expected to complete their reviews and make approval and revocation decisions. Item delegations and reassignments are also done during this period, if permitted by the certification definition. The Active Phase ends when the when its end date/time is reached (calculated based on the Active Period Duration specified on the certification's Lifecycle page). If no Challenge Phase is enabled, the Active Phase can end early, when the certifier signs off on the access review.



The screenshot shows the 'Lifecycle' section with the 'Active Period Duration' configuration. The 'Active Period Duration' is set to '1' month, with a date range of '1/12/12 - 2/12/12' displayed. The 'Active Period Enter Rule' dropdown is set to '- Select a Rule -'. The 'Enable Challenge Period' checkbox is unchecked.

Figure 15: Active Period Timeframe Identified

Certification Reminders and Escalations

Certifications can be configured to send reminders to the certifiers during the Active period if they have not yet completed and signed-off on their Access Reviews. When **Send Email Reminders Before Certification Expires** is selected, the **Reminder Policy** options are displayed for configuration. Reminders can be sent once or at scheduled intervals, beginning a specified number of days before the end of the Active Phase. The template for these emails is also specified in these policy options.

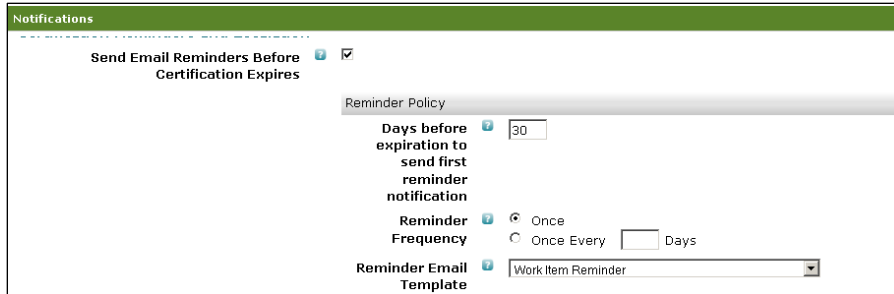


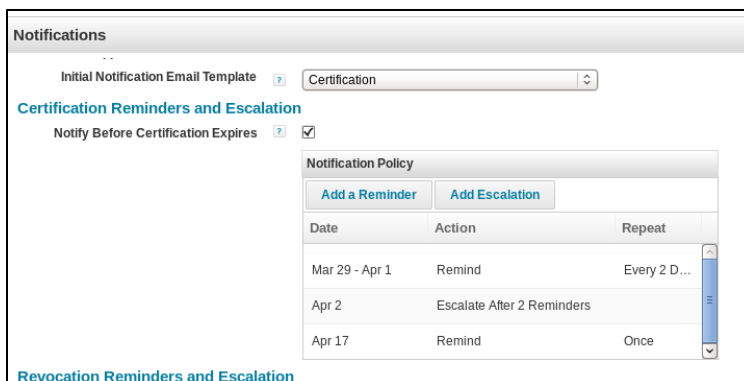
Figure 16: Certification Reminder Configuration

Escalation can be used to notify someone else (often 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. When **Escalate Before Certification Expires** is selected, the **Escalation Policy** options can be seen and set. The **Escalation Trigger** determines how far in advance of the end of the Active Phase the escalation occurs. The **Escalation Rule** determines who gets the escalation notice. The format of the email depends on the **Escalation Email Template** selected.



Figure 17: Certification Escalation Configuration

NOTE: The details around configuring reminders and escalations of certification work items changed in version 6.0, adding increased flexibility to the configuration. In that and subsequent releases, each reminder or escalation can be specified individually with its own date (or date range), email template, etc. This means that different messages, cc configurations, and escalation recipients can be specified for each step in the reminder/escalation process.



| Date | Action | Repeat |
|----------------|----------------------------|--------------|
| Mar 29 - Apr 1 | Remind | Every 2 D... |
| Apr 2 | Escalate After 2 Reminders | |
| Apr 17 | Remind | Once |

Figure 18: 6.0+ Reminder/Escalation Configuration

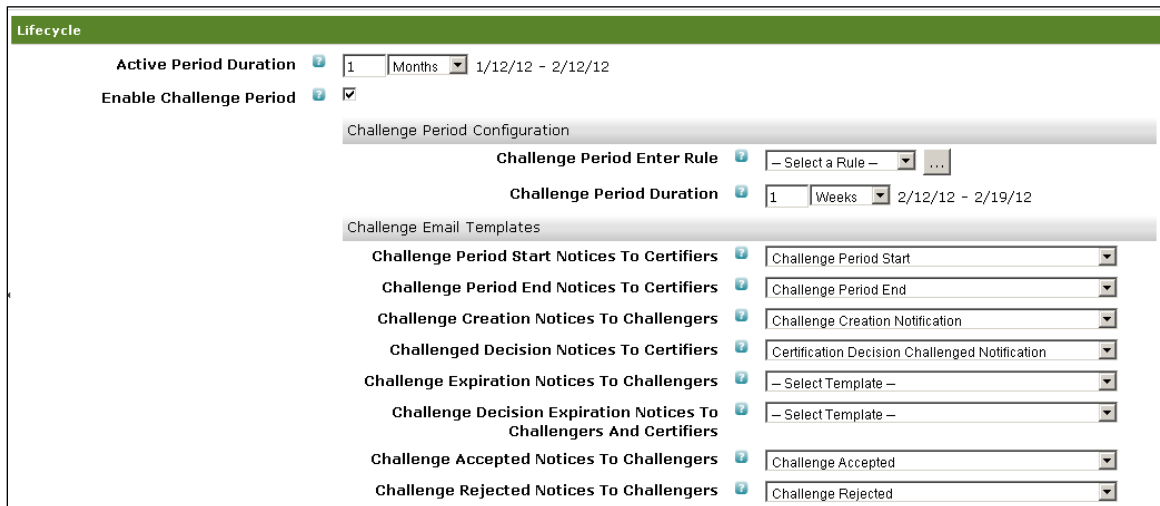
Reminders and Escalations are tied to the work item (in this case the Access Review work item assigned to the certifier). If the work item is not marked complete when the dates for sending reminders or triggering escalations are reached, the specified actions are automatically taken by the system. Escalations and reminders

are managed by the system task called Check Expired Work Items. This task is, by default, scheduled to run once a day at midnight, though it can be scheduled to run more frequently or at a different time if desired. Work Items get marked as “expired” when the next date/time for processing a configured reminder or escalation is reached. (Instructions for testing escalation rules in a development environment without waiting several days for escalation periods to pass can be found in the [Testing Certification Reminders and Escalation Rules](#) Technical White Paper on Compass.)

Challenge Phase

The Challenge Phase begins when the Active Period Duration is over for the Access Review. Identities are then notified of revocation decisions affecting their Entitlements, and they have the option to dispute the revocation and offer an argument for why they need to retain the Entitlement. The certifier may consider their argument and potentially change the decision based on that additional information.

This Access Review phase is only applicable if “Enable Challenge Period” was selected on the Lifecycle page of the certification specification. When that option is selected, other parameters are displayed on the Lifecycle page that will control various aspects of the period. These include the Challenge period duration, the rule to run when the period begins, and the email templates used for notifications to challengers and certifiers during the challenge process.



The screenshot shows the 'Lifecycle' configuration page. At the top, 'Active Period Duration' is set to 1 Month, with a date range of 1/12/12 - 2/12/12. Below this, 'Enable Challenge Period' is checked. The 'Challenge Period Configuration' section includes 'Challenge Period Enter Rule' (set to '- Select a Rule -') and 'Challenge Period Duration' (set to 1 Week, with a date range of 2/12/12 - 2/19/12). The 'Challenge Email Templates' section lists several notification templates: 'Challenge Period Start Notices To Certifiers' (Challenge Period Start), 'Challenge Period End Notices To Certifiers' (Challenge Period End), 'Challenge Creation Notices To Challengers' (Challenge Creation Notification), 'Challenged Decision Notices To Certifiers' (Certification Decision Challenged Notification), 'Challenge Expiration Notices To Challengers' (- Select Template -), 'Challenge Decision Expiration Notices To Challengers And Certifiers' (- Select Template -), 'Challenge Accepted Notices To Challengers' (Challenge Accepted), and 'Challenge Rejected Notices To Challengers' (Challenge Rejected).

Figure 19: Challenge Period Configuration Parameters

NOTE: When the Challenge Period is enabled *and* **Process Revokes Immediately** is also selected, the Challenge Period for each revocation begins immediately when the revocation decision is saved by the certifier and may run concurrently with the Access Review’s Active Period. In this case the **Challenge Period Duration** applies to each revocation request from the moment the request is created instead of from the end of the Active Period. The date range that normally appears next to **Challenge Period Duration** is therefore omitted from the display, as it is not the same for all challenge items. Additionally, the Access Review’s Phase may still be marked as “Active” while challenges are being processed; the review’s phase will not be marked as the “Challenge” phase until

the Active Period Duration is over. Additionally in this case, the Challenge Period Enter Rule runs once for each item as it enters the Challenge Phase, instead of once for the whole Access Review.

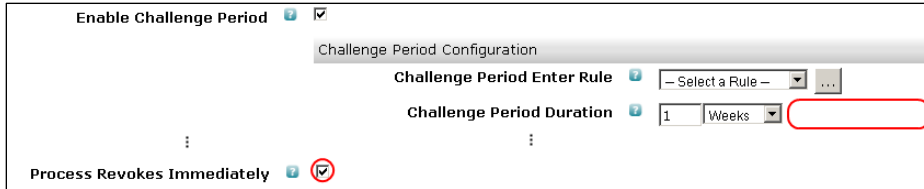


Figure 20: Enable Challenge Period and Process Revokes Immediately selected simultaneously

Sign-Off

When all of the required decisions have been made for the Access Review items (and if a Challenge Period was enabled, all challenges have been addressed or the challenge period has ended), the certifier must click **Sign Off** to complete the review process. Sign-off puts the Access Review into a read-only status that disallows any further changes to the review decisions.

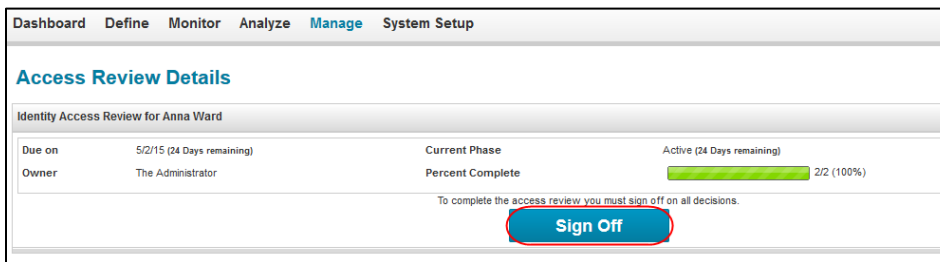


Figure 21: Certification Sign Off

Clicking Sign Off also triggers any Sign off Approver Rule that has been written and selected for the certification (on the Advanced page). The Sign off Approver Rule enables two-level sign-off by identifying a second-level approver Identity to whom the certification should be routed following initial sign-off. (This rule can implement multiple sign-off levels if desired; it is not limited to only two.)

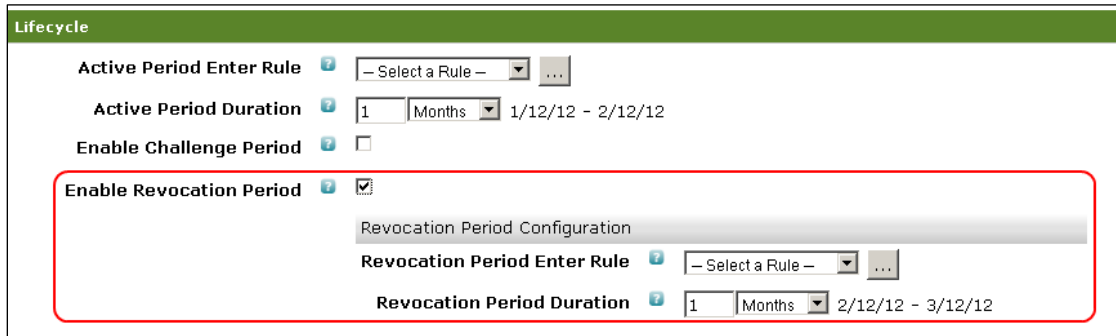
After sign-off and any sign-off approval are complete, a Perform Maintenance task (with the **Finish certifications** and **Transition certification phases** options selected) must run to “finish” the Access Review and move it to the next phase. The next phase is Revocation or End, depending on the options selected in the certification specification.

Remediation and the Revocation Phase

In remediation, the Identities’ Entitlements are altered in the source application to remove any Entitlements that were marked for revocation. Depending on the provisioning features in use, remediations may be processed manually or in an automated fashion. In its most basic form, remediation is managed by sending email messages to, and creating work items for, the Application Revoker or Application Owner, requesting that they change the Identities’ access or permissions manually.

Remediation occurs as a result of an Access Review whether or not a Revocation Period is enabled for the certification. 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.

When a Revocation Period is enabled for the certification (on the Lifecycle page of the certification configuration), two additional parameters appear on the page. These can be used to select a rule to run when the Revocation Period begins and to specify the duration of the Revocation Phase.



The screenshot shows the 'Lifecycle' configuration page. The 'Enable Revocation Period' checkbox is checked. Below it, the 'Revocation Period Configuration' section is expanded, showing the 'Revocation Period Enter Rule' dropdown set to '- Select a Rule -' and the 'Revocation Period Duration' set to '1 Months' with a date range of '2/12/12 - 3/12/12'. The 'Active Period Enter Rule' is also set to '- Select a Rule -' and the 'Active Period Duration' is '1 Months' with a date range of '1/12/12 - 2/12/12'. The 'Enable Challenge Period' checkbox is unchecked.

Figure 22: Revocation Period Configuration

With the Revocation Phase enabled, the Perform Maintenance task checks the requested remediations throughout the Revocation Period to determine whether they have been completed. By default, this remediation check is only done once a day regardless of how often the Perform Maintenance task runs. If desired, this frequency can be adjusted by changing the `remediationScanInterval` value in the System Configuration object (accessible through the IdentityIQ Debug pages). The value specifies the number of milliseconds to wait between remediation scans.

Note: The Perform Maintenance task only does this remediation check when the **Scan for completed revocations** option is selected in its configuration.

Revocation Reminders and Escalations

Revocation reminder emails can be automatically sent to the person assigned the revocation work item if the work item is not yet marked complete after a specified timeframe. When **Send Revocation Reminders** is selected, the Reminder Policy options are displayed and can be set as needed. Reminders can be sent once or at scheduled intervals, beginning a specified number of days before the end of the Revocation period. The template for these emails is set up in the selected **Reminder Email Template**.

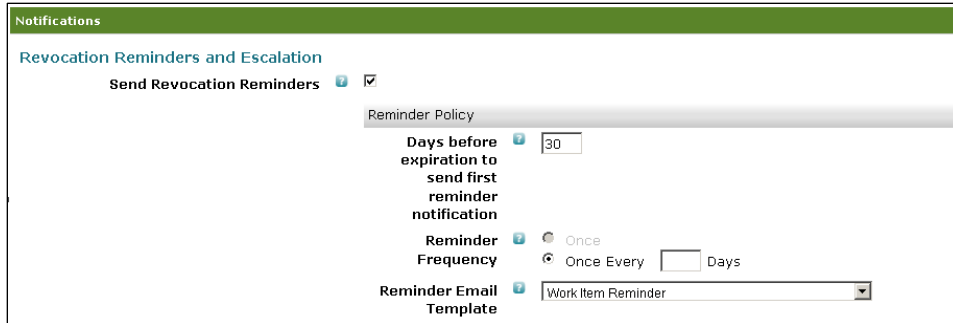


Figure 23: Revocation Reminder Configuration

Escalation can also be automated to notify and transfer control to someone else (for example, the revoker's manager or the Application Owner) if a revocation has not been completed and the end of the Revocation period is near. Selecting the **Escalate Revocations** option displays the Escalation Policy options. The **Escalation Trigger** determines how far in advance of the end of the Active Period the escalation occurs, the **Escalation Rule** determines who receives the work item in the escalation process, and the **Escalation Email Template** selected determines the format of the email sent to notify the new owner.

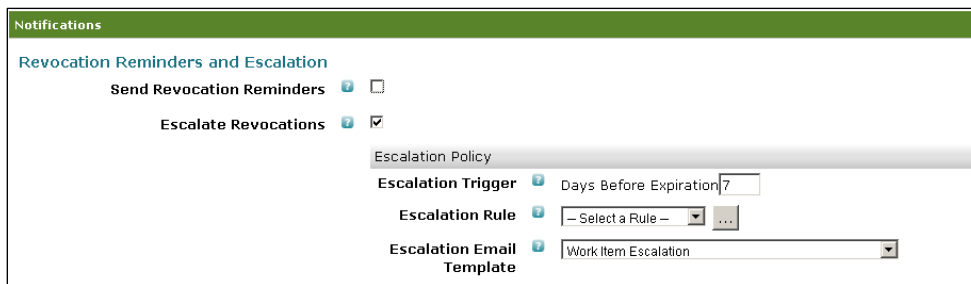


Figure 24: Revocation Escalation Configuration

NOTE: Reminders and Escalations are tied to the work item (in this case the remediation action assigned to the revoker). If the work item is not marked complete when a reminder or escalation date is reached, the reminder email is sent or the escalation is triggered. Like certification reminders and escalations, revocation work item reminders and escalations are managed by the Check Expired Work Items task, which is scheduled to run daily at midnight in the default IdentityIQ configuration. When automated provisioning is in use, work items are not created for revocations so revocation reminders/escalations are not relevant to the process and will not be sent even if these options are selected on the certification specification.

End Phase

The Access Review reaches its End Phase when all Phases configured for it have passed their end date or when all actions required for the process (as configured) are complete. For example, if a certification does not have a Challenge or Revocation Periods enabled, clicking Sign Off allows the Perform Maintenance task to advance the Access Review to the End Phase; with a Revocation Period enabled, the Perform Maintenance task can only advance the review to its End Phase once all remediation requests have been completed or when the Revocation Period's end date passes.

At the start of the End Phase, the “End Period Enter Rule” selected on the Lifecycle page of the certification specification, if any, is triggered.



Figure 25: End Period Enter Rule Specification

Automatic Closing

The Automatic Closing options, if enabled, determine the actions taken by IdentityIQ to close items on an Access Review that is not completed within a specified number of days following the certification’s expiration. A certification “expires” when its Challenge period (if enabled) is over or when its Active period is over if it had no Challenge period. During Automatic Closing, the system automatically completes the actions the human certifier did not finish. This includes making decisions on all open certification items and signing-off on the Access Review.

When Enable Automatic Closing is selected for a certification, the Automatic Closing Configuration options appear. These can be used to set the amount of time that should be allowed to elapse after the expiration date before automatic closing is invoked, the Closing Rule that will be run at that time, the action to take on open Access Review items, and the comment to add to each item for which the automatic action is taken.

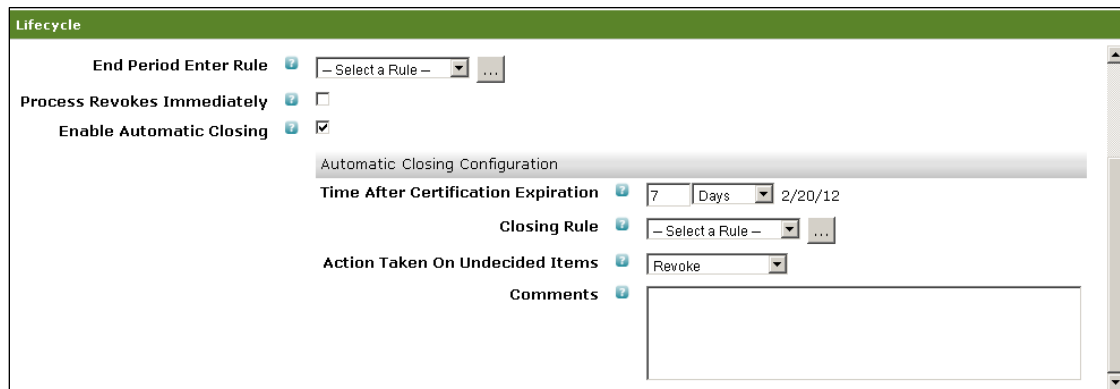


Figure 26: Automatic Closing Options

Continuous Certifications

Most certifications are configured as “periodic certifications,” in which a set of system Entitlements are reviewed as a unit at a single point in time and are signed-off all together. Continuous certifications are different; their Access Reviews remain forever in an Active Phase and are never signed-off, and their individual line items are certified separately and on a rolling, repetitive basis. For example, consider one Identity that has been granted access to three different systems at three different times. If the Identity were in a continuous certification that required recertification once a year, those three Entitlements would each be certified one time per year, but one might be certified in January while the second is certified in March and the third in September, depending on the date the Entitlement was first certified for the Identity.

Though the Access Reviews themselves always stay in the Active Phase, each line item within the Access Review progresses through phases that parallel the phases of a periodic certification. The duration of each phase, and the notifications and escalations associated with each, are defined when the certification is scheduled, just as with periodic certifications. The Challenge and Revocation phases for continuous certifications function exactly the same way they do for periodic certifications, except that they apply to each individual item instead of to the whole Access Review.

Instead of having an Active and End phase, continuous certification items progress from a Certification Required to an Overdue or Certified state (and eventually back to Certification Required when the Certified Duration for the item ends). The Certification Required state indicates that the line-item is due to be certified or re-certified by the assigned reviewer. The Overdue state indicates that the item has not been certified within the required period (determined by the Certification Required Duration on the specification).

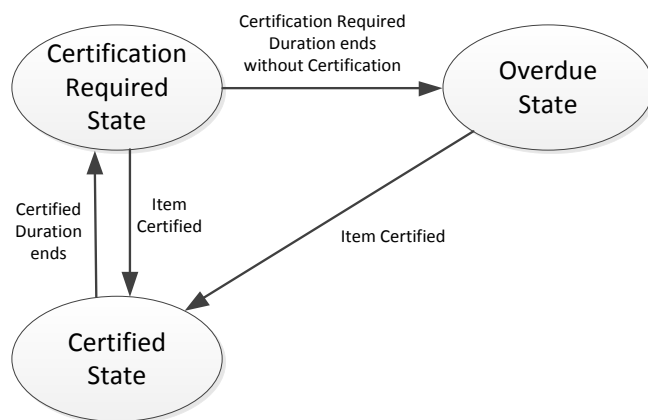
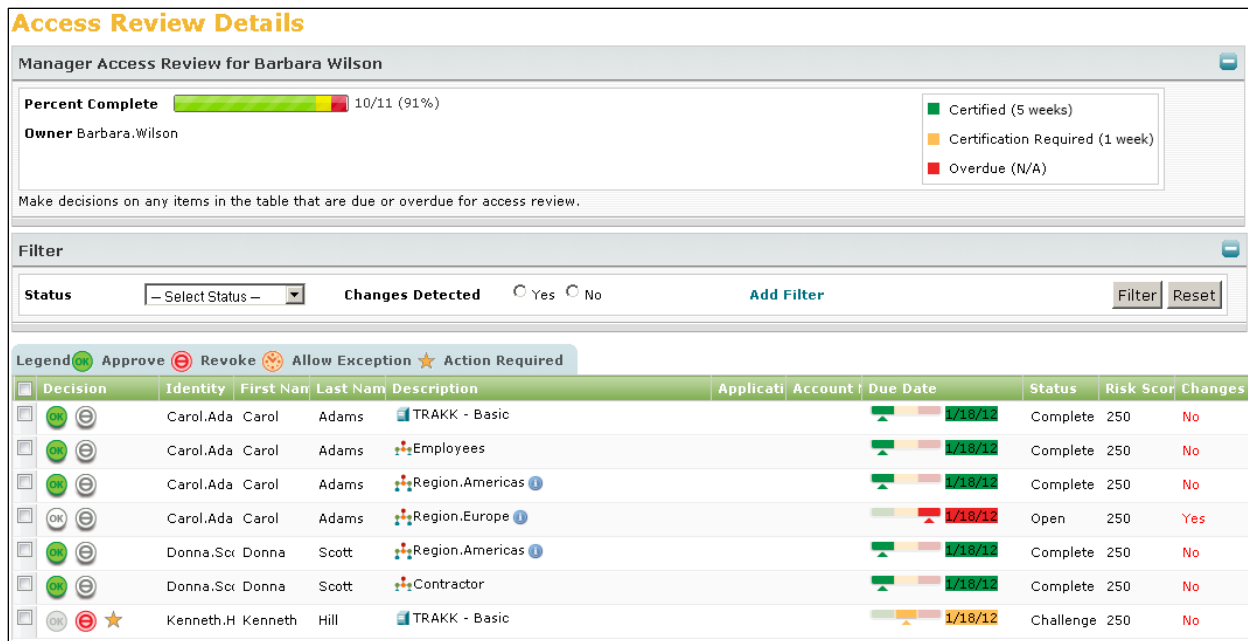


Figure 27: Relationship between Continuous Certification States

IdentityIQ continually tracks the status of each item in a continuous certification. The Access Review Details list flags Overdue items and Certification Required items and indicates when the item is in a Challenge or Revocation phase. As each Certified item reaches the end of its Certified Duration, it is automatically returned to a Certification Required state.



Any certification type can be set up as a continuous certification by selecting “Continuous” from the **Execution Frequency** list on the specification’s Basic page.



Figure 28: Specifying a Certification as Continuous

This changes the parameters displayed on the Lifecycle page for the certification to allow specification of the Certified Duration (time between certifications for a given item) and the Certification Required Duration (the amount of time allowed for the certifier’s review before the certification becomes “overdue”). (NOTE: A continuous certification’s **Active Period Enter Rule**, if specified, runs once when the certification first becomes an Active certification – i.e. when it is created. It does not run for each Item as it returns to a Certification Required status. Because these are seldom used together, the Active Period Enter Rule is no longer displayed as an option in the UI when continuous certification is selected, beginning in version 6.2+; however, if one were specified in the XML, it would still run when the certification first became active.)

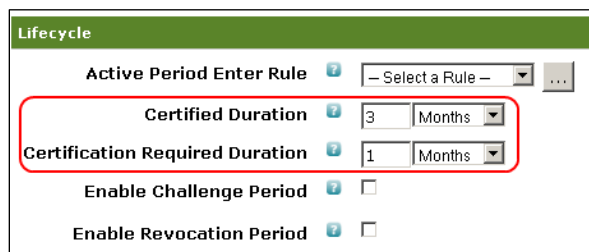


Figure 29: Continuous Certification Lifecycle Page

Choosing continuous certification also alters the certification reminder and escalation options available on the Notifications page.

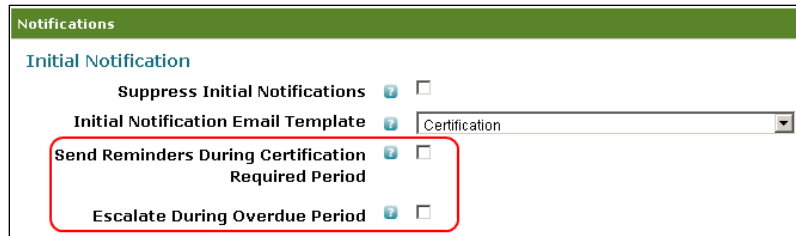


Figure 30: Continuous Certification Notifications Page

The information within a continuous certification is updated on a regular basis by the Refresh Continuous Certifications task. This ensures that when any Identity or Entitlement associated with the certification changes, the certification information is updated. For example, if an Identity that is part of a continuous certification is assigned a new Role, the task will add that Role to the continuous certification. Likewise, if an Identity changes departments, it will be removed from a continuous Manager certification for the former manager (and added to the new manager's continuous Manager certification if one is in place). Items are added to a continuous certification in the "Certification Required" state to ensure that they are certified immediately. The rolling certification cycle starts for each item at the time it is added to the certification by the Refresh Continuous Certifications task.

Certification Events

Certifications can be triggered by events that happen within IdentityIQ. Certification Events trigger an Identity certification, which includes only a single Identity. One common usage of Certification Events is running a certification when an Identity changes managers so the new manager can confirm or change the Identity's Entitlements as appropriate for their new position. The triggering events and the associated certifications are specified on the **Certification Events** tab under **Monitor -> Certifications** by clicking **Add New Certification Event**.

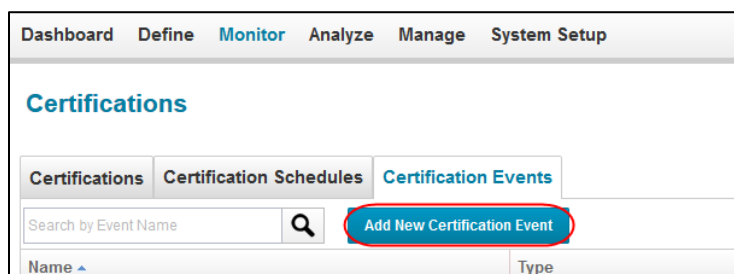


Figure 31: Create New Certification Event

The certification specification is divided across the same 5 pages as any other certification (Basic, Lifecycle, Notifications, Behavior, and Advanced), most of which are exactly identical to any other certification specification. The Basic page's **Event Options** section is the major difference between this certification type and others; that is where the triggers are specified.

Certification Event

Summary << Basic

Steps

1. **Basic**
2. Lifecycle
3. Notifications
4. Behavior
5. Advanced

Specify options about what to certify, when the certification should be created, and who is responsible for certification.

Event Options

Name ?

Description ?

Event type ?

Create ▼

Disabled ? ☐

Included Identities ? ☒ All ☐ Match List ☐ Filter ☐ Script ☐ Rule ☐ Population

Certification Properties

Figure 32: Event Options section of Certification Event Basic Page

The **Event type** field identifies which event will trigger the certification:

- Create:** certification runs when an Identity is created
- Manager Transfer:** certification is triggered based on a change in the Identity's Manager attribute. If desired, the event can be restricted to a move to or from a specific manager.
- Attribute Change:** certification runs when the value of a specified Identity Attribute changes. This trigger can optionally be restricted to changes from or to a specific value.
- Rule:** certification is triggered when the specified IdentityTrigger rule returns a "True" result. IdentityTrigger rules run anytime an Identity is changed in an Identity Refresh or Aggregation and they are passed the Identity as it existed before and after the change. The rule's logic determines what attributes are evaluated, and the rule can return a True or False value; True fires the certification and False does not.
- Native Change:** certification runs when an account attribute being watched for native changes (changes occurring directly in the target application rather than through an IdentityIQ-driven action) are detected; Native Change Events were introduced in version 6.0.

Different fields are displayed on the page depending on the **Event type** selected so the specific parameters available for that event type can be set.

The **Include Identities** options can be used to limit the Event to only certain Identities if desired, meaning the certification will only be triggered for Identities undergoing the required Event *and* matching the inclusion criteria. The rule type for a Rule specified as the **Include Identities** filter is IdentitySelector; it is passed the Identity undergoing the required Event and can return an Identity to run the certification or a Null value to bypass the certification.

Summary of Rules Triggered by Certifications

Rules Configured during Certification Specification

All of these rules can be created and selected while configuring each individual certification. Some only apply to specific certification types. They are listed here in the order they would be run if all were specified and triggered for a given certification.

| Rule Name | Rule Type | Triggering Time/Event | Effect of Rule |
|-------------------------------|----------------------------|--|---|
| Exclusion Rule | CertificationExclusion | Executed as part of Certification creation process | Excludes entitlements from the certification process based on rule logic |
| Pre-delegation Rule | CertificationPreDelegation | Executed as part of certification creation process | Automatically delegates specific certifications based on rule logic |
| Group Factory Certifier | Certifier | Executed as part of certification creation process (only for Advanced certifications run for Groups Factories); runs once for each Group | Assigns certifier for each group's certification |
| Active Period Enter Rule | CertificationPhaseChange | Run at the start of the Active Period (time during which certifier review and makes access decisions) | Open-ended; Depends on rule logic |
| Certification Escalation Rule | WorkItemExcalationRule | Triggered at time specified as the Escalation Trigger on the certification if Access Review has not yet been finished and signed-off by certifier | Provides name of the Identity who should be notified incomplete Access Review and impending deadline (often this is 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 after Active Period ends; in the case where Process Revokes Immediately is selected, Challenge period begins for each Entitlement at the moment it is revoked and challenge period enter rule runs once for each revocation | No return value; effect of rule depends on rule logic |

| | | | |
|------------------------------|-------------------------------|---|---|
| Closing Rule | CertificationAutomaticClosing | Run according to timeframe after certification expiration (end of Challenge – if enabled – or Active phase) specified in the Automatic Closing Configuration | No return value; effect of rule depends on rule logic |
| Sign-off Approver Rule | CertificationSignOffApprover | Triggered by certifier Sign-Off on Access Review | Returns the Identity (if any) of the person who needs to approve the certification decisions made by the certifier (Enables two-level sign-off) |
| Revocation Period Enter Rule | CertificationPhaseChange | Executed at the start of the Revocation Period (if enabled); this period immediately follows Challenge Period, if enabled, or Active Period if Challenge is not enabled | No return value; effect of rule depends on rule logic |
| Revocation Escalation Rule | WorkItemExcalationRule | Triggered at time specified as the Revocation Escalation Trigger if remediation action has not yet been completed by revoker | Provides name of the Identity who should be notified incomplete revocation (often this is the revoker's manager or the Application Owner) |
| End Period Enter Rule | CertificationPhaseChange | Run at the beginning of the End Period; End Period starts after all other periods configured for the certification are complete. | No return value; effect of rule depends on rule logic |
| Certification Event | IdentityTrigger | Runs when an Identity is changed in an Identity Refresh or Aggregation | Determines whether to kick off a Certification Event that triggered by the Rule ("True" result fires the certification) |
| Include Identities | IdentitySelector | Runs when a Certification Event is triggered that has the Rule option selected as the Include Identities parameter | Determine whether to run the Identity certification or not (Null return value bypasses while Identity return value executes certification) |

Other Certification-Related Rules

These are rules that run as part the certification process but are not specified on the Certification Specification windows. Except for the FallbackWorkItemForward rule, they are all defined in the System Configuration xml.

| Rule | Rule Type | Triggering Time/Event | Effect of Rule |
|------------------------------------|----------------------------------|---|--|
| Fallback Work Item Forward | FallbackWorkItemForward | Runs when system detects that configured automatic forwarding of a work item would result in a self-certification situation (owner of work item is also subject of certification); specified in System Setup -> IdentityIQ Configuration -> Rules tab | Determines the Identity to send a work item to instead of the automatically selected owner |
| Certification Entity Customization | CertificationEntityCustomization | Runs when certification is generated | Allows custom fields on the Certification Entity to be populated (seldom-used rule) |
| Certification Entity Refresh | CertificationEntityRefresh | Runs when a CertificationEntity is refreshed (refresh occurs when a decision is saved for the CertificationEntity or its associated CertificationItems) | Performs actions on Entity as specified in rule logic; e.g. could copy a custom field from the Entity down to all sub-items (seldom-used rule) |
| Certification Entity Completion | CertificationEntityCompletion | Runs when a CertificationEntity is refreshed and has been determined to be otherwise complete (all CertificationItems on the entity are complete) | Determines whether the entity is still missing any information; if errors are found, adds them to a list and returns them to the caller |
| Certification Item Customization | CertificationItemCustomization | Runs when certification is generated | Allows custom fields on the Certification Item to be populated (seldom-used rule) |
| Certification Item Completion | CertificationItemCompletion | Runs when a CertificationItem decision is saved | Performs actions on the Item as specified in rule logic (seldom-used rule) |

Summary of Tasks affecting Certifications

| Task Type | Effect on Certifications |
|----------------------------------|--|
| Continuous Certification Refresh | Only applicable to Continuous certifications; used to update any continuous certifications with the latest identity information, including actions such as adding an Identity's newly-assigned Entitlements to the certification or removing an Identity from the certification when it has been removed from the system |

| | |
|---------------------|---|
| | <p>Can be run manually to update certifications immediately or can be scheduled to run periodically to keep the certifications up-to-date.</p> <p>The Continuous Certification Refresh task scans any identities that have been updated since the last time it ran. If changes are detected the task updates the continuous certifications as required. Items added to continuous certifications are placed in the certification require state.</p> |
| Perform Maintenance | <p>Must run after certifier clicks “Sign Off” to mark certification completed and move it to next phase; also manages remediation checking during Revocation Period</p> <p>Scheduled to run every 5 minutes by default; remediation checking is done only once a day by default.</p> |

Setting Certification Defaults

Default values for many certification parameters can be set on the **System Setup -> Certification Configuration** window in IdentityIQ. This includes defaults for the Behavior page, the Lifecycle page, and some parts of the Advanced page. Additionally, default email templates can be specified on this window for various notifications sent during the certification process. All of these values can be overridden for individual certifications.

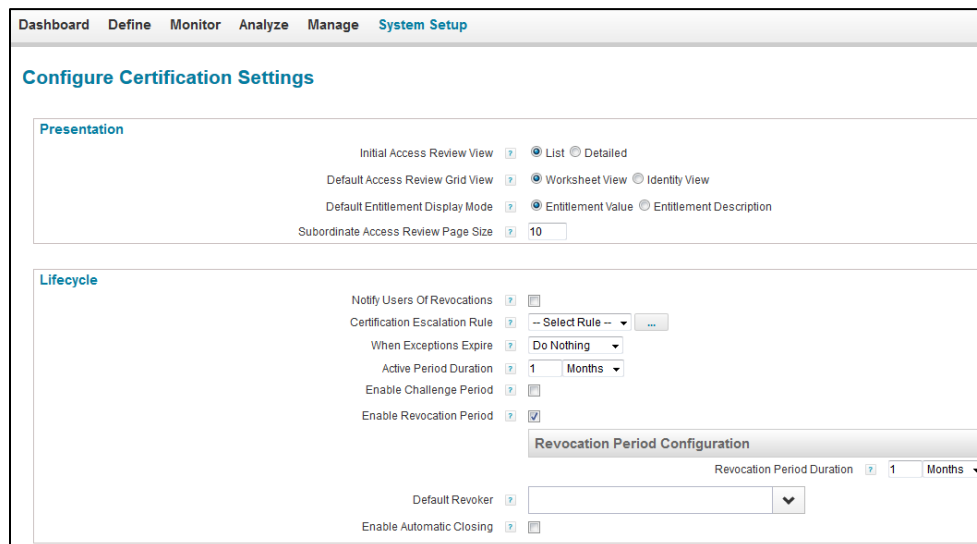


Figure 33: Global Certification Configuration Settings