Table of Contents

[1 Overview 2](#_Toc1457227)

[2 Native Change Certification Options 2](#_Toc1457228)

[3 Native Change Certification Configuration 2](#_Toc1457229)

[4 Include Only Privileged Access Configuration 7](#_Toc1457230)

[5 System Certification Item Rule 7](#_Toc1457231)

[6 Application Inclusion 7](#_Toc1457232)

[7 Certification Exclusion Rule 7](#_Toc1457233)

[8 Native Change Process 7](#_Toc1457234)

[9 Native Change Data Flow 8](#_Toc1457235)

[10 Notify Operations Native Change 8](#_Toc1457236)

.

**Document Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Author** | **Summary of Changes** |
| Version 1 | 3/2/18 |  | Rohit Gupta |  |
| Version 2 | 5/8/18 |  | Cathy Mallet | Minor edits |

# Overview

The purpose of this document is to explain the Native Change Feature that is built within the Accelerator Pack. This feature requires some configuration in IdentityIQ for the manager certification option and these configurations are described in this document.

# Native Change Certification Options

Native Change Manager certification can be kicked off using two options. Both options are mutually exclusive.

* Lifecycle Event
  + By Default, it is enabled
  + Workflow Based
  + Uses Certification Settings from Disabled Certification Event and Custom Object
  + Uses Application native change drop-down options
    - Do Nothing
    - Automated Recovery and Revocation
    - Manager Certification Revocation
    - Manager Certification Revocation and Automated Recovery
* Certification Event
  + By Default, it is disabled
  + Certification Event Based
  + Uses Certification Settings from Enabled Certification Event
  + Application native change drop-down options are not supported. Only Manager Certification is supported

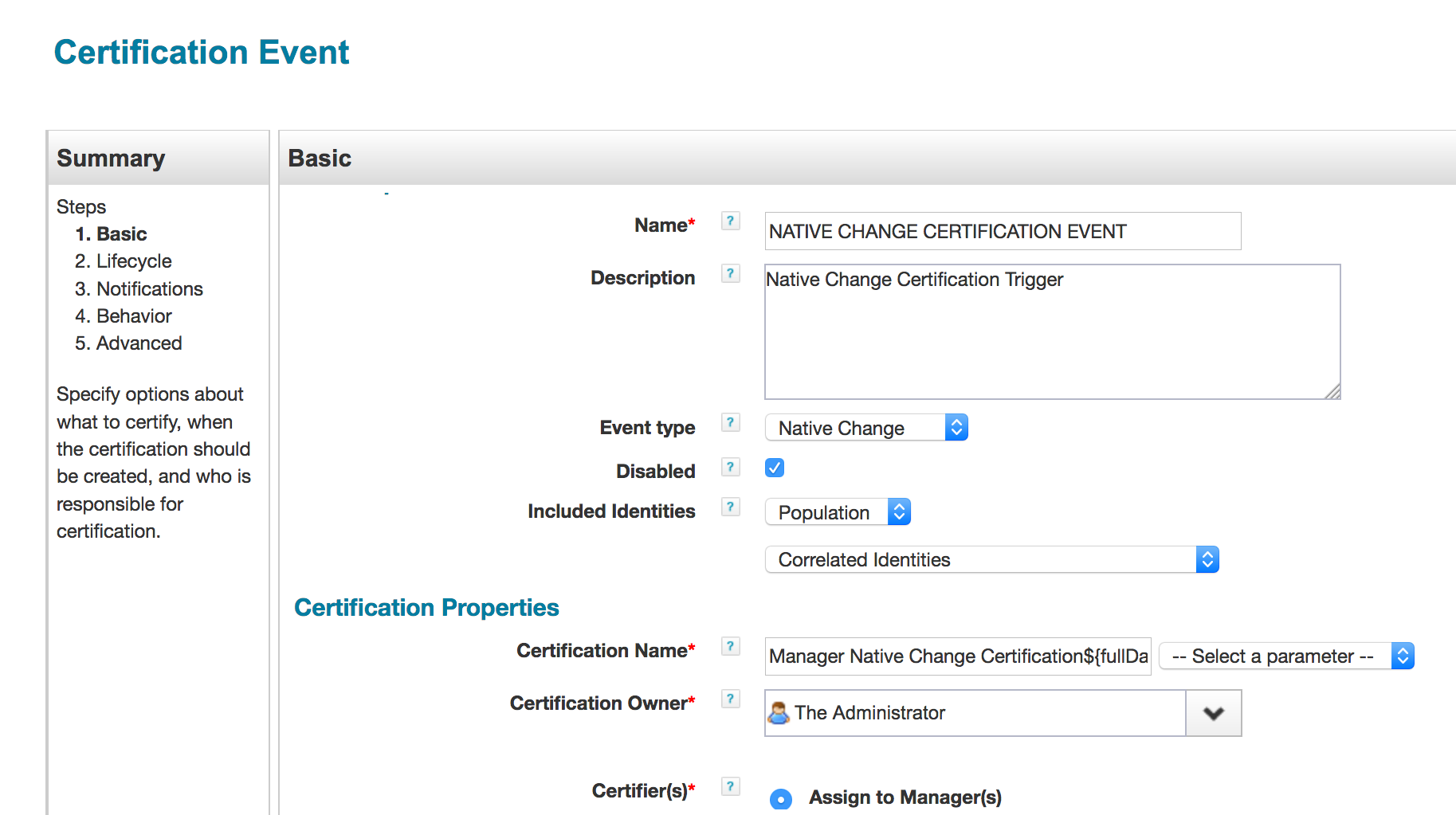
# Native Change Certification Configuration

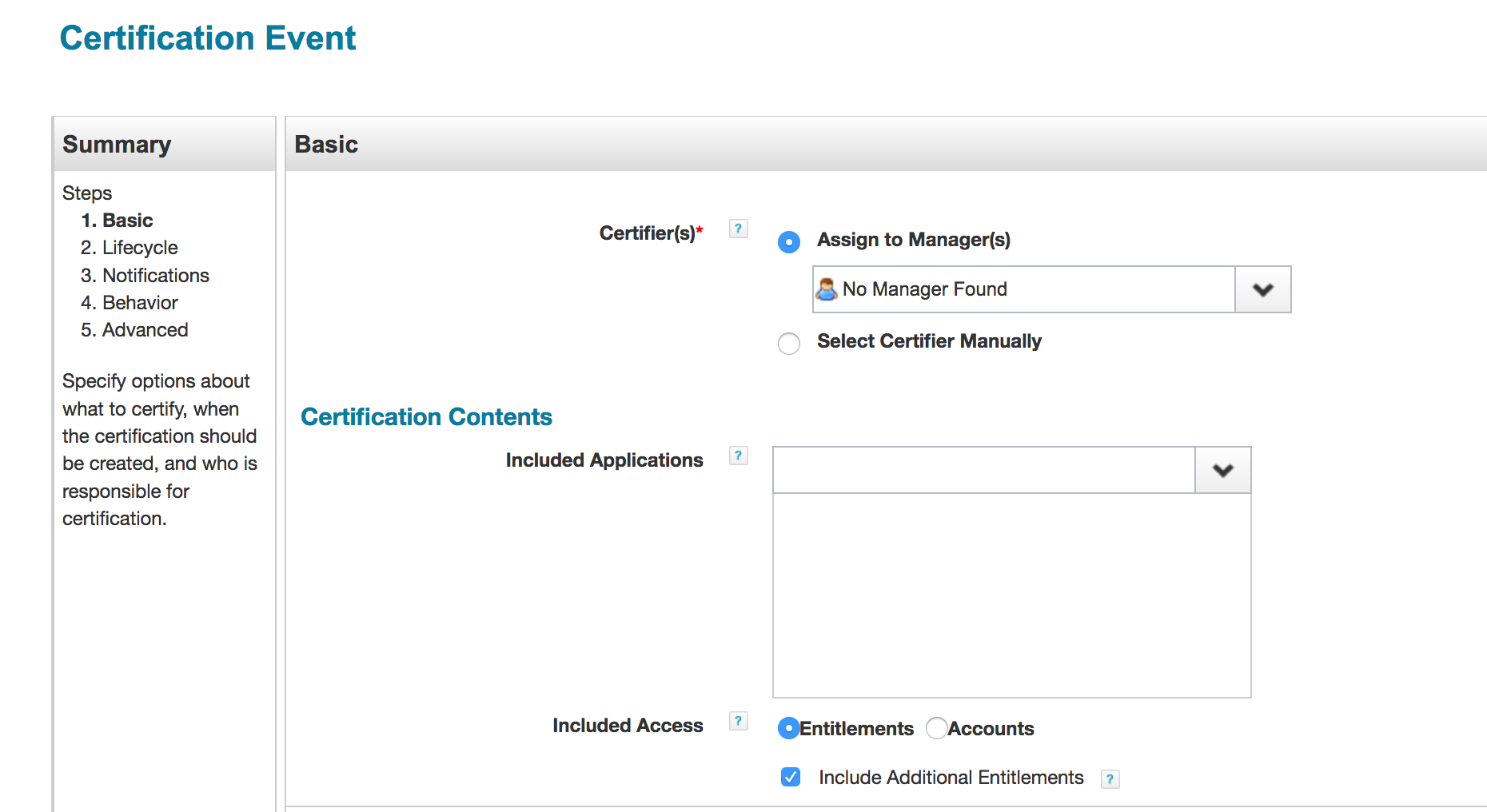
For a Lifecycle Event, the native change certification notification scheme, email templates, and certifications settings are picked up from a certification event “**NATIVE CHANGE CERTIFICATION EVENT**” and custom object “**Custom-Native-Change-Settings**”. For a Certification Event, a custom object is not used.

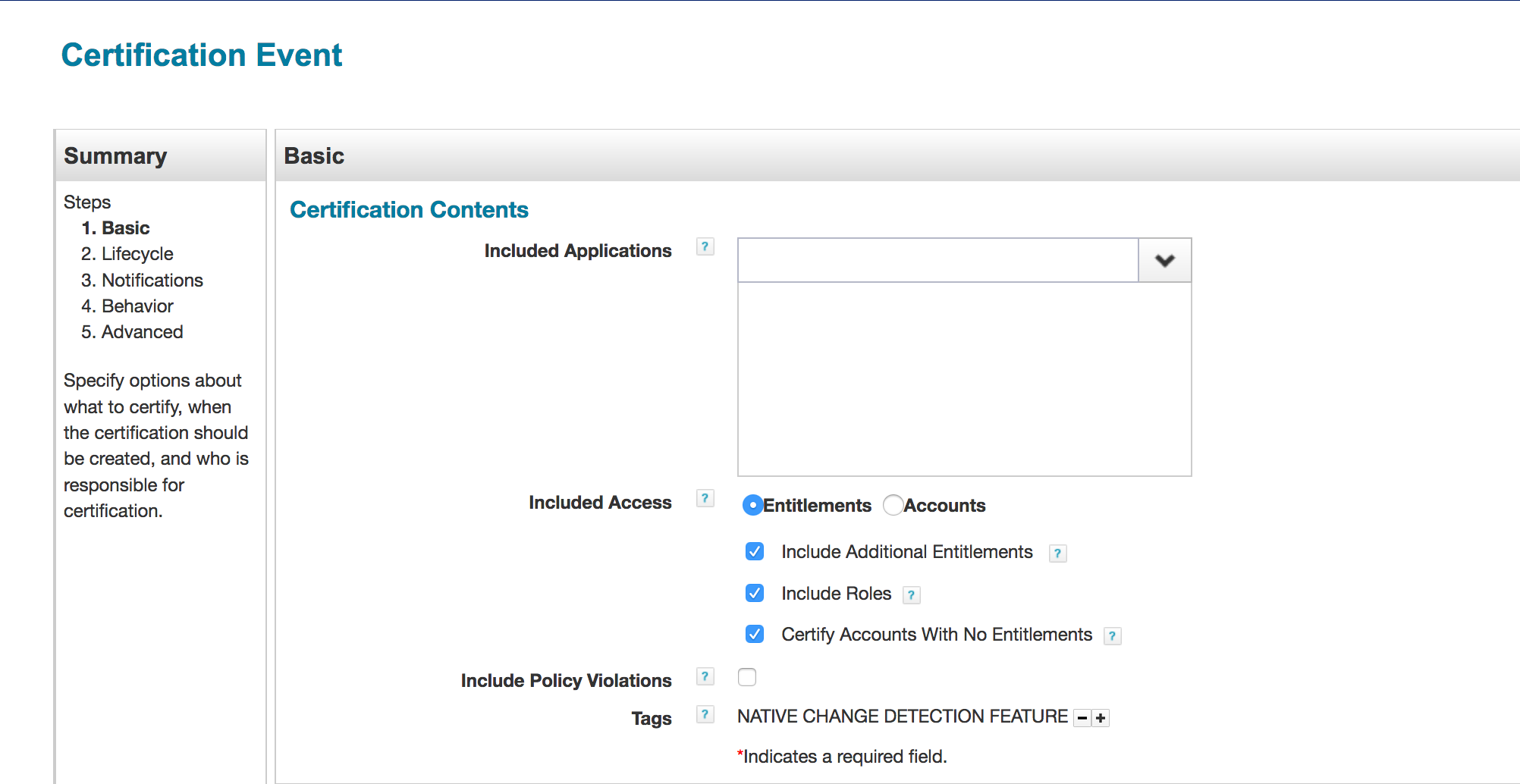
See the table below for “**Custom-Native-Change-Settings”** Custom object settings that are packaged with this feature. By default, staging is not enabled for native change certifications.

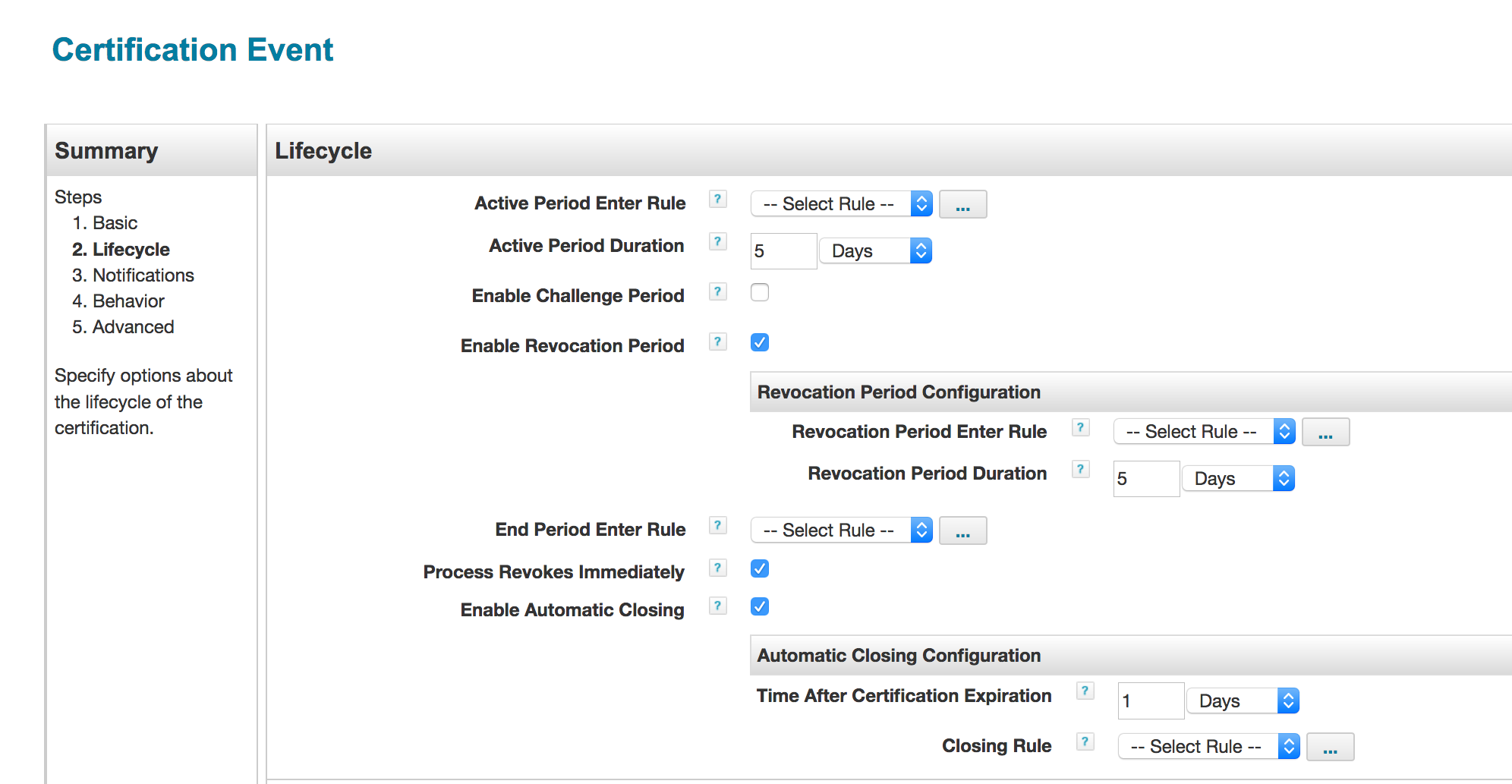
|  |  |  |
| --- | --- | --- |
| Key Name | Category | Default Value |
| certificationNamePrefix | Certification Name | “Native Change Detected For” (Identity Name is Prefixed) |
| certificationNameSuffix | Certification Name | “Assigned To” (Manager Name is Suffixed) |
| stagingEnabled | Staging | False |
| securityGroupName | Reassign Certification To WorkGroup instead of Manager | Empty |

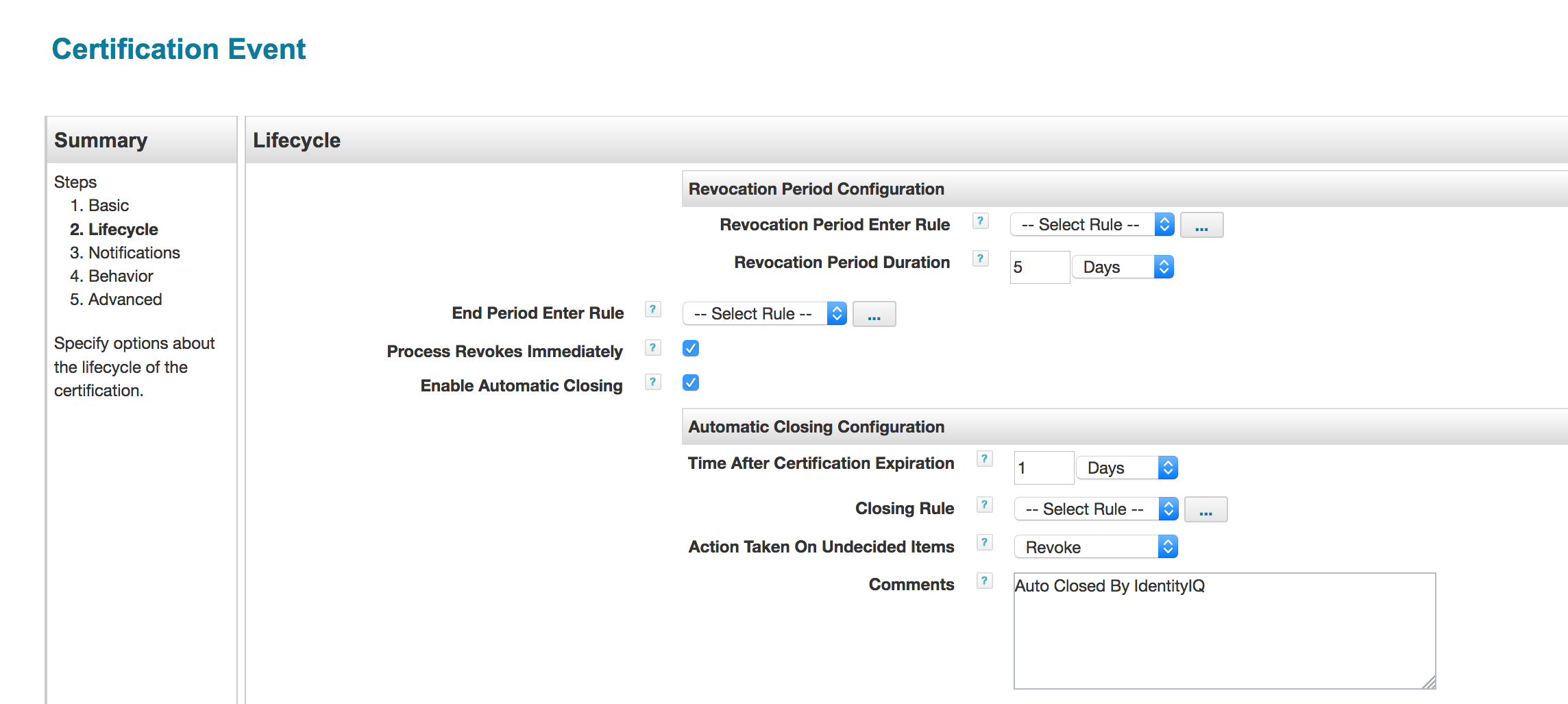
Please see below for screen shots of the **“NATIVE CHANGE CERTIFICATION EVENT**” CertificationDefinition object that is packaged with this feature.

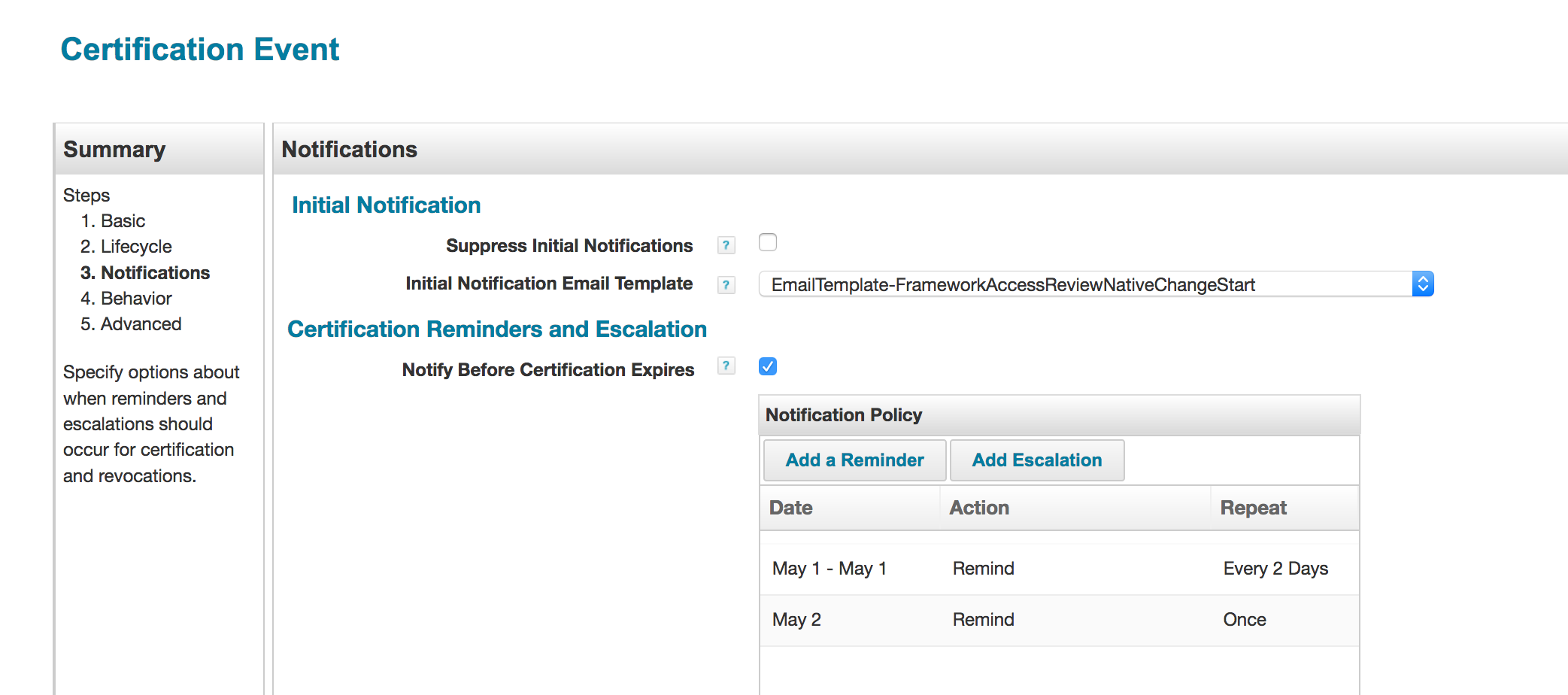


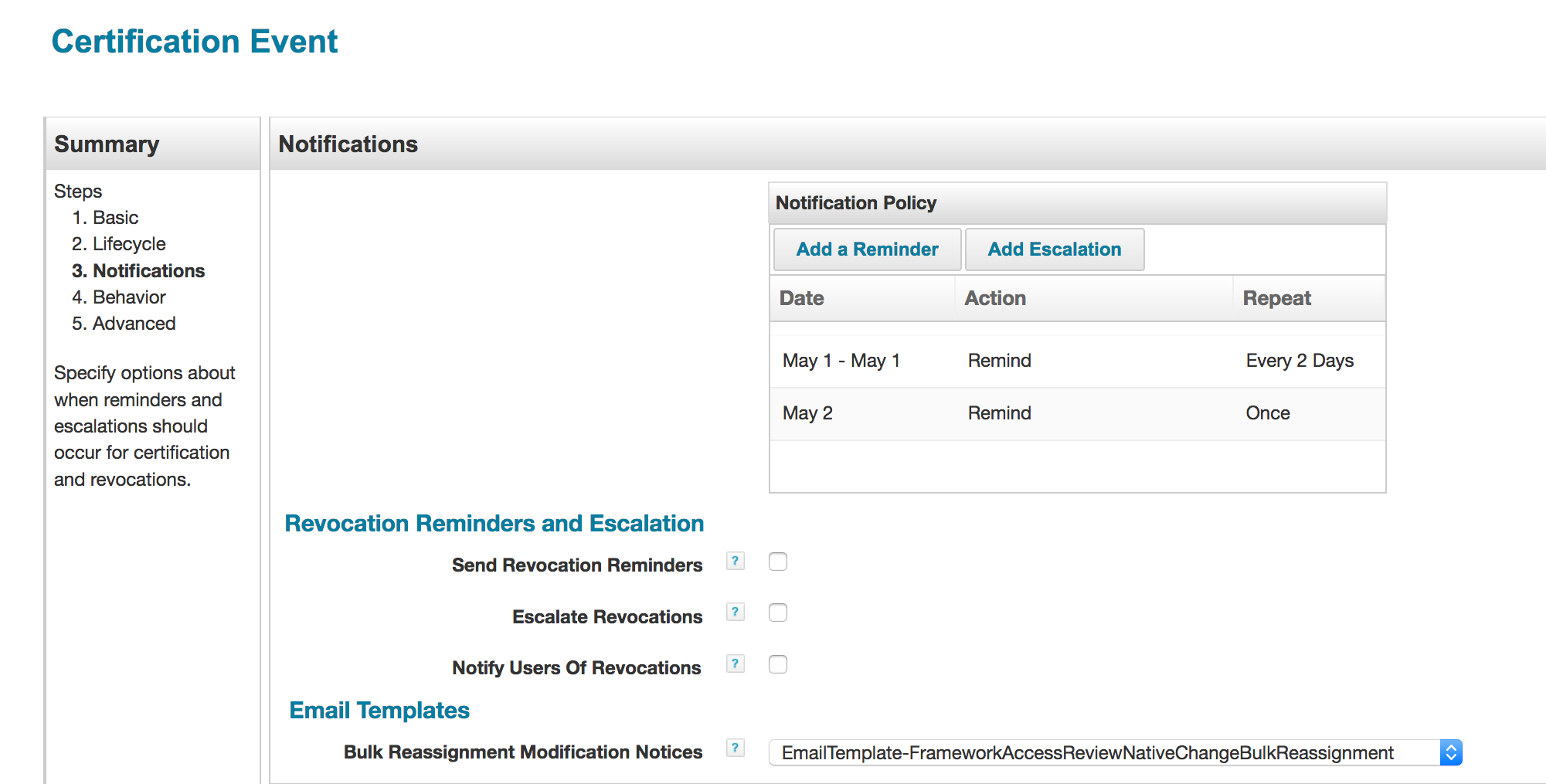


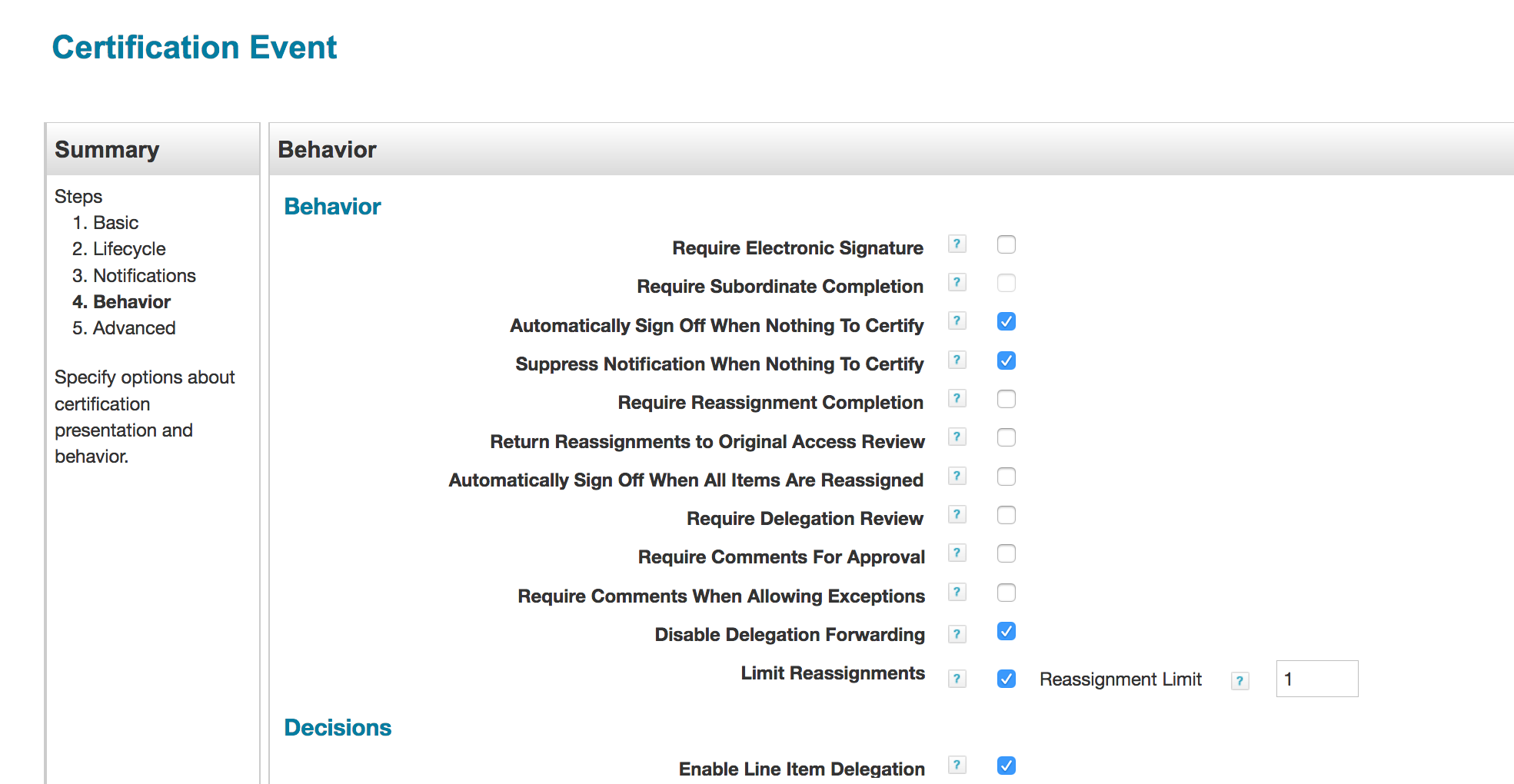


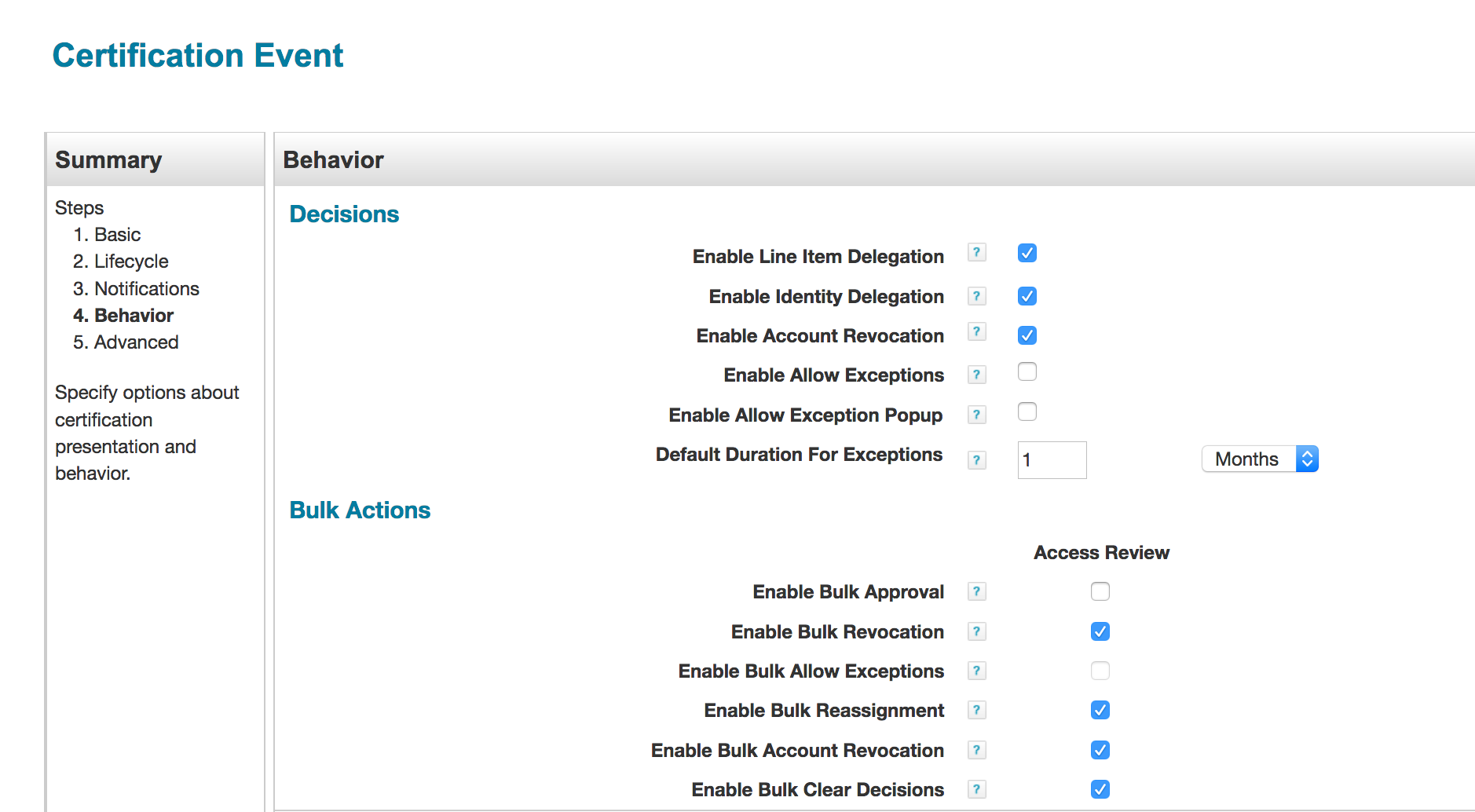


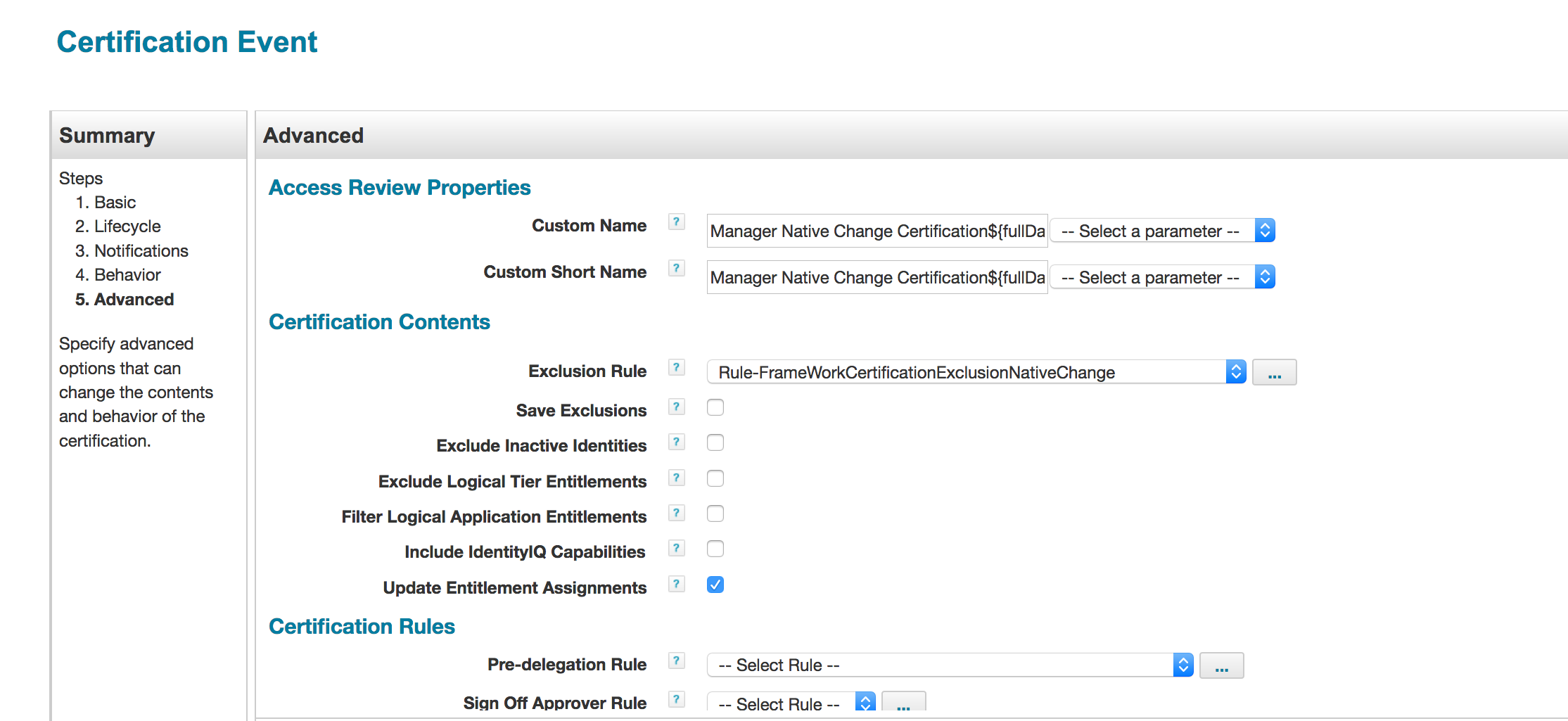




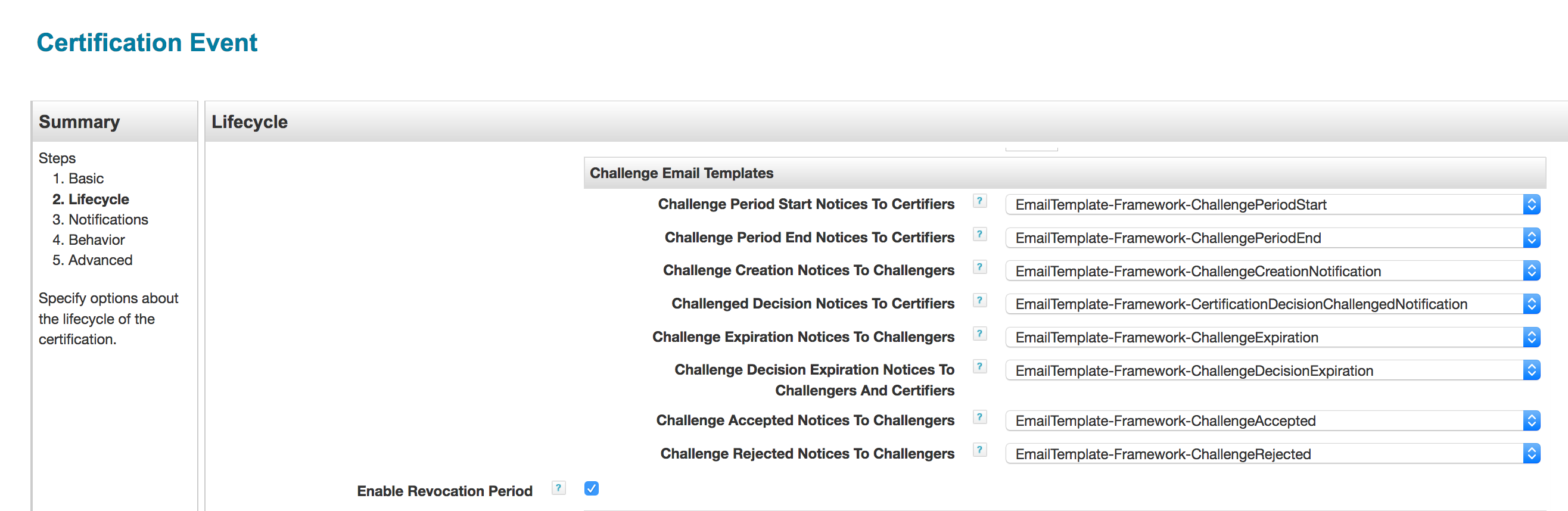








By default, a challenge period is not enabled. This screen shot shows the packaged challenge period email templates if it is enabled.



# Include Only Privileged Access Configuration

In case only privileged access is required for native change detection, custom object “**Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess**” can be configured by QuickLink “Global Definition” to only include sensitive/privileged access for certification .

See the table below for “**Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess”** Custom object settings that are packaged with this feature.

|  |  |  |
| --- | --- | --- |
| Key Name | Category | Default Value |
| includeOnlyPrivilegedAccessNativeChangeCert | Include Only Privileged Access | False |

# System Certification Item Rule

A certification item rule named “**Rule-Framework-Certification-Item-Rule**” copies the logical application name from roles and entitlements to the certification item attribute “Custom1”.

Also, this rule copies the “entPrivileged” and “rolePrivileged” extended attribute values from entitlements and roles to the certification item attribute “Custom2”.

# Application Inclusion

For Lifecycle Events, applications configured for Native Change and access on those applications is detected as native (assigned outside IdentityIQ) after aggregation, and these applications are included automatically for certification.

For Certification Events, applications configured for Native Change need to be selected manually and saved on the Certification Event.

# Certification Exclusion Rule

The “**Rule-FrameWorkCertificationExclusionNativeChange**” rule excludes all access from an Identity Cube except native changes. Here is pseudo algorithm of this rule:

* First, get native changes from an Identity cube
* If not found, get native changes from a configuration object “**Certification-NativeChange**”. The native changes are saved to this object during Workflow based Lifecycle Events
* Exclude all access that is not detected as native change

# Native Change Process

This process starts with either a Workflow-based Lifecycle Event or Certification-based Certification Event.

The Native Change process can be kicked off manually by the Operations QuickLink “Process Identity Event”. This QuickLink is accessible to the “Operations” workgroup.

This workflow builds a provisioning plan and /or certification based on **native changes on an Identity**. Here is the pseudo algorithm:

* If the option is “Automated Recovery and Revocation”, build a provisioning plan with a remove account request for native access that is added to an identity, and build a provisioning plan with an add account request for native access that is removed from an identity
* If the option is “Manager Certification Revocation”, build a Certification for native access that is added to an identity
* If the option is “Manager Certification Revocation and Automated Recovery”, build a certification for native access that is added to an identity, and build a provisioning plan with an add account request for native access that is removed from an identity
* Override certification for manager to security group, if configured by “Global Definition” QuickLink
* Include Only Privileged Access , if configured by “Global Definition” QuickLink

# Native Change Data Flow



# Notify Operations Native Change

By Default, Native Change Email is sent out to Operations on provisioning failures only. A Global Definition Configuration "Notify Operations on Native Change for an Identity" can be used to send out email to Operations on Native Change provisioning action.

If there is a requirement to cc this email, an extended rule can be used and referenced using Global Definition configuration “CC Email Rule” option.