*IdentityIQ Group Management*

Table of Contents

[Entitlement/Group Management. 2](#_Toc172015985)

[Scope: 2](#_Toc172015986)

[Group Management - Global Configurations 3](#_Toc172015987)

[Create / Edit Group Configurations 3](#_Toc172015988)

[Orphan Group Configurations 3](#_Toc172015989)

[Group Management Application Configurations 4](#_Toc172015990)

[Pre and Post Rules 4](#_Toc172015991)

[Orphan Entitlement / Group Management Task 5](#_Toc172015992)

[Synchronization of Ownership / Approvers Task 5](#_Toc172015993)

[Group Management Artifacts 6](#_Toc172015994)

[Quick Links 6](#_Toc172015995)

[Application Group Type Form 6](#_Toc172015996)

[Create Group Form Attributes 6](#_Toc172015997)

[Edit Group Form Attributes 7](#_Toc172015998)

# Entitlement/Group Management.

## Scope:

* Allow scoped identities to define a new group using the IIQ interface
* Allow scoped identities to define a new group and add members to the group using the IIQ interface
* Allow scoped identities to remove members from an existing group using the IIQ interface
* Aggregate AD groups and their metadata (owners, description etc.) from scoped domains in active directory.
* Update primary and secondary owners for groups in active directory.
* Remove groups that do not have any direct members and sub-groups within it.
* Establish an approval process (if required) for group creation and group update use-cases and execute actions post approval completion.
* Require all group deletion actions to be approved by an owner (either a manager, application or group owner).
* Allow the user to select an AD domain / application to make changes as defined above.
* Display group types (security group, distribution group etc.) on the request form.
* Display help instructions for each group type on the request page.
* Enable email notifications to be sent on completion of the group change request.
* Enable logging and auditing of events utilizing the existing out-of-the-box logging and auditing capabilities in IIQ.
* Access Request would be created for each request for tracking/reporting.

## Group Management - Global Configurations

These following configurations can be used by the technical team to apply configurations globally for all applications that are onboarded for Group/Entitlement Management. These global Group management configurations will be configured in the **Configuration** Object of SailPoint IdentityIQ.

## Create / Edit Group Configurations

* Approvals
  + Approval Scheme
  + Hours Befor First Reminder
  + Hours Between Reminders
  + Escalation Options
  + Emails
    - Submission Email To Requestor
    - Approval Email For Approver
    - Reminders Email For Approver
    - Escalations Email For Approver
    - Rejection To Requestor
    - Completion Email To Requestor
* Provisioning
  + Add Group Membership
    - Workflow for Group Membership: (Default: LCM Provisioning (No Appovals)
    - If Approvals Needed.
      * Approval Scheme
      * Hours Befor First Reminder
      * Hours Between Reminders
      * Escalation Options
      * Emails
        + Approval Email For Approver
        + Reminders Email For Approver
        + Escalations Email For Approver
  + Provisioning Errors will be embedded in to Completion Email
* Maximum Members Limit: Default 500.

## Orphan Group Configurations

* Orphan Group Form
  + The default orphan approval form for owners
* Orphan Group Confirmation Form
  + This default orphan approval confirmation form for owners
* Skip Confirmation Form
* Approvals
  + Approval Scheme
  + Hours Befor First Reminder
  + Hours Between Reminders
  + Escalation Options
  + Emails
    - Submission Email To Owner
    - Approval Email For Approver
    - Reminders Email For Approver
    - Escalations Email For Approver
    - Rejection To Requestor
    - Completion Email To Owner
* Provisioning Errors will be embedded in to Completion Email

**NOTE**: Each of the above configurations can be overridden for specific applications by applying the above options in each of the **Application** object attributes section.

## Group Management Application Configurations

Chronological behavior of Create/Edit group functionality. Below items can be configured in **Application object attributes** section**.**

* Group Schema Types
  + Group Types (Supported Group Schema Type for Group Management)
* Create Form
  + Application Create Group Provisioning Policy Form
* Create Confirmation Form
* Skip Confirmation Form
* Group naming format (The Regex expression for naming of the Group)
* Owner Workgroup definition (The Name of the workgroup which the **Ownership/Approver** task creates for each group of an application.)
* Elevated Access for Group Membership
  + Elevated Access Attribute: Searchable account Attribute used to filter the elevated accounts for group membersip provisioning.
  + Elevated Access Attribute Value: Value using which the filter to be applied for elevated accounts for group membersip provisioning.

### Pre and Post Rules

List of rules that overrides Global Group Definition Quick Link Settings

* Create Entitlement Form Pre Rule
  + Input Argument
    - Entitlement Model
* Create Entitlement Form Post Rule
  + Input Argument
    - Entitlement Model
* Create Entitlement Provisioning Pre Rule
  + Input Argument
    - Entitlement Model
* Create Entitlement Provisioning Post Rule
  + Input Argument
    - Entitlement Model
* Edit Entitlement Form Pre Rule
  + Input Argument
    - Entitlement Model
* Edit Entitlement Form Post Rule
  + Input Argument
    - Entitlement Model
* Edit Entitlement Provisioning Pre Rule
  + Input Argument
    - Entitlement Model
* Edit Entitlement Provisioning Post Rule
  + Input Argument
    - Entitlement Model
* Orphan Entitlement Form Pre Rule
  + Input Argument
    - Entitlement Model
* Orphan Entitlement Form Post Rule
  + Input Argument
    - Entitlement Model
* Orphan Entitlement Provisioning Pre Rule
  + Input Argument
    - Entitlement Model
* Orphan Entitlement Provisioning Post Rule
  + Input Argument
    - Entitlement Model

## Orphan Entitlement / Group Management Task

Managing of Orphan (Groups without memberships) groups can be handled via the following tasks based on their usage and group-membership. This task would trigger a workflow to intiate the Orphan Group Management. Task “**Orphan Entitlements**” which is Rule based detection on entitlement extended attributes and group membership and which triggers the workflow for Orphan management. Task “**Orphan Entitlements**” must be scheduled for detection to take place

## Synchronization of Ownership / Approvers Task

Owners and Approvers can be synchronized from managed systems/ applications using rule based task “**Synchronize Groups and Work Groups”.** This task creates one workgroup for each group on an application. Name of the workgroup can be configured using “**Owner Workgroup Definition**” defined in the Global group configurations. Task “**Synchronize Groups and Work Groups**” must be scheduled for synchronization to take place.

## Group Management Artifacts

### Quick Links

Four new quick links are designed for group management functionality. These quicklinks provides three modules

1. Self Service Group Management
   1. Create New Group
   2. Edit My Group

### Application Group Type Form

This form will be displayed to select the application and group types to be onboarded by Group Management process.

### Create Group Form Attributes

Following is the List of the attributes that are defined on create group form**.**

* Forest
  + List of Forests from Active Directory Application
  + Visible for Selection if there are multiple forests
* Domain
  + Selected Forest’s Domains from Active Directory Application
  + Visible for Selection if there are multiple domains Hidden
* Organizational Unit
  + Name for the Domain’s Group Organizational Unit
* Group Name
  + Required
  + Validations
    - In Flight Uniqueness Check
    - Uniqueness Check against Entitlement Catalog
    - Additional Validation Via Group Global Definition
* Description
  + Required
* Comment
  + Required
* Primary / Secondory Owners
  + List of Identities
  + Default is Requestor
* Is Requestable
* Is Group Membership for Elevated Access.
* Identity Membership
  + Initial Identities who should be a member of this group
  + If Group Membership for elevated access is TRUE, The group membership will only be applied to the elevated accounts of the Identities selected.
* Group Types
  + Security
  + Distribution
* Group Scope
  + Local Domain
  + Global
  + Universal

### Edit Group Form Attributes

Following is the List of the attributes that are defined on edit group form for either “Edit My Group” form.

* Description
  + Required
* Comment
  + Required
* Primary / Secondory Owners
  + List of Identities
* Is Requestable
* Members
* Group Types
  + Security
  + Distribution
* Group Scope
  + Local Domain
  + Global
  + Universal