PopMedNet Support Guide

Contents

[1 Overview 6](#_Toc391997050)

[2 Creating a new organization 7](#_Toc391997051)

[2.1 Organization Information Data 7](#_Toc391997053)

[2.2 Organization Provider Connection 7](#_Toc391997056)

[2.3 Organization Access Control 7](#_Toc391997057)

[2.3.1 Organization Access Control: Operations Center System Administrators Security Group 7](#_Toc391997058)

[2.3.2 Organization Access Control: Organization Administrators Security Group 8](#_Toc391997059)

[2.3.3 Organization Access Control: Organization Everyone Security Groups 9](#_Toc391997060)

[2.4 Organization Default Request ACL (Access Control List) 10](#_Toc391997061)

[2.5 Organization Default DataMart ACL 12](#_Toc391997062)

[2.5.1 Organization Default DataMart: Operations Center System Administrators Security Group 12](#_Toc391997063)

[2.5.2 Organization Default DataMart: Organization Administrators Security Group 13](#_Toc391997064)

[2.5.3 Organization Default DataMart: Organization DataMartAdministrators Security Group 15](#_Toc391997065)

[2.5.4 Organization Default DataMart: Organization Everyone Security Groups 18](#_Toc391997066)

[2.6 Organization Default User ACL 19](#_Toc391997067)

[2.6.1 Organization Default User: Operations Center System Administrators Security Group 19](#_Toc391997068)

[2.6.2 Organization Default User: Organization Administrators Security Group 20](#_Toc391997069)

[2.6.3 Organization Default User:Everyone Security Groups 20](#_Toc391997070)

[2.7 Organization Users 21](#_Toc391997071)

[2.8 Organization DataMarts 21](#_Toc391997072)

[2.9 Organization Security Groups 21](#_Toc391997073)

[2.9.1 Organization Security Groups: Organization Everyone Security Group 24](#_Toc391997074)

[2.9.2 Organization Security Groups: Organization Administrators Security Group 25](#_Toc391997075)

[3 Creating a new DataMart 27](#_Toc391997076)

[3.1 DataMart Information Data 27](#_Toc391997077)

[3.2 DataMart Installed Models 27](#_Toc391997079)

[3.3 DataMart Settings 28](#_Toc391997080)

[3.4 DataMart Access Control 28](#_Toc391997081)

[3.5 DataMart Downloads 31](#_Toc391997082)

[4 Creating a new group 31](#_Toc391997083)

[4.1 Group Information 31](#_Toc391997084)

[4.2 Group Organizations 32](#_Toc391997085)

[4.3 Group Projects 32](#_Toc391997086)

[4.4 Group Access Control 32](#_Toc391997087)

[4.4.1 Group Access Control: Operation Center System Administrators Security Group 32](#_Toc391997089)

[4.4.2 Group Access Control: Everyone Security Groups 33](#_Toc391997090)

[4.4.3 Group Access Control: Organization Group Administrators Security Group 33](#_Toc391997091)

[5 Creating a new project within a network 34](#_Toc391997092)

[5.1 Project Information 34](#_Toc391997093)

[5.2 Project Access Control 35](#_Toc391997094)

[5.2.1 Project Access Control: Operation Center System Administrators 35](#_Toc391997095)

[5.2.2 Project Access Control: Project Administrators 35](#_Toc391997096)

[5.2.3 Project Access Control: Group Administrators 36](#_Toc391997097)

[5.2.4 Project Access Control: Project DataMartAdministrators 36](#_Toc391997098)

[5.2.5 Project Access Control: Project Enhanced Investigators 37](#_Toc391997099)

[5.2.6 Project Access Control Project Observers 37](#_Toc391997100)

[5.3 Project Default DataMart ACL 38](#_Toc391997105)

[5.4 Project Default Request ACL 38](#_Toc391997106)

[5.4.1 Project Default Request: Enhanced Investigators 39](#_Toc391997107)

[5.4.2 Project Default Request: Observers 41](#_Toc391997108)

[5.5 Project Security Groups 41](#_Toc391997109)

[5.6 Project DataMarts 41](#_Toc391997110)

[5.6.1 Project DataMart: Organization DataMartAdministrators 42](#_Toc391997111)

[Project DataMart: Project Enhanced Investigators 45](#_Toc391997112)

[5.6.2 45](#_Toc391997113)

[5.7 Project Organizations 48](#_Toc391997114)

[6 Creating a new user 56](#_Toc391997134)

[6.1 Create a new user through the registration form 56](#_Toc391997135)

[6.1.1 New User Registration Task List 57](#_Toc391997136)

[6.1.2 New User Registration Review and Approval 58](#_Toc391997137)

[6.2 Create a new user through the user list page 60](#_Toc391997139)

[6.3 User Contact Information 61](#_Toc391997140)

[6.4 User Member of Groups 62](#_Toc391997141)

[6.5 Permissions on this User Object 62](#_Toc391997142)

[6.6 User Credentials 63](#_Toc391997144)

[6.7 User Notifications 63](#_Toc391997145)

[7 Issues 63](#_Toc391997146)

[7.1 Group Administrators 63](#_Toc391997147)

[7.2 Creating New Users 63](#_Toc391997148)

[7.3 Approving New Users 64](#_Toc391997149)

[7.4 Defaulting Project Organization Rights 64](#_Toc391997150)

[7.5 Defaulting Project DataMarts Rights 64](#_Toc391997151)

**Change Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Author** | **Date** | **Description** |
| 0.1 | Bruce Swan | 4/24/2013 | Created |
| 0.2 | Melanie Davies | 7/1/2013 | Edited |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Overview

PopMedNet administrators need to understand how to support PopMedNet (PMN) networks. This guide is intended to assist administrators in configuring new Groups, Organizations, Users, DataMarts, and Projects. Assuming administrators understand the major entities and relationships to each other within PMN (i.e. has read the PMN user guides), the most difficult part of creating new PMN entities is configuring access control for them. To assist this process we have created a starter PMN database that may be used for a new PMN instance. It contains a set of templates that may be referenced and copied when administrators are creating new entities.

This guide references two configuration options:

* Centralized access control management: only system administrators are permitted to manage access controls, including approving users. This is the configuration option used in all HPHCI-administered networks.
* Decentralized access control management: system administrators manage network-wide access, but share project and organization-level access control management with project and organization administrators.

# Creating a new organization

PMN may have one or more Organizations, each of which may have one or more Users and one or more DataMarts. There are two ways to create an organization. Copy the “Organization Template” or click on the **Add** button the Network/Organizations list. The template has a set of preconfigured security groups that can be used to assign to users. The security groups are listed under the Security Groups section below. If the organization is created by clicking the **Add** button, the template can be used as a reference to configure the organization’s security groups and access controls.

## Organization Information Data

Enter the name and acronym, used as a short name in some displays, for the organization. Organizations may be configured as parents and children. If the organization is a child, click the Parent link and select the parent organization. All other information and metadata fields within the organization, including registries and research data sets, may be entered by the organization administrator.

## Organization Provider Connection

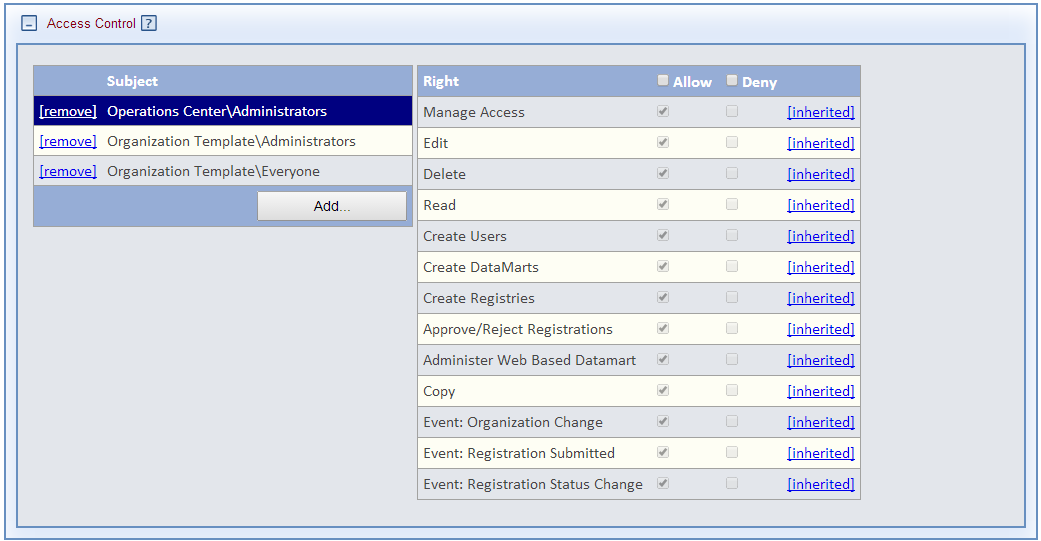
The provider connection panel is used to connect an instance of the web based DataMart client to the portal to administer the organization’s DataMarts. Additionally, one organization within the physical PMN network instance must be designated as the network owner. This role will be held by the Operations Center organization on each network.

## Organization Access Control

The Access Control panel is used to configure the rights to administer the organization.

### Organization Access Control: Operations Center System Administrators Security Group

Operations Center System Administrators have rights to completely administer any organization. These rights are inherited from the Global Access Controls and are shown below:

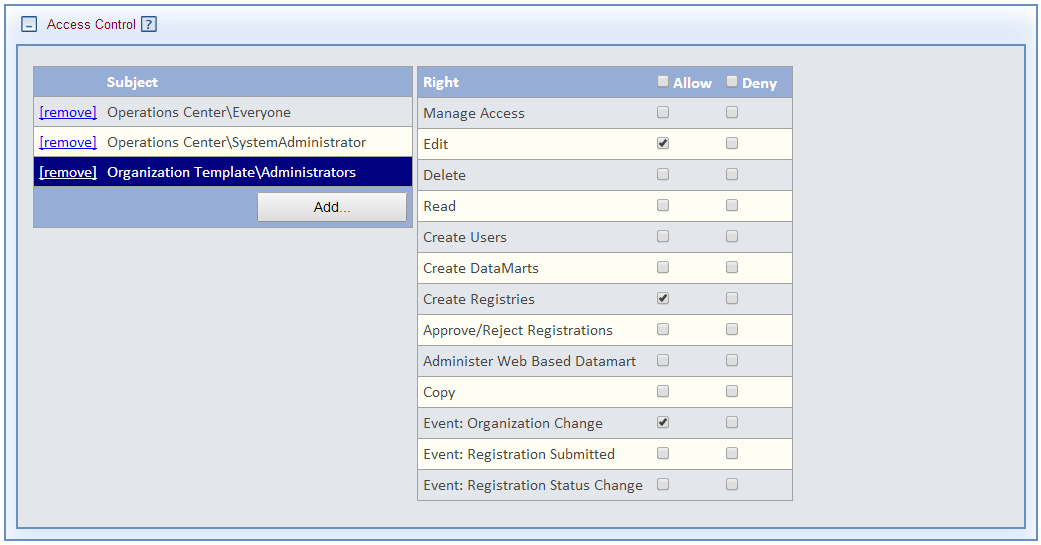


### Organization Access Control: Organization Administrators Security Group

Each organization should have one or more users who are Administrators of their organizations. This role may also be designated to a user from another organization.

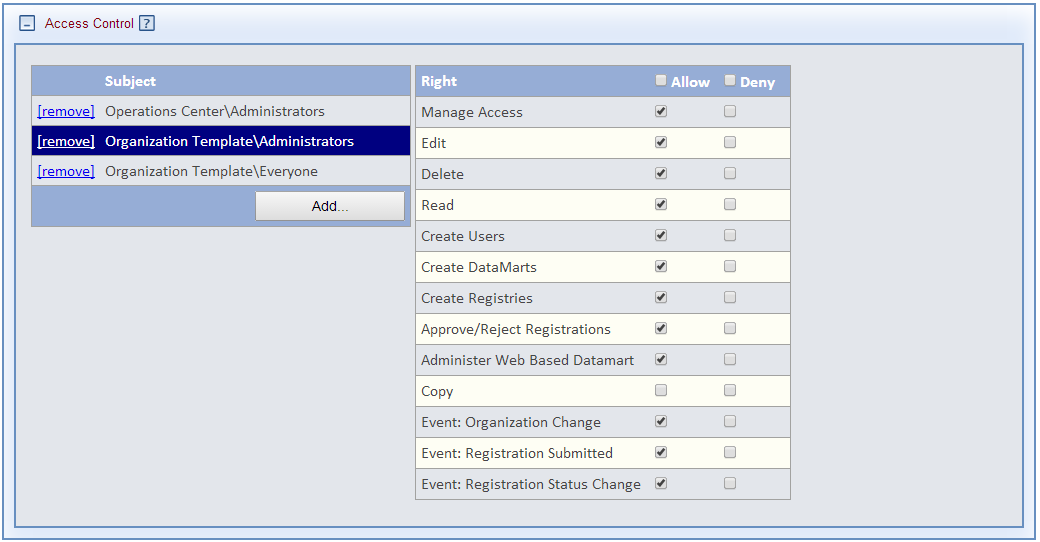
#### Centralized

Organization administrators are restricted to editing metadata about the organization and receiving notifications when their organization profile is changed. The security group should be configured as follows:



#### Decentralized

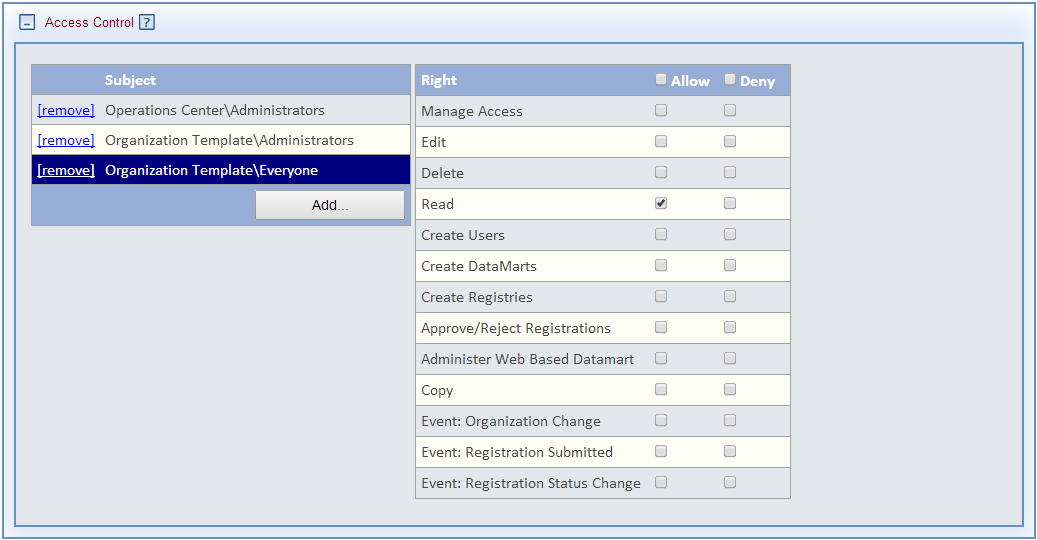
Organization administrators have full access to administer the organization and the organization’s entities (users, DataMarts, child organizations). The security group should be configured as follows:



### Organization Access Control: Organization Everyone Security Groups

The **Read** organization access control grants users the right to view the organization’s metadata information. Which security groups are granted access to this right will differ by network/sub-network:

* Anyone in the network: Enable the right for the Operations Center Everyone security group.
* Only users from select organizations (e.g. members of a group): Enable the right for every organization’s Everyone security group.
* Only users in the organization: Enable the right for only the organization’s Everyone security group. This is shown in the figure below:



## Organization Default Request ACL (Access Control List)

The Default Request ACL panel can be used to configure request rights that are in effect across all projects the organization participates in. Alternatively, these same rights can be specified for each project, allowing the rights to vary by projects. Rights enabled in the organization may be overridden in a given project. Because members of an organization may participate in different projects, it is generally preferred to assign request permissions at the project level. Therefore, this ACL panel may be left empty.

## Organization Default DataMart ACL

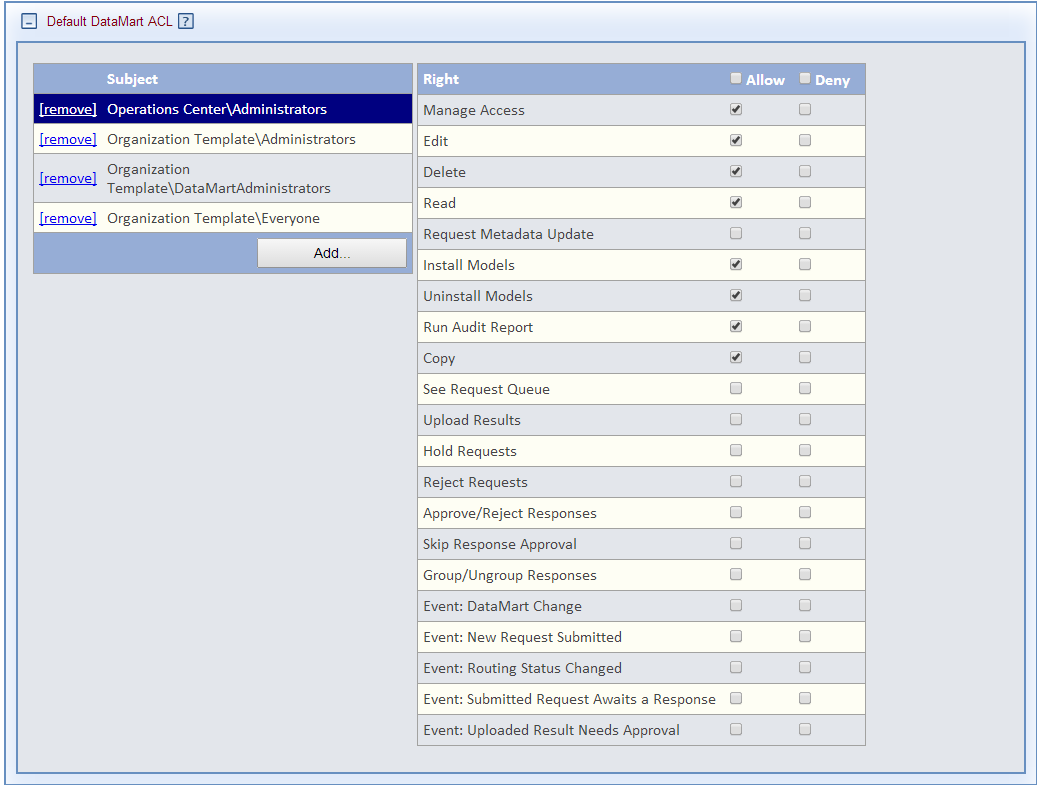
The Default DataMart ACL panel can be used to configure DataMart administration rights that are in effect across all projects the organization participates in. Alternatively, these same rights can be specified at the project level, allowing the rights to vary by projects. Rights enabled at the organization level may be overridden in a given project. Because members of an organization may participate in different projects, it is generally preferred to assign most DataMart permissions at the project level.

The “Organization Template” contains defaults for three security groups.

### Organization Default DataMart: Operations Center System Administrators Security Group

The Operations Center System Administrators group should be configured to administer all DataMarts in the organization.

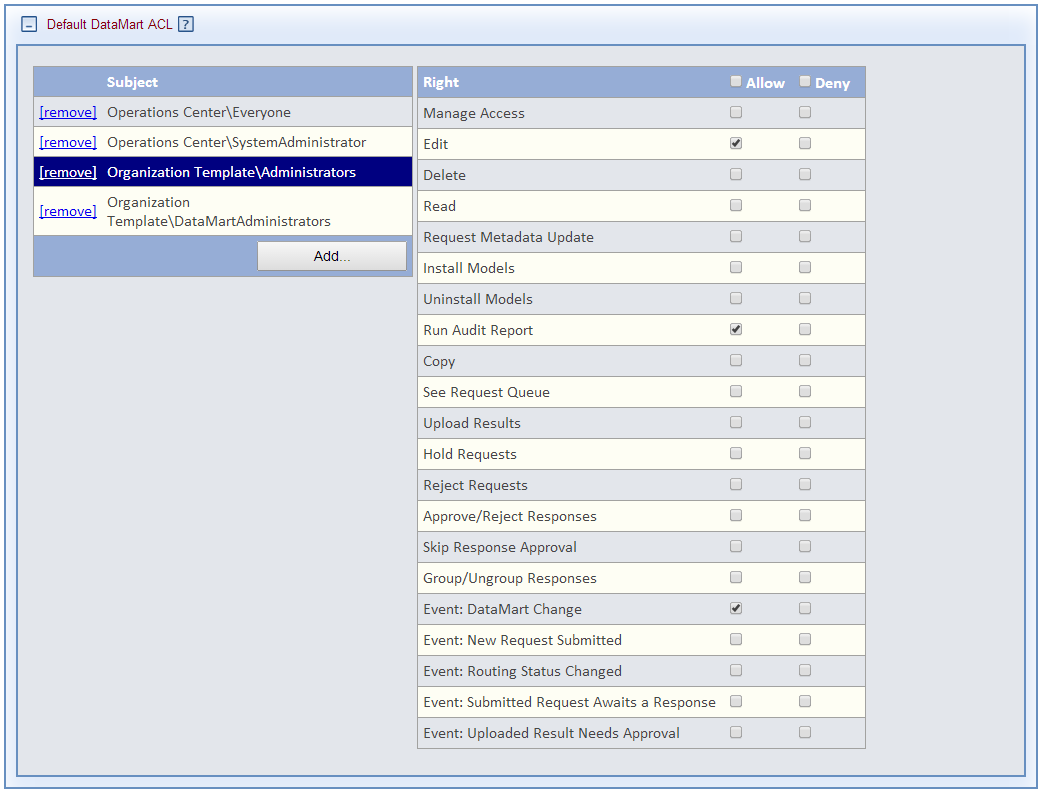
It is configured as follows:



### Organization Default DataMart: Organization Administrators Security Group

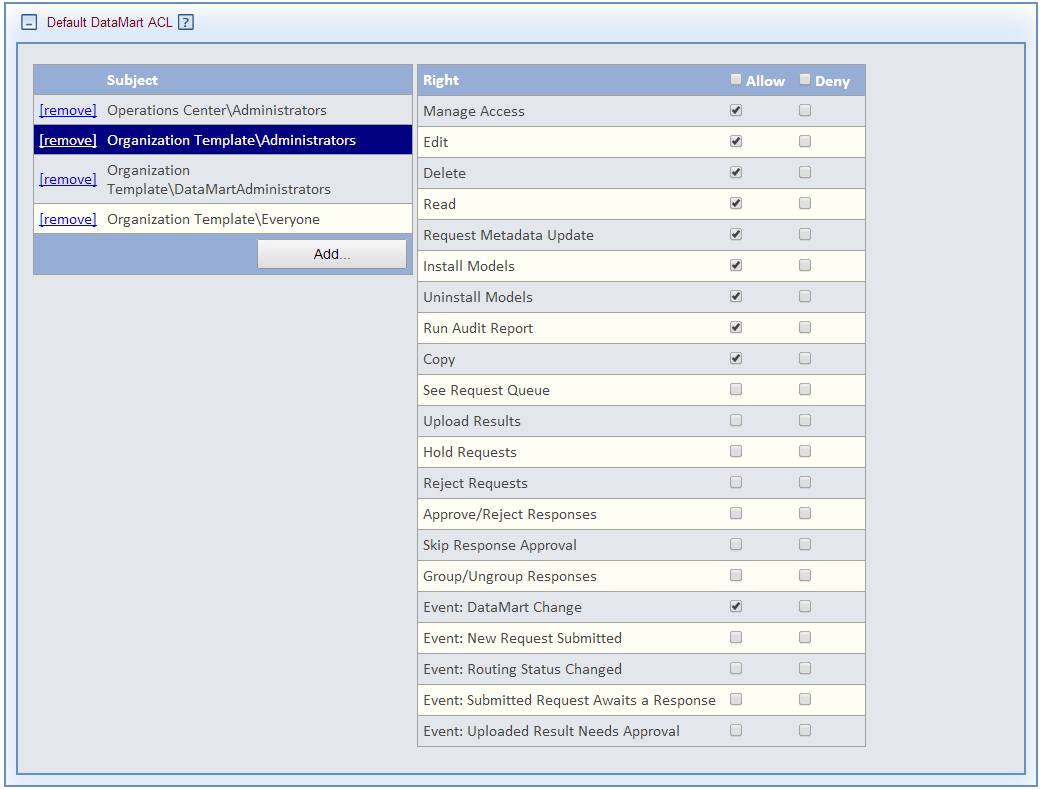
#### Centralized

Organization Administrators should be able to edit the metadata for the organization’s DataMarts and monitor their DataMart activity. This security group is configured as follows:



#### Decentralized

Organization Administrators should be able to configure and manage the organization’s DataMarts. This security group is configured as follows:

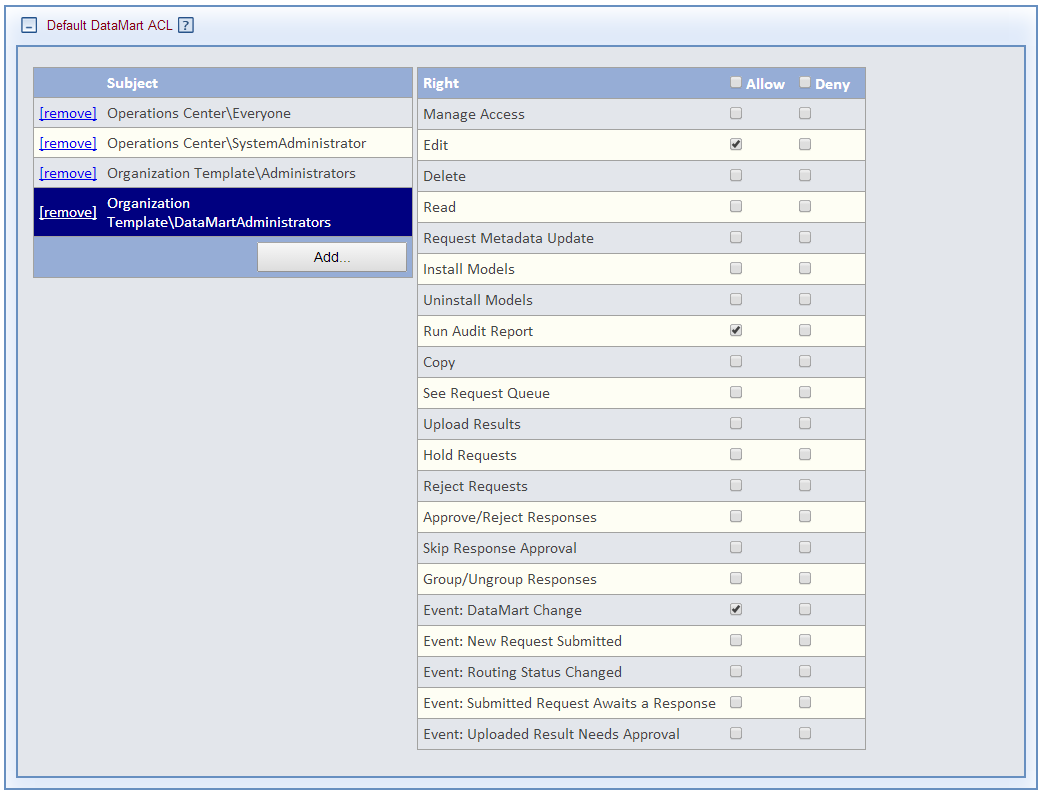


### Organization Default DataMart: Organization DataMartAdministrators Security Group

The organization’s DataMartAdministrators group is assigned to users who administer the organization’s DataMarts.

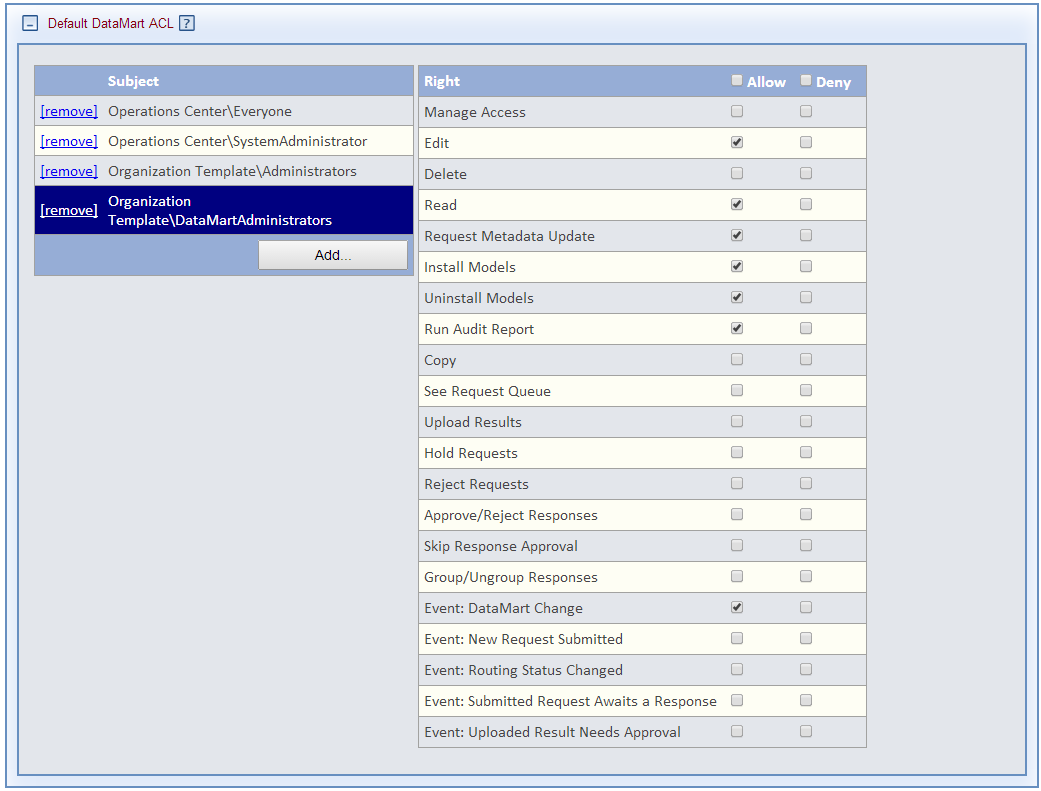
#### Centralized

Organization DataMartAdministrators should be able to edit the metadata for the organization’s DataMarts and monitor their DataMarts activities. This security group should be configured as follows:



#### Decentralized

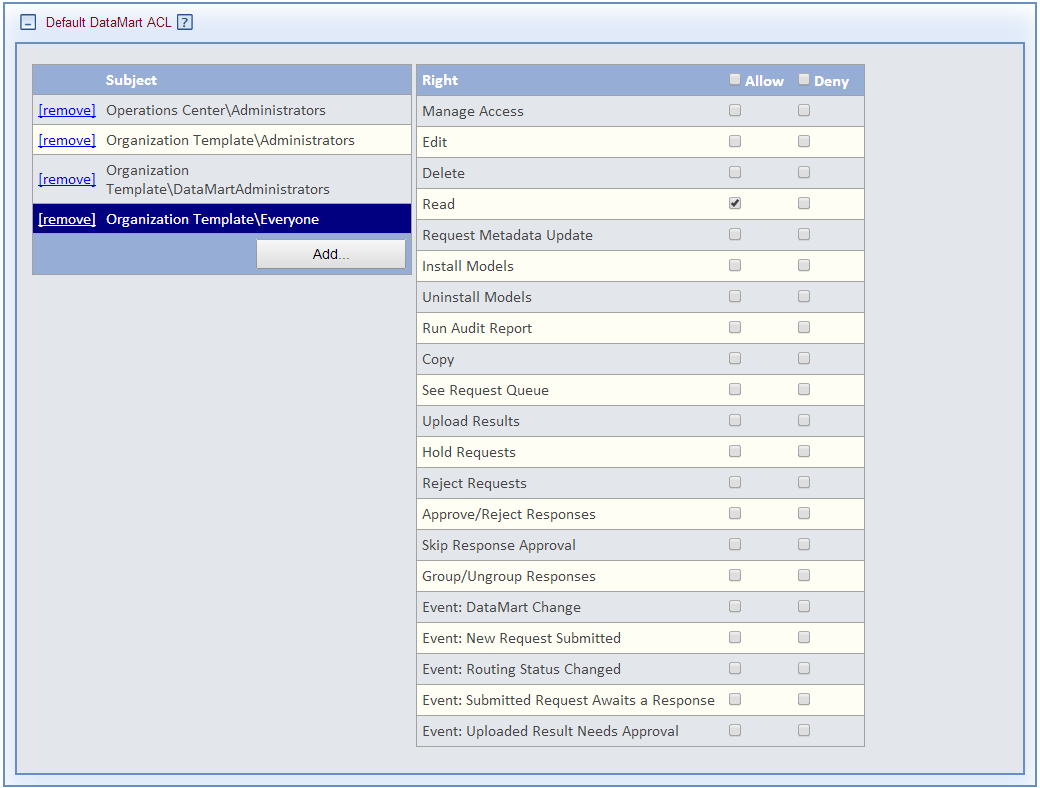
Organization DataMartAdministrators should be able to configure and manage the organization’s DataMarts. This security group is configured as follows:



### Organization Default DataMart: Organization Everyone Security Groups

The **Read** organization access control grants users the right to view the DataMart’s metadata information. Which security groups are granted access to this right will differ by network/sub-network:

* Anyone in the network: Enable the right for the Operations Center Everyone security group.
* Only users from select organizations (e.g. members of a group): Enable the right for every organization’s Everyone security group.
* Only users in the organization: Enable the right for only the organization’s Everyone security group. This is shown in the figure below:

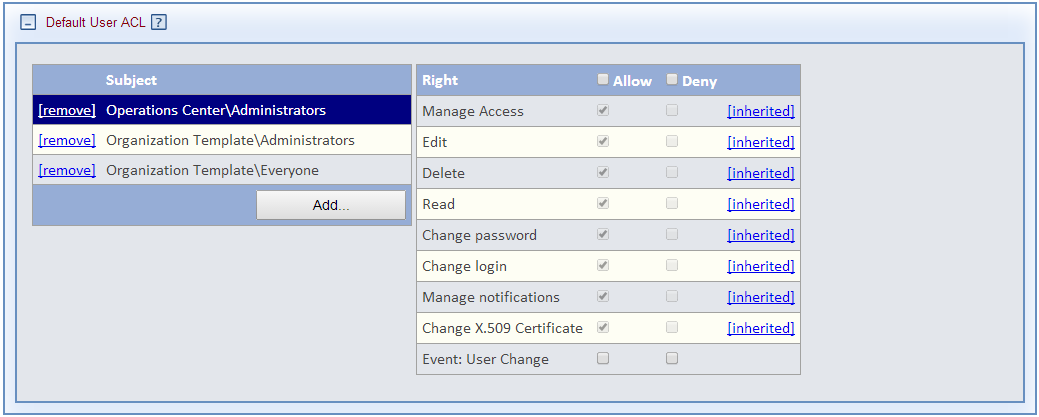


## Organization Default User ACL

The Default User ACL panel is used to grant the rights to configure users within the organization and manage their profile.

### Organization Default User: Operations Center System Administrators Security Group

By default, the Operations Center System Administrators group is configured to administer all users in the organization. The rights are inherited from the Global Access Controls. It is configured as follows:



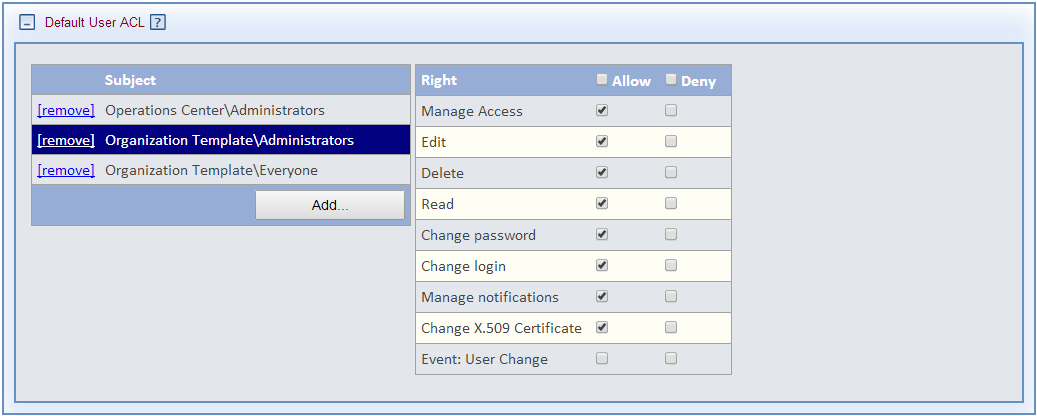
### Organization Default User: Organization Administrators Security Group

#### Centralized

Organization Administrators should not have rights to configure or manage their users.

#### Decentralized

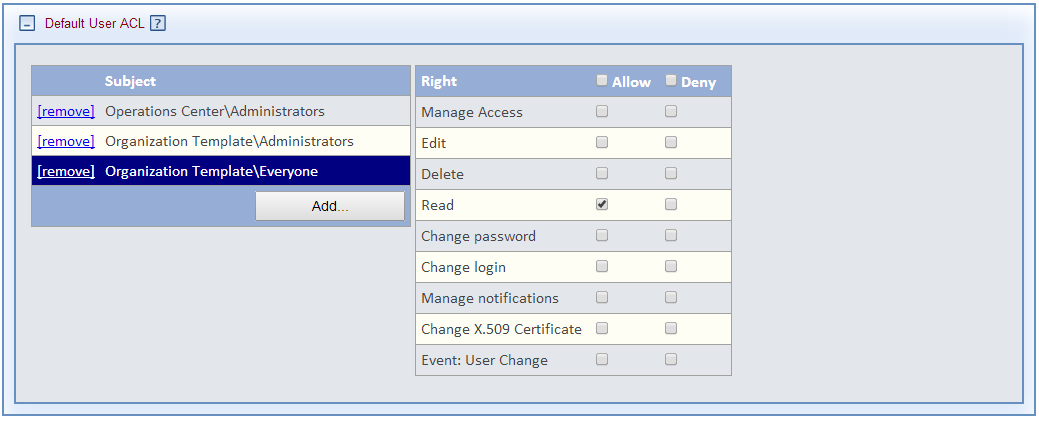
Organization Administrators should be able to configure and manage their users. The security group is configured as follows:



### Organization Default User:Everyone Security Groups

The **Read** organization access control grants users the right to view the DataMart’s metadata information. Which security groups are granted access to this right will differ by network:

* Anyone in the network: Enable the right for the Operations Center Everyone security group.
* Only users from select organizations (e.g. members of a group): Enable the right for every organization’s Everyone security group.
* Only users in the organization: Enable the right for only the organization’s Everyone security group. This is shown in the figure below:



## Organization Users

The Users panel displays the list of users within the organization. Users can be added here or through the Network Users list, or a user can use the “Register for a new account” link on the logon page. See the section on Creating a new user below for details on this process.

**Note: It is highly recommended that users go through the new user registration process rather than have administrator manually create them to reduce the need for administrators to handle user credentials.**

## Organization DataMarts

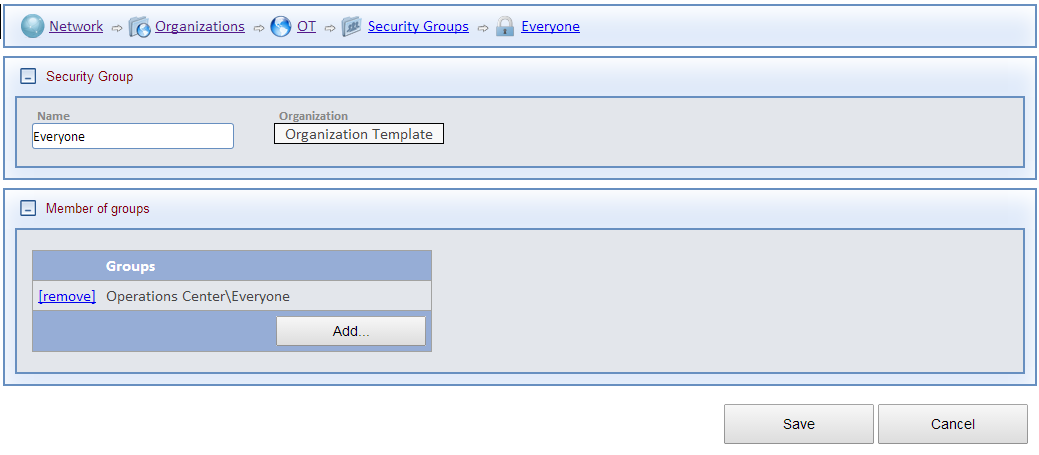
The DataMarts panel displays the list of DataMarts within the organization. A DataMart can be added here or through the Network DataMarts. See the section on Creating a new DataMart below for details on this process.

## Organization Security Groups

Users may be assigned rights directly or indirectly through Security Groups. A Security Group has one or more rights assigned to it. Users may be a member of one or more Security Groups where they inherit the rights of the group. A Security Group may itself inherit the rights of another Security Group to form a hierarchy of rights. An Organization may have one or more Security Groups that may be assigned to users of the organization or to users of another organization within the organizational group. Note that Projects also have a set of predefined Security Groups that are specific to a given project. Together security groups allow administrators to configure roles for users. Custom security groups may be created, configured, and assigned to users in addition to the predefined set.

**NOTE: It is recommended that rights be assigned to users through Security Groups rather than by directly assigning a right to specific user.**

To make a security group inherit another security group, click the name of the security group that will inherit the rights. Click **Add** on the next screen and select the security group that the rights should be inherited from.

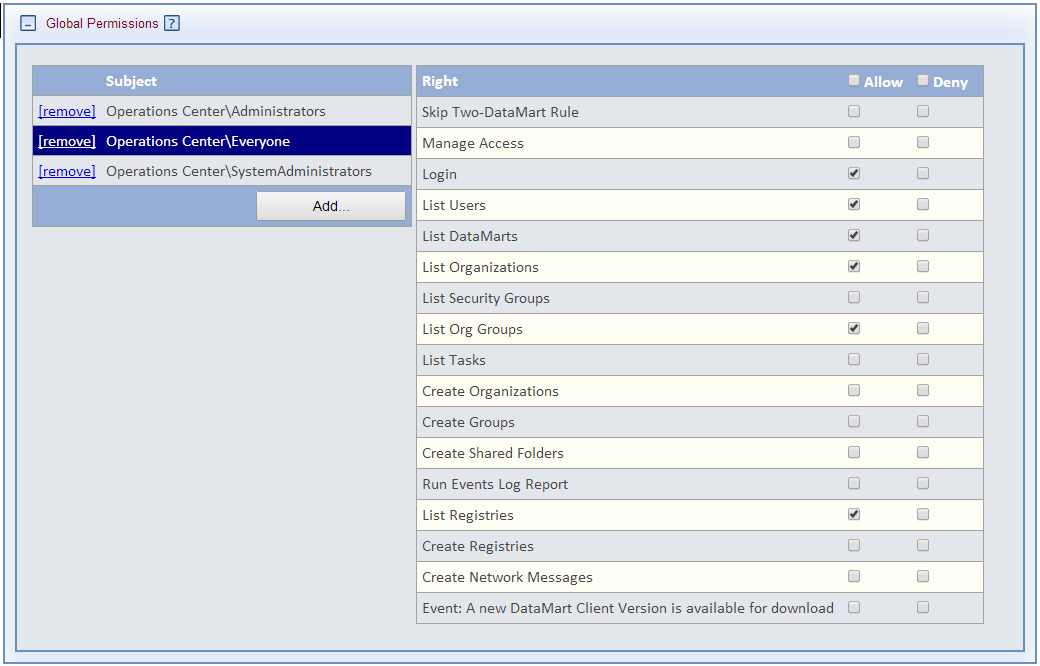


To assist Administrators, there a set of predefined Security Groups that are part of an Organization and Project. See the “Organizational Template” to view the rights assigned to each of these groups. The table below describe these groups.

|  |  |
| --- | --- |
| Security Group | Description |
| Everyone | Base security group for which each organization’s user should be a member. This includes the rights to login and view their own organization, its users and DataMarts. This group inherits the rights of the Operations Center Everyone security group. |
| Administrators | Users who administer an organization  *Centralized* – includes the rights to edit organization and DataMart metadata and monitor organization and DataMart activity  *Decentralized -* includes the rights to create/modify/delete users, approve new users, create/modify/delete DataMarts, edit their organization and DataMart metadata and create/modify/delete sub-organizations. This group inherits the rights of the Operations Center Administrator security group. |
| Investigators | Users who issue queries and can view the aggregated results from DataMarts |
| Enhanced Investigators | Users who issue queries and can view the individual and aggregated results of DataMarts. |
| QueryAdministrators | Users who approve queries issued from investigators within their organization |
| DataMartAdministrators | Users who administer one or more of their organization’s DataMarts |
| GroupDataMartAdministrators | Users who approve the results that have been uploaded by DataMart administrators within their organization or sub-organizations |
| Observers | Users who monitor queries and other activities within their organization |

### Organization Security Groups: Organization Everyone Security Group

The organization’s Everyone security group should inherit the Operations Center Everyone security group. Basic access, such as the right to login and view lists, is granted to the Operations Center Everyone security group and then inherited by each organization. The figure below shows the settings for the Operations Center Everyone security group, configured at the Global Access Control level.



### Organization Security Groups: Organization Administrators Security Group

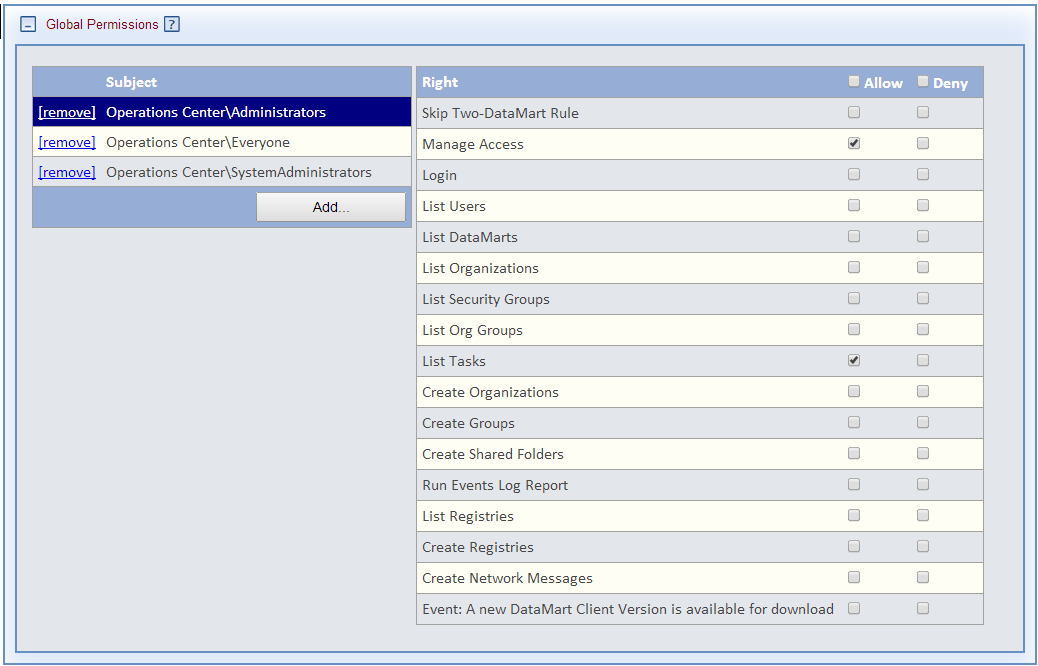
#### Centralized

The organization’s Administrator group does not inherit any security groups.

#### Decentralized

The organization’s Everyone security group should inherit the Operations Center Administrator security group. This grants organization Administrators the rights to view the Task panel where they may approve users. The figure below shows the settings for the Operations Center Administrators group.

**Note: this setup requires that Operations Center Administrators do not have system administration rights and instead that a custom System Administrator security group was created for the Operations Center and system administrator rights were granted to that group.**



# Creating a new DataMart

An Organization may have zero, one, or more DataMarts. There are two ways to create a DataMart. Copy the “DataMart Template” or click on the **Add** button the Network/DataMarts list or from the organization’s DataMart list.

## DataMart Information Data

Enter the name and acronym, used as a short name in some displays, for the DataMart. All the other information and metadata fields within the organization may be entered by the organization Administrator or the DataMart Administrator.

**NOTE: When adding new DataMart, ensure the organization link in the information panel is set to the correct organization.**

## DataMart Installed Models

The “DataMart Template” has two models installed, the ESP plugin containing the Query Composer, and the File Distribution plugin. Additional models may be installed and existing models uninstalled from the Install Models panel.

#### Centralized

Only System Administrators may install and uninstall models.

#### Decentralized

Organization and DataMart Administrators may install and uninstall models.

## DataMart Settings

The Settings panel allows organization or DataMart Administrators to set the operating mode of the DataMart. This directly affects the operation of the Web-based DataMart Client. This setting is configured directly in the desktop-based DataMart Client.

**Note: DataMart unattended operations settings interact with the request settings at the project or organization level. If a request type is not set to auto at the project or organization level, it will not run automatically in the DataMart Client regardless of the unattended operation settings.**

## DataMart Access Control

The Access Control panel is used to configure the default DataMart rights. All rights in this panel are inherited from the DataMart’s organization access controls.

## DataMart Downloads

The Downloads panel is used by DataMart administrators to download and install the desktop DataMart client application.

# Creating a new group

PMN uses Groups to organize one or more Organizations into a sub-network to work on one or more Projects. To create a new group, click on Network/Groups to see the list of existing groups. Click the **Add** button to view the group form, enter its name, and click **Save**. Once saved, edit the group and configure it according the following sections.

**Note: the term Group is used in two different contexts within PMN; as an organizational group described here, and as a Security Group, used to assign sets of rights to users.**

## Group Information

Enter a short display name for the group.

## Group Organizations

In order for an organization to participate in a group project, it must be a member of the group. Click the **Add** button to see the list of organizations that are available to join the group. Once saved, the new organization’s security groups, users, and DataMarts will be visible within the group’s project page controls.

## Group Projects

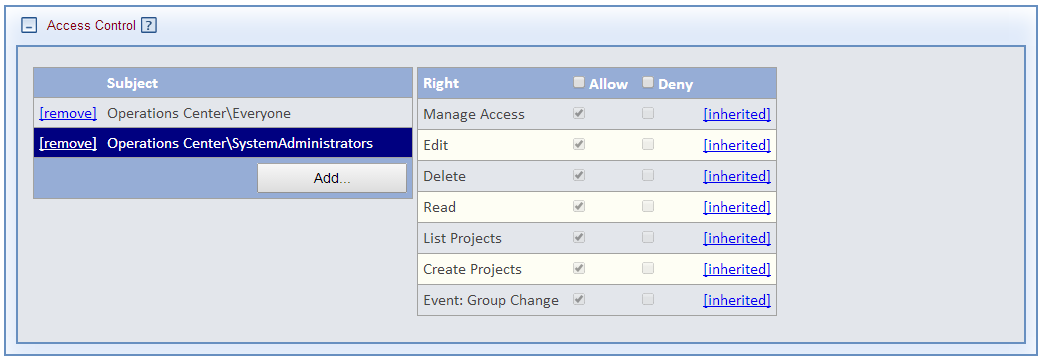
Projects are used to issue and respond to requests and view responses. A Group may have one or more projects. There are two ways to add a project: copy the “Project Template” or click the **Add** button to create a project. See the section below on Creating a new project within a network for details on configuring a project.

## Group Access Control

The Group Access Control panel contains rights to edit, manage access to the group, and create projects within the group. There is a Group Template that may be used a reference when creating new groups. Note that, unlike organizations, DataMarts, and projects, groups may not be copied.

### Group Access Control: Operation Center System Administrators Security Group

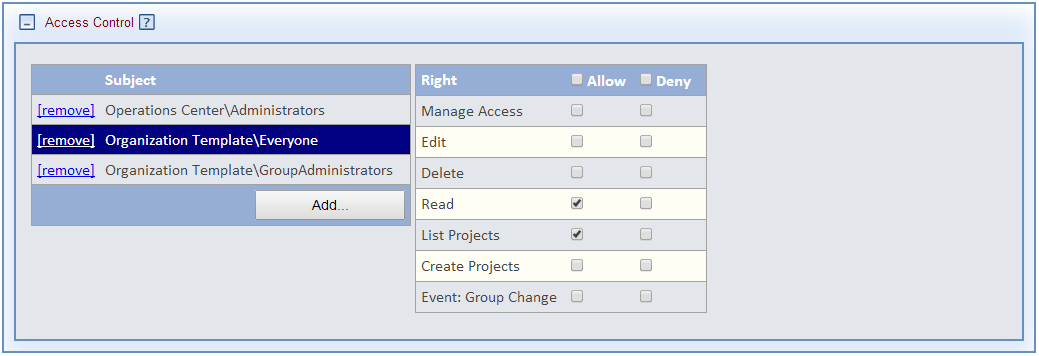
Operations Center System Administrators may completely manage any group. These rights are inherited from the Global Access Controls. The figure below shows these inherited rights:



### Group Access Control: Everyone Security Groups

The **Read** organization access control grants users the right to view the group’s metadata information and projects. Which security groups are granted access to this right will differ by network/sub-network:

* Anyone in the network: Enable the right for the Operations Center/Everyone security group.
* Only users in the group (sub-network): Among organizations that belong to the group, enable the right for their organization Everyone security groups. This is shown in the figure below:



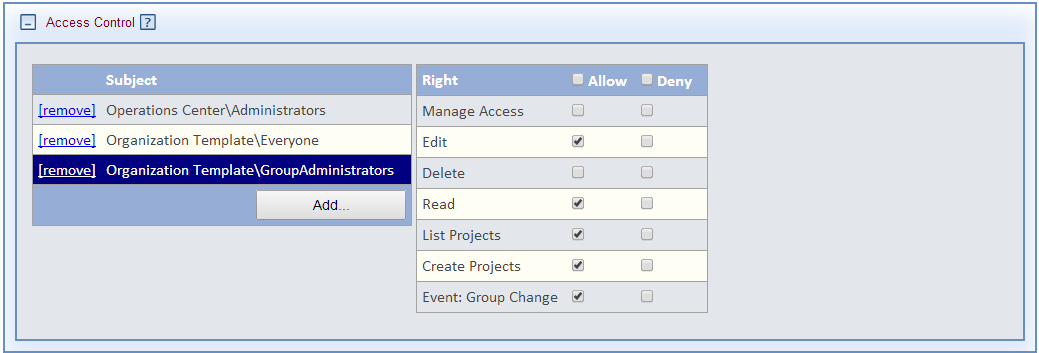
### Group Access Control: Organization Group Administrators Security Group

#### Centralized

Only System Administrators have rights to manage groups.

#### Decentralized

An organization’s Group Administrator may be granted rights to manage the group and create projects. These settings are shown in the figure below.



# Creating a new project within a network

A PMN Group may have one or more Projects. All requests are issued within the context of a project. A project may configured to include users and DataMarts from any organization that is a member of the project’s group. There are two ways to create a project: copy the “Project Template” or click on the **Add** button the Network/Projects list or the Group Projects panel.

The template has a set of preconfigured security groups that can be used to assign to users. The security groups are listed under the Security Groups section below. If the project is created by clicking the **Add** button, the template can be used as a reference to configure the project’s security groups and access controls.

## Project Information

Enter the name and acronym, used as a short name in some displays, for the project. The Start Date and End Date is used to control the period for which new requests can be submitted. The Active flag is used to control submitting new requests to the project within the start/end period.

**NOTE: When adding a new Project, ensure the Group link in the information panel is set to the correct group.**

#### Centralized

The description field may only be entered by the System Administrator.

#### Decentralized

The description field may be entered by the project Administrator.

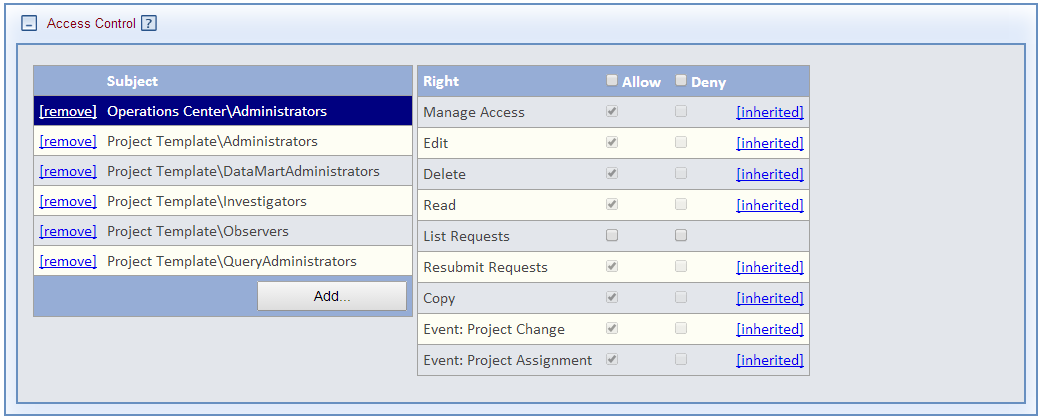
## Project Access Control

The Access Control panel is used to configure the rights to administer the project and to use the project. Projects have their own Security Groups that may be used to assign sets of rights to users. The “Project Template” has a set of security groups that mirror those that are in the “Organization Template”. See the section on Security Groups in the Organization section above for details.

**Note: The access controls for this project are based on the most common project configuration across the PopMedNet networks. In this configuration, all investigators are Enhanced Investigators and may view individual results. DataMart Administrators may submit requests to their own DataMart. There is no approval required for submitting requests or approval needed before results are returned to the investigator.**

### Project Access Control: Operation Center System Administrators

By default, the Operations Center System Administrator has rights to completely administer any project. These rights are inherited from the Global Access Controls.



### Project Access Control: Project Administrators

#### Centralized

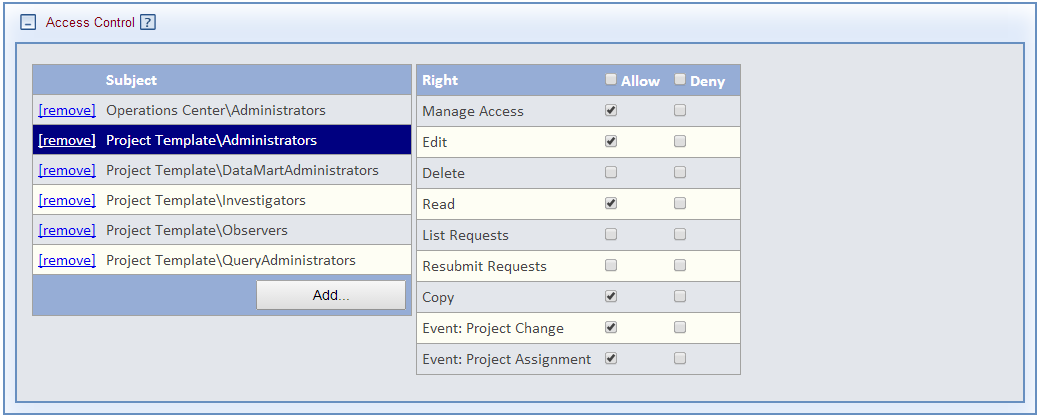
Only System Administrators have the rights to administer projects in the network.

#### Decentralized

Project Administrators may manage the access control of the project, edit the project information, and copy the project.

**NOTE: It is recommended that at least one user from one of the organizations participating in the project be assigned as the project Administrator.**

The project Administrators security group is configured as follows:



### Project Access Control: Group Administrators

#### Centralized

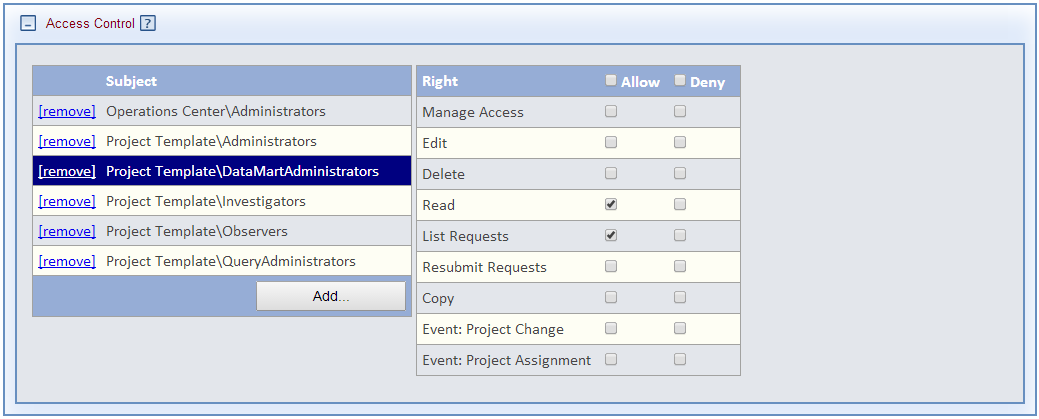
Only System Administrators have rights to administer projects in the network.

#### Decentralized

If Group Administrators were utilized in step Group Project Access Control Organization GroupAdministrators Security Group above, then they should be granted the same rights as project Administrators above.

### Project Access Control: Project DataMartAdministrators

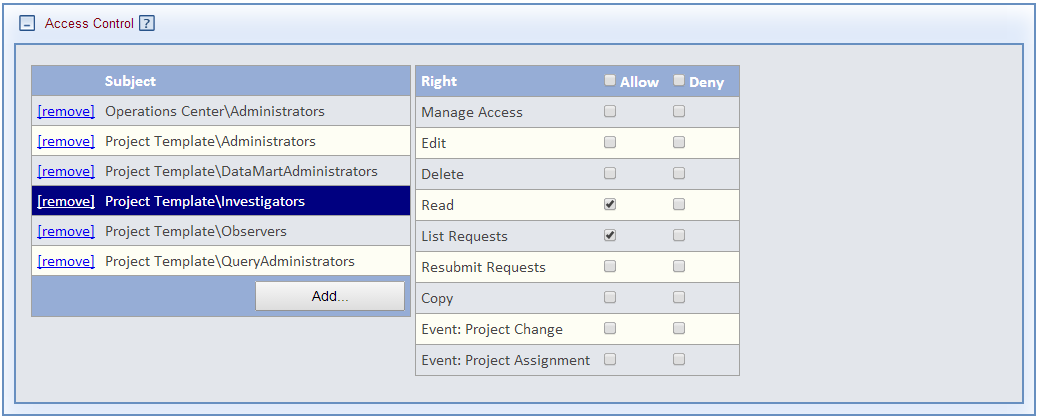
DataMart administrators whose DataMarts participate in the project must be assigned rights to view and list requests within the project so they can submit queries to the DataMarts they administer. The DataMartAdminstrators security group is configured as follows:



### Project Access Control: Project Enhanced Investigators

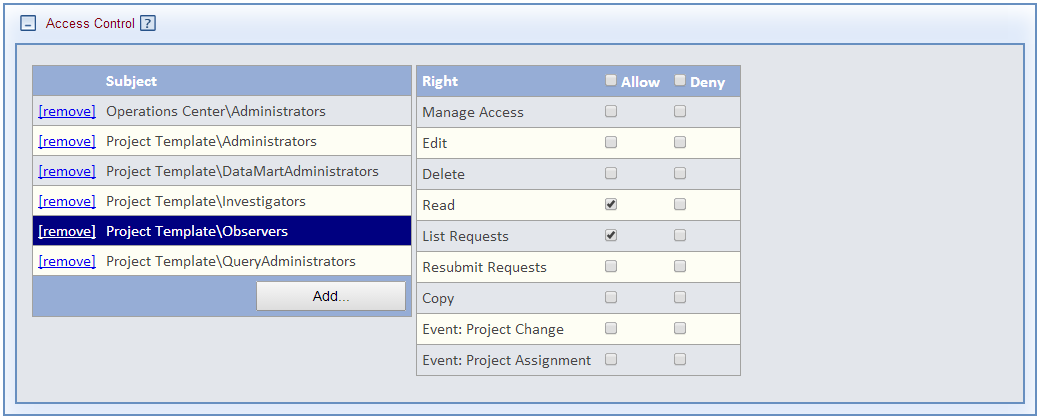
Enhanced Investigators who participate in the project must be assigned rights to view and list requests within the project so they can submit queries to the project DataMarts.

The Enhanced Investigators security group is configured as follows:



### Project Access Control Project Observers

Observers monitor the activities of the project. They must be assigned rights to view the project and see requests issue within the project. The Observers security group is configured as follows:



## Project Default DataMart ACL

The Default DataMart ACL panel is used to configure default rights for all DataMarts that are used in the project. At this time, it is not recommended that any settings be applied in this panel.

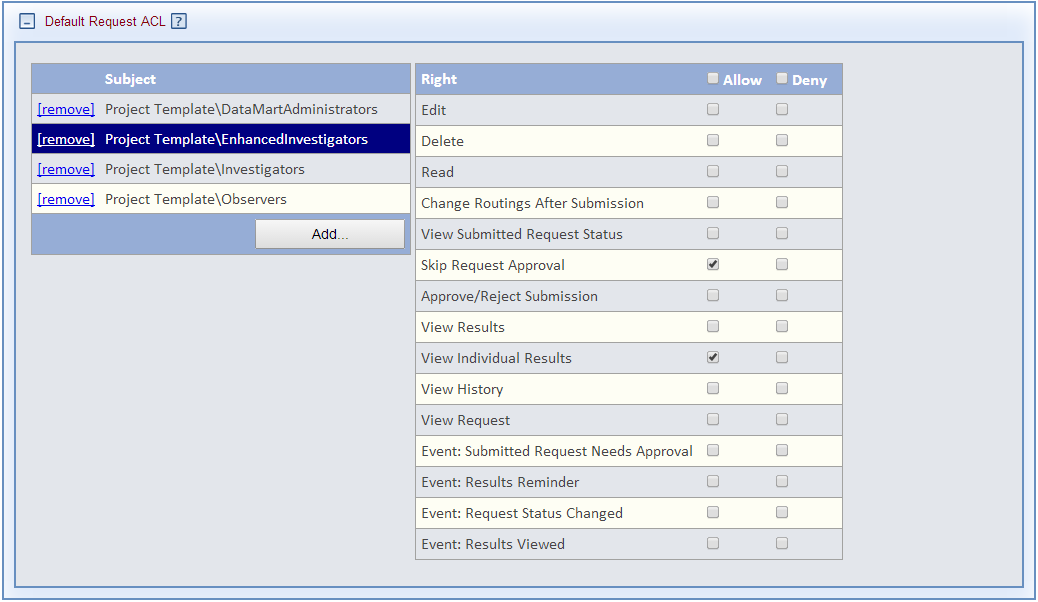
## Project Default Request ACL

The Default Request ACL panel is used to configure default rights for all requests that are issued within the project. The “Project Template” has a set of assignments to its security groups.

### Project Default Request: Enhanced Investigators

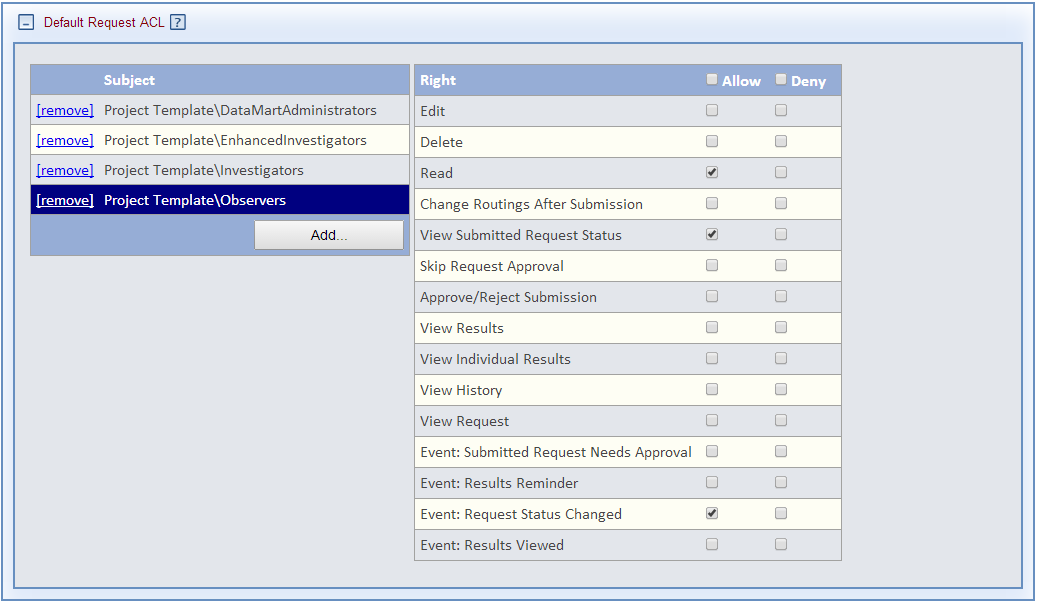
Project Enhanced Investigators have rights that allow them to delete their draft requests, change DataMart routings after submission, skip request approval, view individual results, and view the history of their requests.

**Note: There are certain rights that users receive implicitly if they have rights to submit requests. These include the rights to view their requests, edit their draft requests, view the results of their requests, and subscribe to notifications regarding their requests. The rights granted in the Default Request ACL panel apply to every request in the project that the user has permission to view. Therefore security groups should only be granted the Read right if they should be able to view every request in the Project. If they do not have the Read right, then the rights selected in this panel will only apply to the requests that the user has created.**



### Project Default Request: Observers

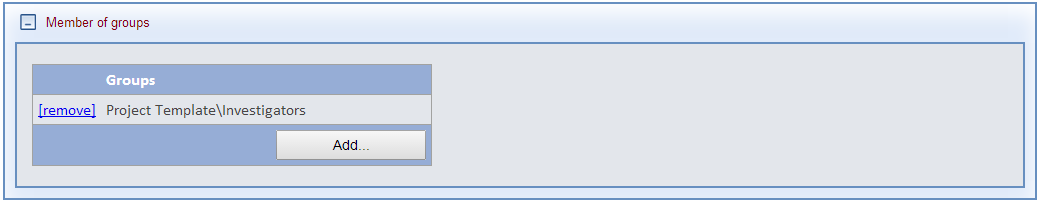
Project Observers have rights to view all requests submitted within the project, see their request status, view history, and subscribe to events that notify them when a request status changes.



## Project Security Groups

Projects have a set of security groups that may be assigned rights within the project. These groups match those from organizations. The security groups in “Template Project” have the ACL assignments presented in the above sections.

The Enhanced Investigators group inherits the rights assigned from the Investigators group as follows:



## Project DataMarts

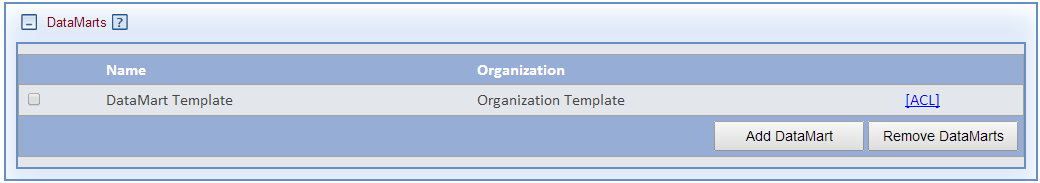
The DataMarts panel is used to select DataMarts to participate in a project. For a DataMart to be eligible for participation in a project, its organization or parent organization must be a member of the project’s group parent. Once a DataMart is added to the project, it can be configured for use within the project.

DataMart ACLs may be configured at three locations:

* ACL panel on the DataMart page
* Default DataMart ACL panel on the DataMart’s organization page
* In the ACL panel on the project’s DataMart entry in the DataMart panel

**NOTE: Given that the rights to a DataMart may differ by project and that the DataMart may be administered by users from different projects, it is recommend to configure the organization’s DataMart rights at the project level.**

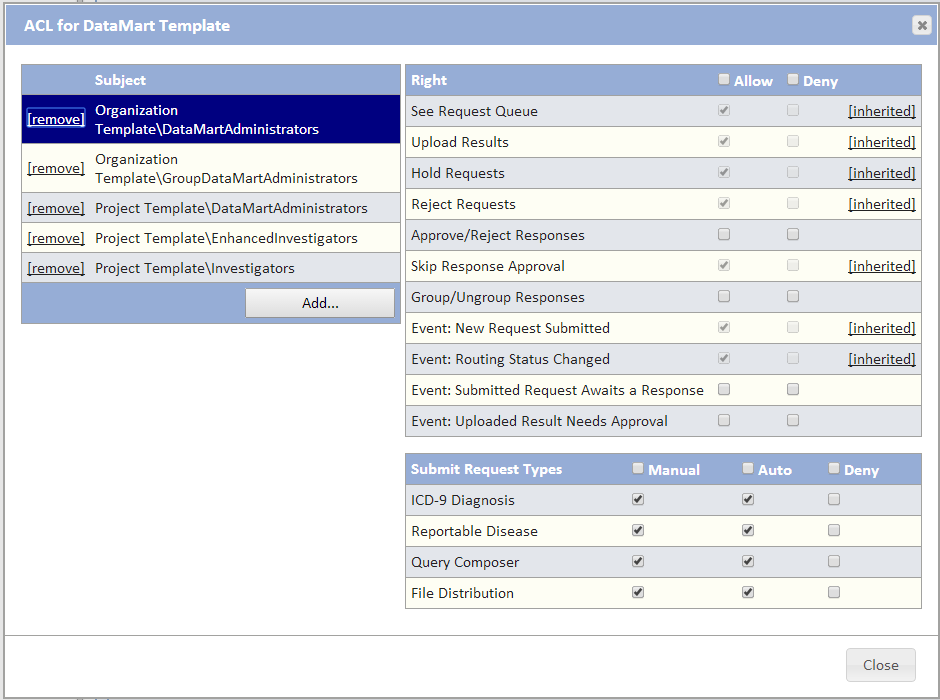
The “Project Template” has a single “DataMart Template” configured for use in the project.



The “DataMart Template” in the “Project Template” has the following settings.

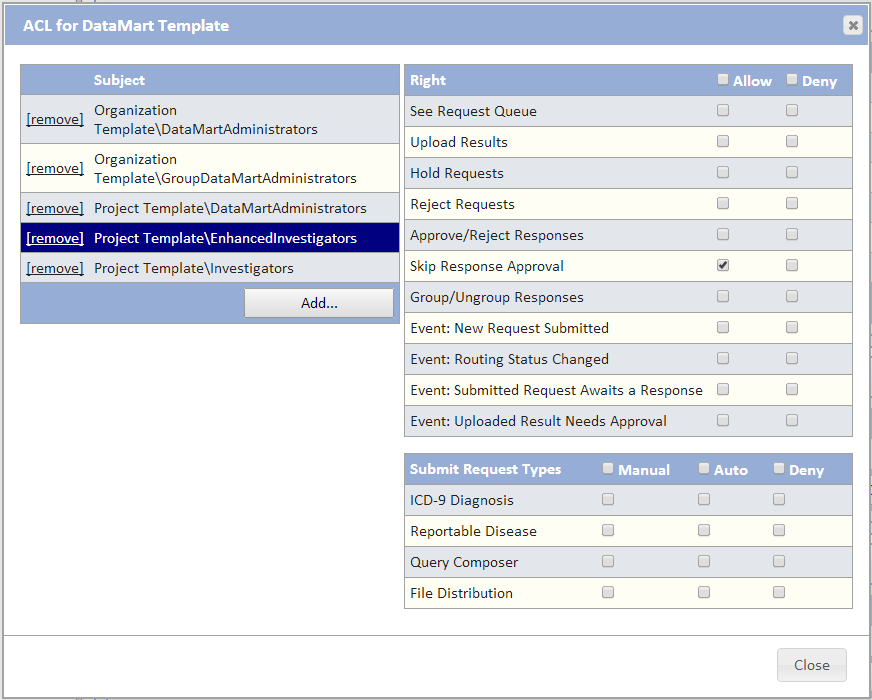
### Project DataMart: Organization DataMartAdministrators

The *Organization Template*/DataMartAdministrators has rights to administer the “DataMart Template” DataMart and to issue query types within the project, as shown below.



### Project DataMart: Project Enhanced Investigators

Enhanced Investigators should be granted the rights to skip response approval and to submit requests to this DataMart.



## Project Organizations

The Organizations panel is used to configure organization-specific access controls for organizations who participate in a project. For an Organization to be eligible for participation in a project, it must be a member of the project’s group parent. Once an Organization is added to the project, it can be configured for use within the project.

Organization ACLs may be configured in two locations:

* ACL panel on the Organization page
* In the Project Organization ACL panel Organization entry

This section is not used in the typical project configuration, although there may be organizations listed in this panel as a result of inherited rights.

# Creating a new user

Users can be added two ways:

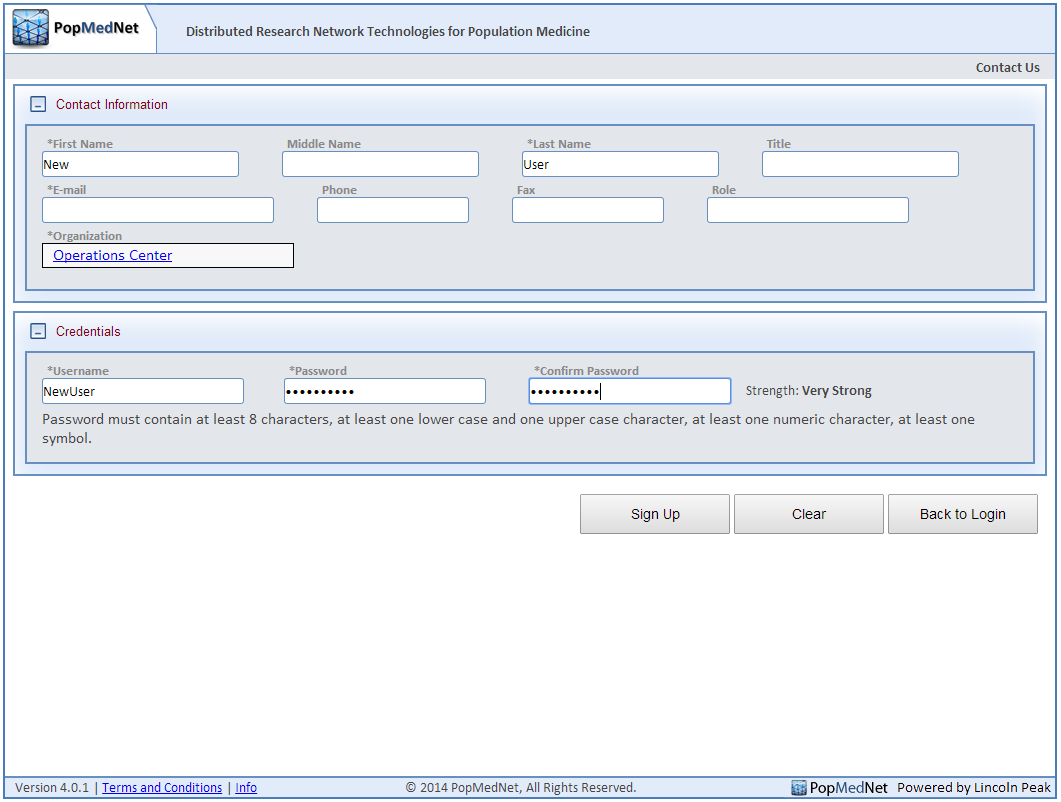
* Manually by an administrator clicking the **Add User** button on the Users panel of the organization page or the Network/Users list.
* Through the new user registration process by clicking the **Register for a new account** link on the logon page.

Once the administrator is on the User Profile page, the process can be completed as described in the following sections.

**Note: It is highly recommended that users go through the new user registration process described next rather than have administrator manually create them to reduce the need for administrators to handle user credentials.**

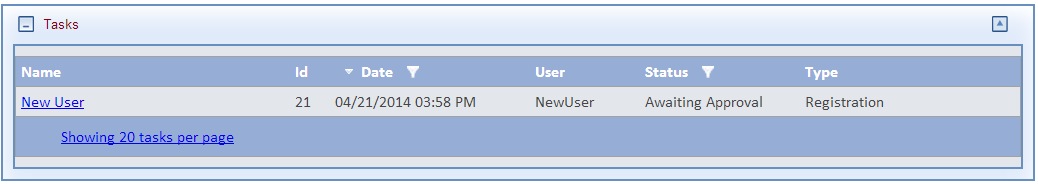
## Create a new user through the registration form

New users can use the self-registration link on the PMN logon page to register themselves.



### New User Registration Task List

The registration request will be displayed in the Task panel on the PMN Home page of any administrator that has rights to approve the user as shown in the following image.



#### Centralized

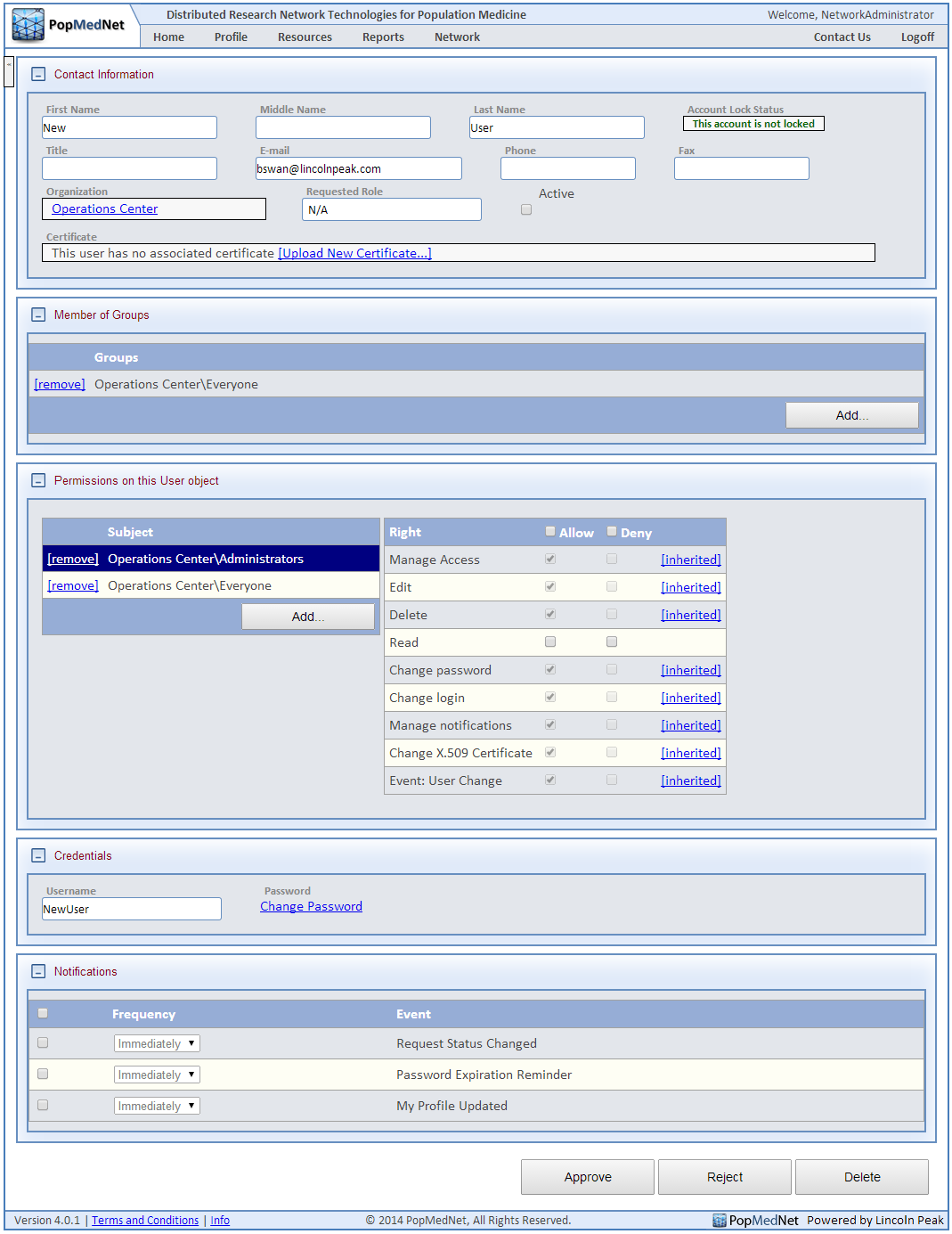
This right is inherited from the Global Access Controls for the System Administrators security group.

#### Decentralized

This right is inherited from the “Organization Template” Administrator security group and is applied to the “TemplateAdministrator”. The Operation Center System Administrators also have the rights to approve users for any organization by default.

### New User Registration Review and Approval

Clicking on the new user registration link will display the user profile page for the user containing the contact information entered by the user in the registration form.



The administrator should validate this user, in particular ensure the organization is correct and what role the user should be assigned.

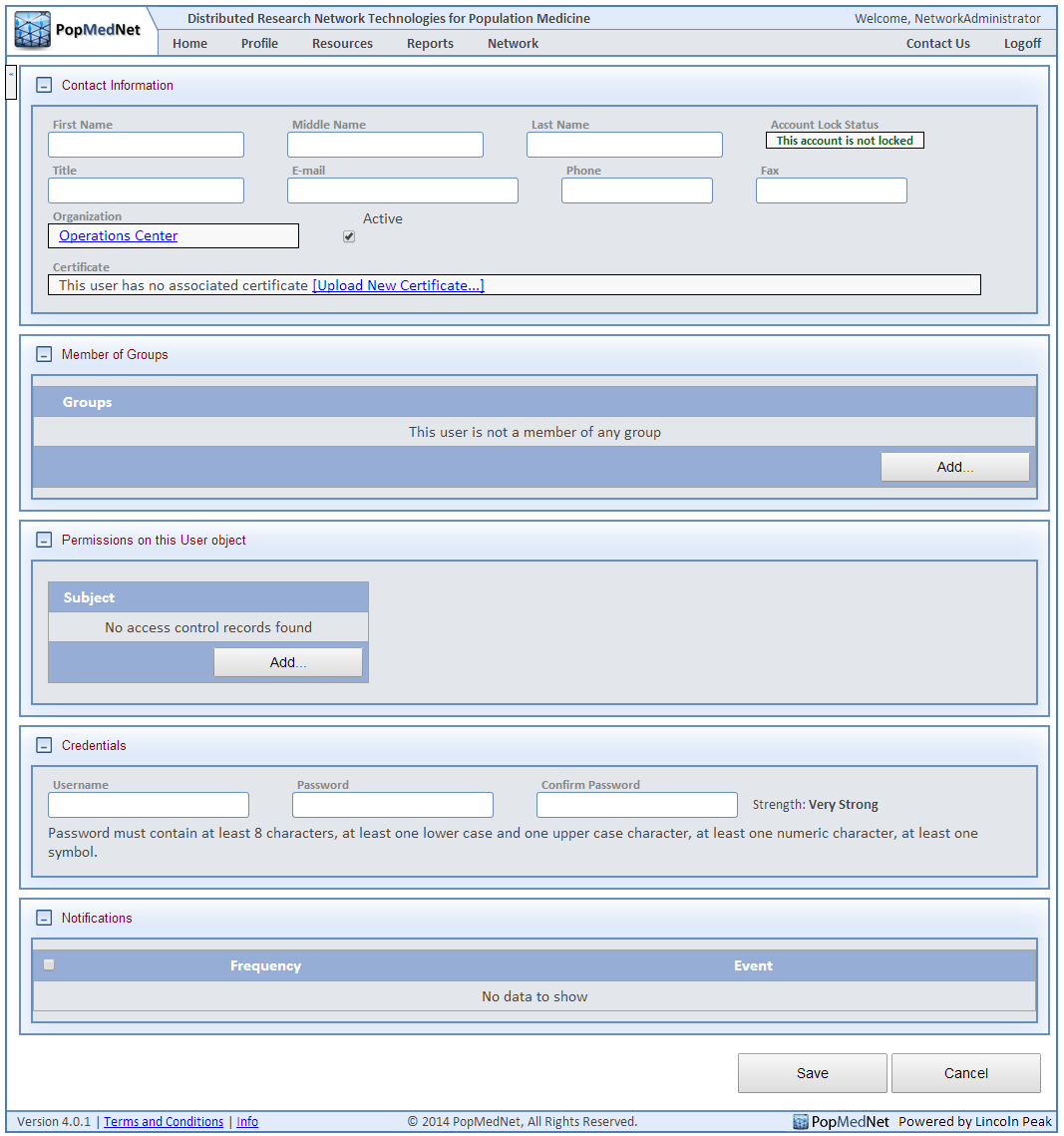
At this point, configuring the user is the same as manually adding a new user. Once this is done, click Approve to finish the registration.

#### Decentralized

As the network grows, this task should be delegated to the administrator within the organization the user selected rather than have system administrator perform this function since the organization administrator should/will have the knowledge necessary to configure the user’s security group membership and finish the approval process.

## Create a new user through the user list page

Administrators can manually add the user to an organization through the Users panel or from the Network/Users list page. This will display the User profile page.

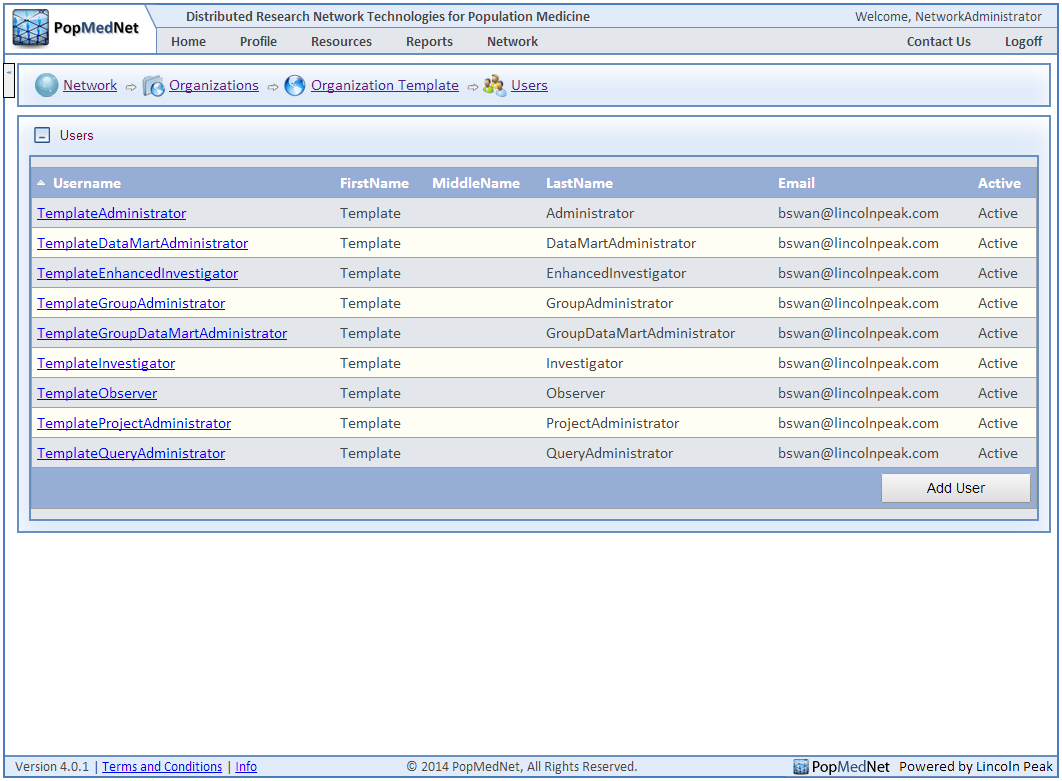


## User Contact Information

If the user was manually added, then the administrator should enter the user contact information. At a minimum, the user’s first name, last name and email address should be entered and the organization selected. Many times the user’s email address domain can be used to validate the user.

## User Member of Groups

The Member of Groups panel is where the user is assigned their role. The organization’s security groups and the security groups of any project the organization participates in will be available to assign to the user. Administrators can use the template users in the “Organization Template” as a guide in configuring security group membership for the user. Additionally, the “Organization Template” has a set of preconfigured users that may be used as a guide by administrators in configuring new users. These users mirror the predefined security groups for an organization. The following figure shows the set of preconfigured users in the decentralized version of the “Organization Template”.



## Permissions on this User Object

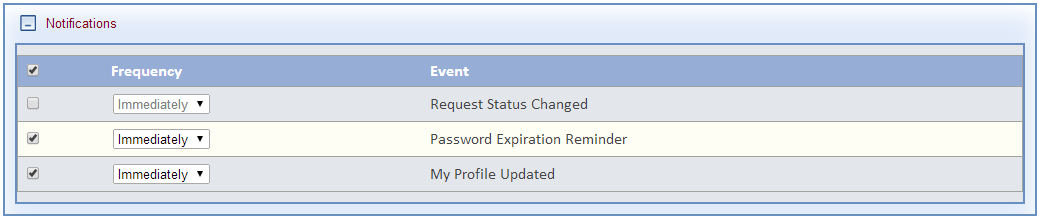
This panel controls which security groups may access and manage this user. These rights are typically inherited from either the Global Access Controls or from the organization access control for the user’s organization.

## User Credentials

If the user was created through the registration process, their credentials will have already been entered, else the administrator will need to enter a set of credentials for the user and communicate this information to the user via an email. Note it is highly recommended that users to use the registration process rather than have administrators enter this information manually.

## User Notifications

The Notification’s panel allows the user to subscribe the notifications generated from events within PMN that are related to their roles. When a user is added to a security group, zero, one, or more notifications options may be visible in the user’s profile. It is recommended that the administrator approving or adding the new user select the following notifications for the user.



After this, users should choose what notifications to subscribe to.

# Issues

The following are a set of issues that need to be addressed prior to releasing this document

## Group Administrators

This document recommends establishing one or more Administrators selected from organizations that are members of the group. Should this be the recommended approach or should be only allow the Operations Center administrators to perform this function?

To account for this issue, sections of the manual were split into centralized vs. decentralized configuration options. Centralized keeps all powers in the hands of the system administrators, decentralized shares powers between system administrators, organization administrators, project administrators, and/or group administrators.

## Creating New Users

This document recommends that organization administrators be granted the rights to create new users within their organization. Should this be the recommended approach or should be only allow the Operations Center administrators to perform this function?

Centralized – only system administrators may create users

Decentralized – organization administrators may create users

## Approving New Users

This document recommends that organization administrators be granted the rights to approve new users within their organization. Should this be the recommended approach or should be only allow the Operations Center administrators to perform this function?

Centralized – only system administrators may approve users

Decentralized – organization administrators may approve users

## Defaulting Project Organization Rights

This document recommended using the organization page to set default rights for any project within the group. Should this be the recommended approach or should we set organization rights explicitly on each project?

Preferred to configure most rights at the project level

## Defaulting Project DataMarts Rights

This document recommended using the DataMart page to set default rights for any project within the group. Should this be the recommended approach or should we set DataMart rights explicitly on each project?

Preferred to configure most rights at the project level.