

Security Policies Plug-In

© 2017 PTC Inc. All Rights Reserved.

Table of Contents

Security Policies Plug-In	1
Table of Contents	2
Overview	3
Installation	4
Accessing the Security Policies Tab	5
Navigating the Security Policies Tab	6
Security Policies	8
Custom Permissions	9
Navigating the Access Categories	12
Dynamic Addressing	13
I/O Tags	14
System Tags	14
Internal Tags	15
Browsing	15
More Options	16
Error Descriptions	17
Custom <access category> access control permissions will not be applied to <object path> because it does not exist.	17
Failed to load client access permissions: Unable to map client access permissions for all user groups.	17
Failed to load client access permissions: User group <name> does not exist.	17
Policy defined for user group <user group name> does not match any existing user group. .	18
Index	19

Security Policies Plug-In

Version 1.013

CONTENTS

Overview

What is the Security Policies Plug-In?

Accessing the Security Policies Tab

How do I access the Security Policies Plug-In's interface?

Security Policies

How do I assign security policies and access permissions with the Security Policies Plug-In?


Error Descriptions

What error messages does this plug-in produce?

Overview

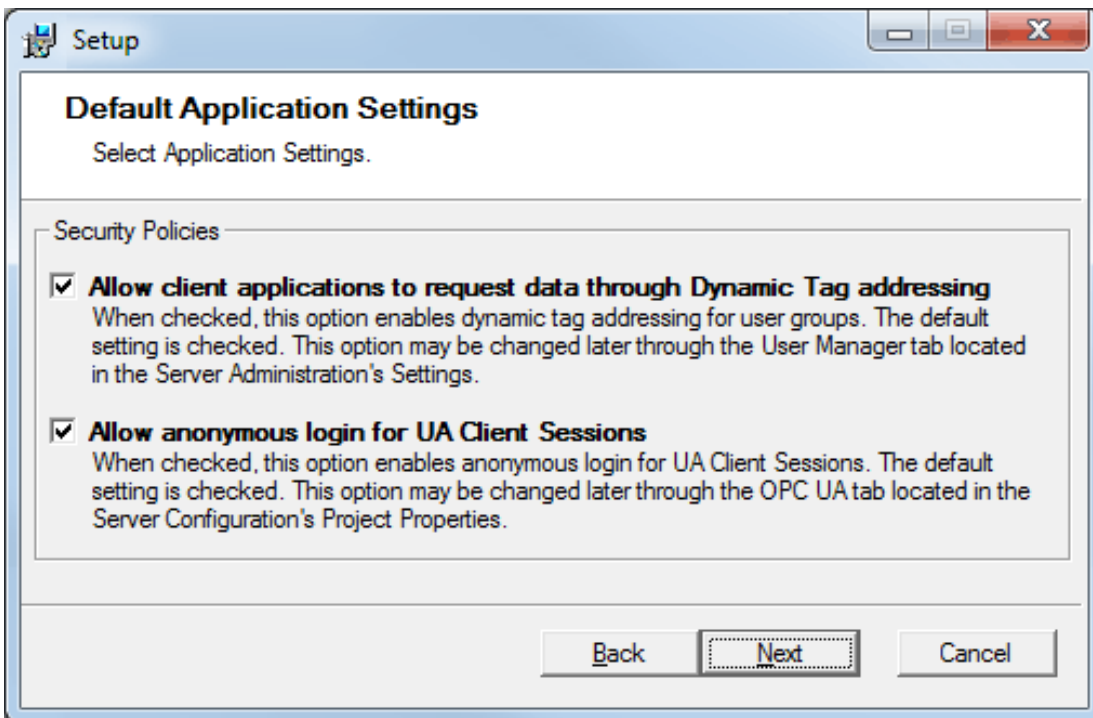
The Security Policies Plug-In allows users to selectively apply security access permissions to individual objects (such as channels, devices, and tags) within a runtime project. It is used in conjunction with the server's User Manager, which specifies global permissions by user group.

To configure access permissions at the object level, the user must belong to a user group that has been allowed access in a given category. Users can apply different access permissions to objects within the same project. Changes made to the access permissions will be applied dynamically as they occur, and do not require the Runtime to restart or reinitialize.

 **Caution:** Once security permissions have been applied in the Security Policies tab, the project can only be saved as a .opf file: it cannot be saved as a .xml file. Furthermore, a project that contains security permissions will not be able to load into the Server Runtime or Server Configuration unless the Security Policies Plug-In is present.

Installation

This dialog is presented during server installation, and is used to select the Default Application Settings for the Security Policies Plug-In.



Descriptions of the options are as follows:

- **Allow client applications to request data through Dynamic Tag addressing:** When checked, this option enables dynamic tag addressing for user groups. The default setting is checked. This option may be changed later through the User Manager tab located in the Server Administration's Settings.
- **Allow anonymous login for UA Client Sessions:** When checked, this option enables anonymous login for UA Client Sessions. The default setting is checked. This option may be changed later through the OPC UA tab located in the Server Configuration's Project Properties.

● **Note:** Anonymous users include OPC .NET or OPC DA clients that are not required to authenticate directly with the server. Authenticated users are required to authenticate directly with the server by supplying a verified user name and password.

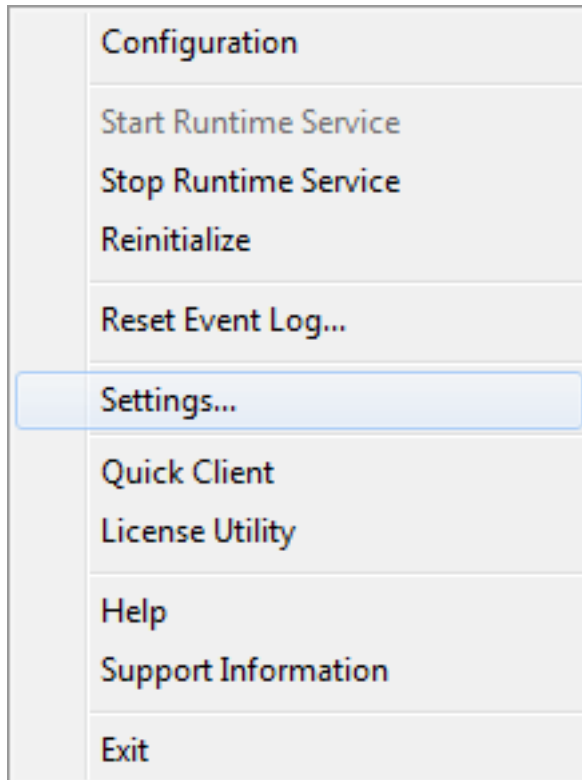
● *For more information on both the User Manager and Project Properties, refer to the server help file.*

Accessing the Security Policies Tab

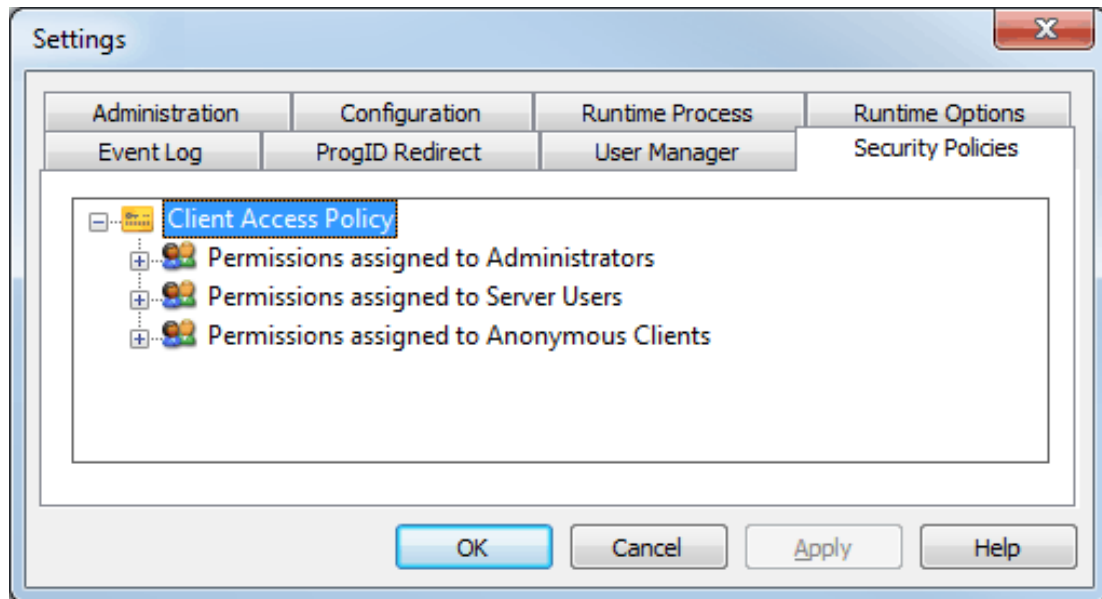
The Security Policies Plug-In is configured through the server's Administration Settings dialog.

● **Note:** The server Runtime must be running in order to define access permissions. If it is not, the Client Access Policy tree and associated branches will not be displayed. Once a Runtime connection has been established, any existing Server Configuration client connections will be demoted to Read Only access until the Security Policies tab is closed. This allows the Server Administration exclusive access to the Runtime project.

1. To start, right-click on the **Administration** icon located in the **System Tray**. Then, select **Settings**.



2. Next, select the **Security Policies** tab.





● **Note:** The image above displays the default user groups that are present in all projects and managed through the User Manager. For more information, refer to the "Settings - User Manager" in the server help file.

Navigating the Security Policies Tab

Icons

The Security Policies tab displays icons to make it easier for users to determine whether a category has access permissions available.

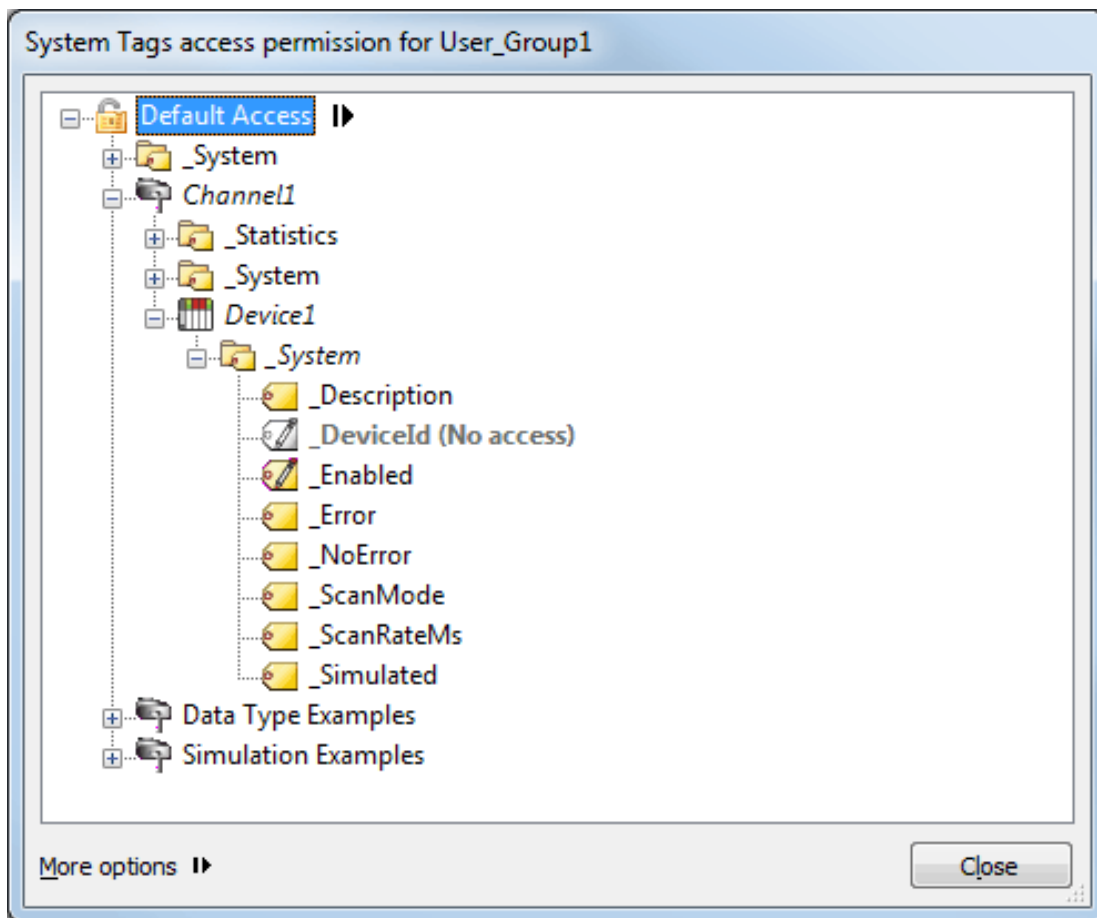
-  The lock icon indicates that the category has been disabled at the user group level. When locked, users cannot define per-object client access permissions in the category.
-  The double-key icon indicates that the category is enabled at the user group level. When unlocked, users can define per-object client access permissions in the category.

● **Note:** User group access is specified through the User Manager tab. For more information, refer to "Settings - User Manager" in the server help file.

Font Styling

The Security Policies Plug-In also uses variations in font styling to make it easier for users to locate previous changes made to an object's access permissions. The styling will persist after the changes have been applied and the dialog has been closed.

- **Regular Text:** This style indicates that no custom access permissions have been assigned in any category for any user group.
- **Bold Text:** This style indicates that a custom access permission has been assigned in a category for a user group. It will be displayed for both the user group and access category.
- **Italic:** This style indicates that per-object custom access permissions have been assigned within a branch in a category. It will only be displayed in the access category's permissions dialog.

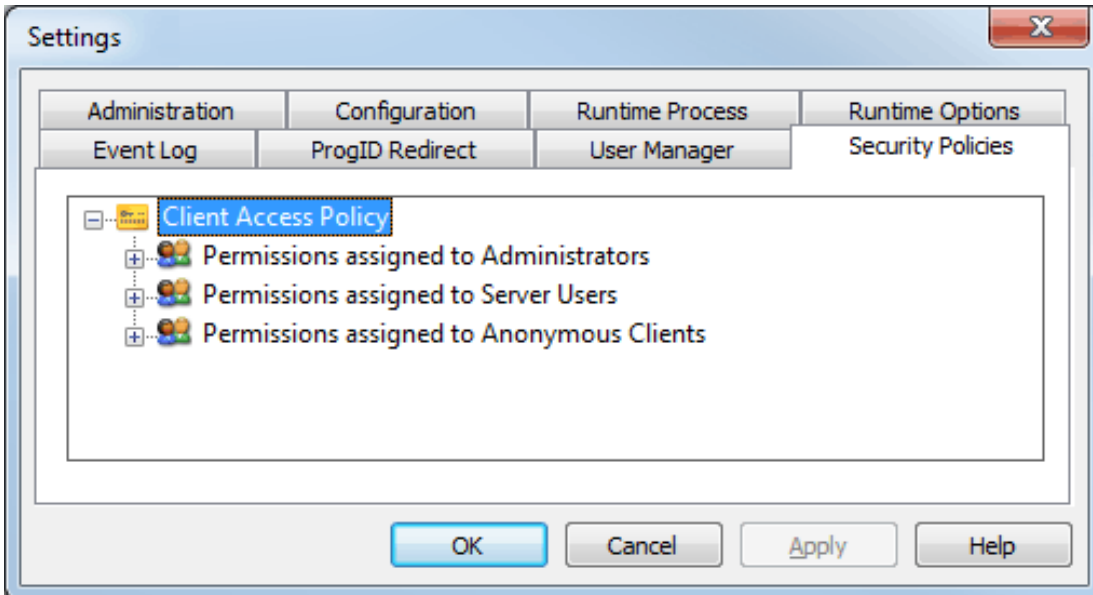


● **Note:** A gray font color indicates an object has been disabled.

Security Policies

The Security Policies dialog separates permissions by user group, and organizes the user groups beneath a central heading called "Client Access Policy."

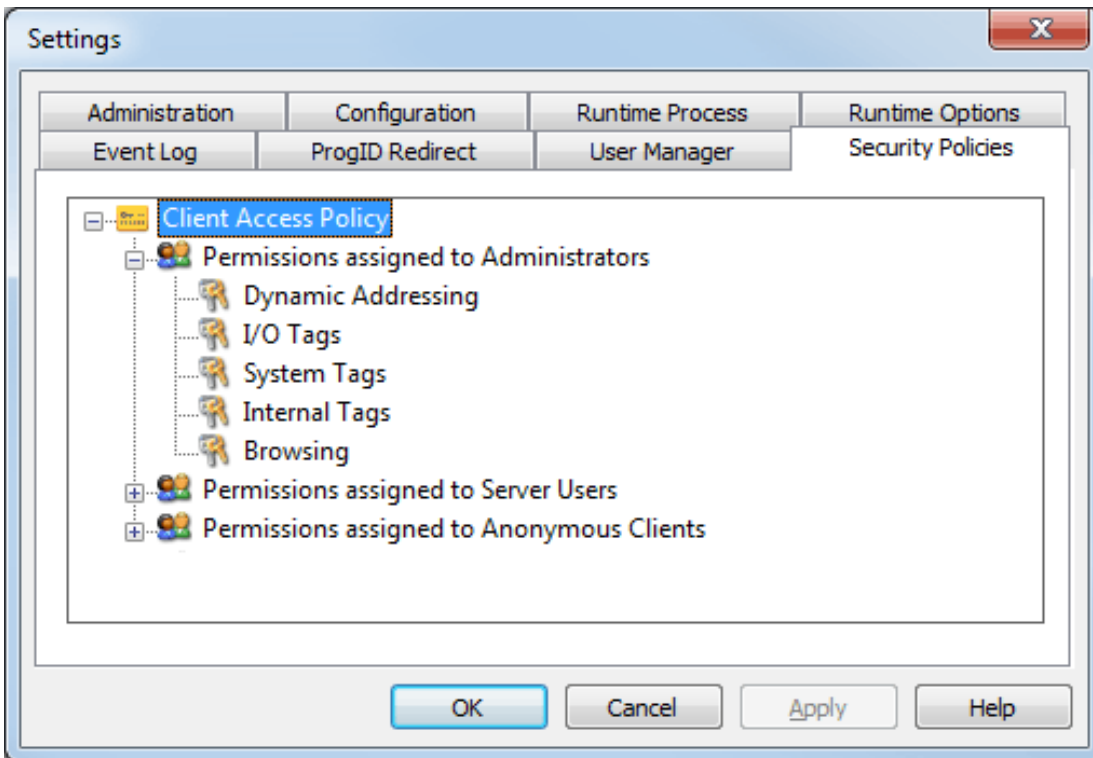
● **Note:** A "Permissions assigned to" branch will be displayed for all user groups that have been defined in the User Manager. After custom user groups have been defined, users must press **Apply** in order for the changes to be reflected in the Security Policies tab.



● **Important:** User groups and their associated permissions are stored in a User Information file. It is recommended that users backup the default User Information file through the export functionality available in the User Manager. For more information, refer to "Settings - User Manager" in the server help file.

Displaying a User Group's Access Categories

To view a user group's access categories, either double-click or expand its associated plus sign. There are five access categories: Dynamic Addressing, I/O Tags, System Tags, Internal Tags, and Browsing.



Descriptions of the access categories are as follows:

- **Dynamic Addressing:** This category specifies permissions for an object's dynamic addressing.
- **I/O Tags:** This category specifies permissions for an object's device-level I/O Tag data.
- **System Tags:** This category specifies permissions for an object's System Tags.
- **Internal Tags:** This category specifies permissions for an object's Internal Tags.
- **Browsing:** This category specifies permissions for an object's browse access to the project namespace.

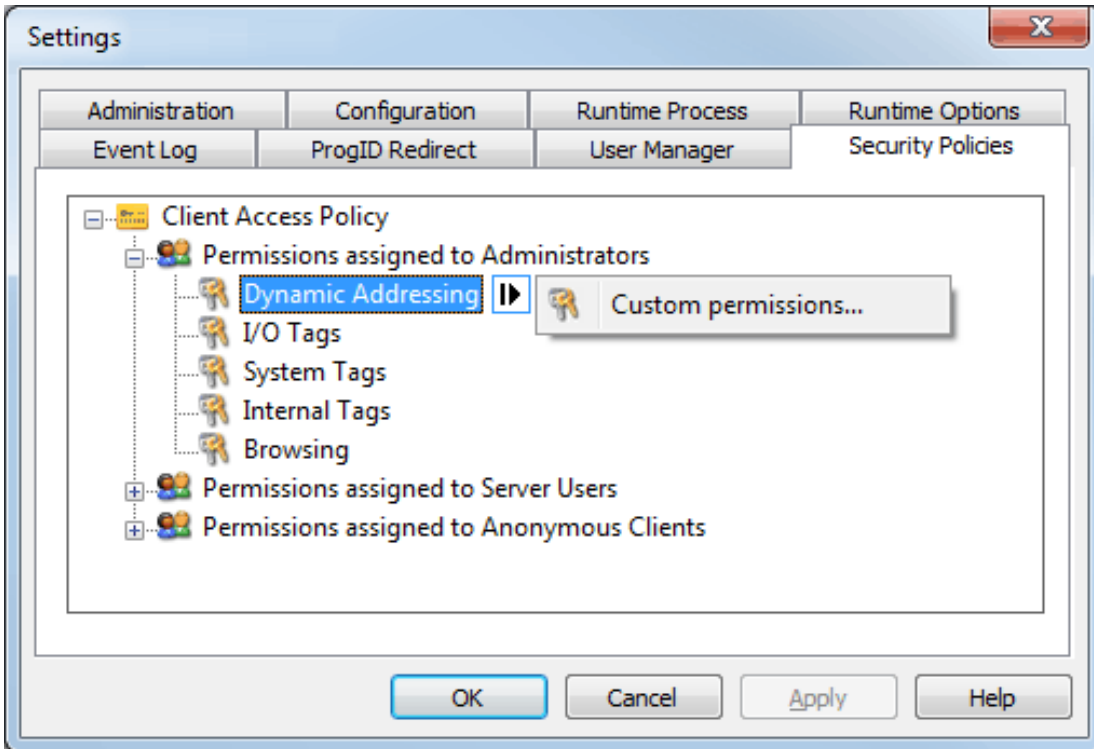
• **See Also:** [Navigating the Access Categories](#)

Custom Permissions

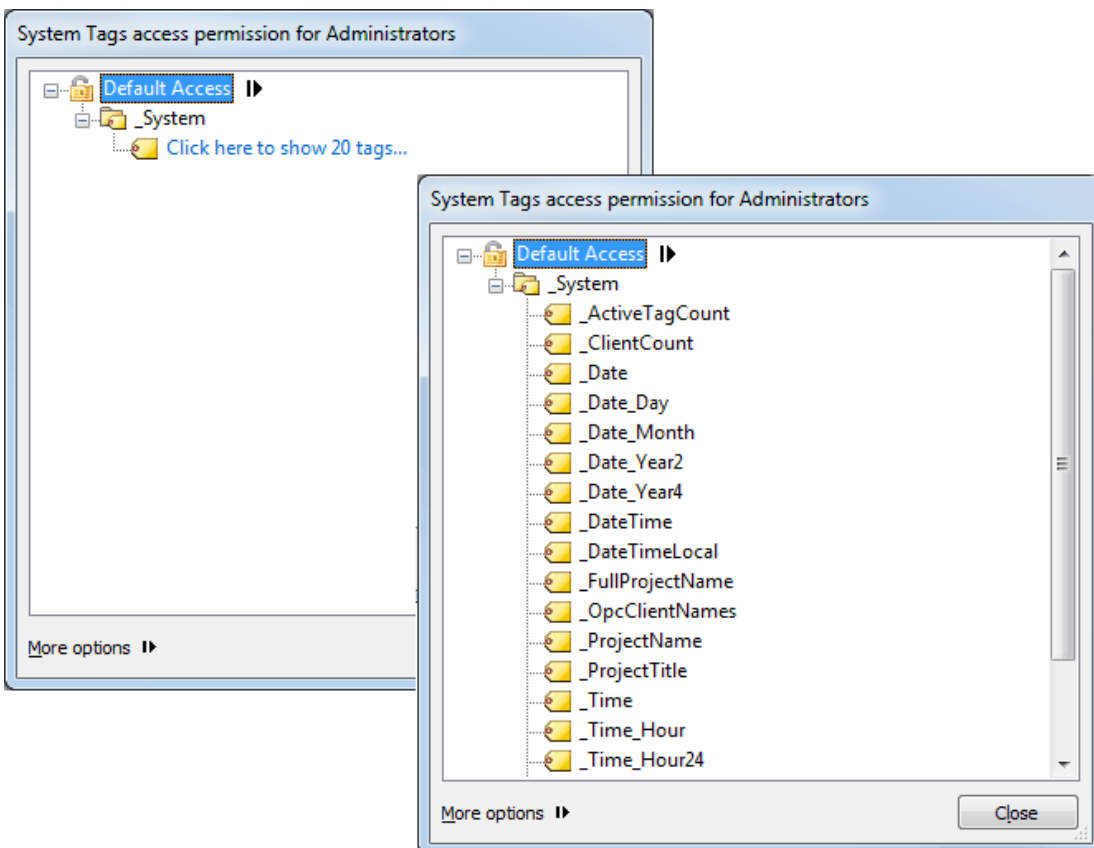
Applying Custom Permissions

Users can assign custom permissions to objects within an access category. To do so, first select it. Then, click the actuator and select **Custom permissions**.

• **Caution:** Permissions that have been configured in the Security Policies tab become part of the project file when the project is saved. Because permissions relate to user groups, the user groups that are in place when a secure project is opened should match those that were in place when security was configured; otherwise, a message will be displayed providing more information.



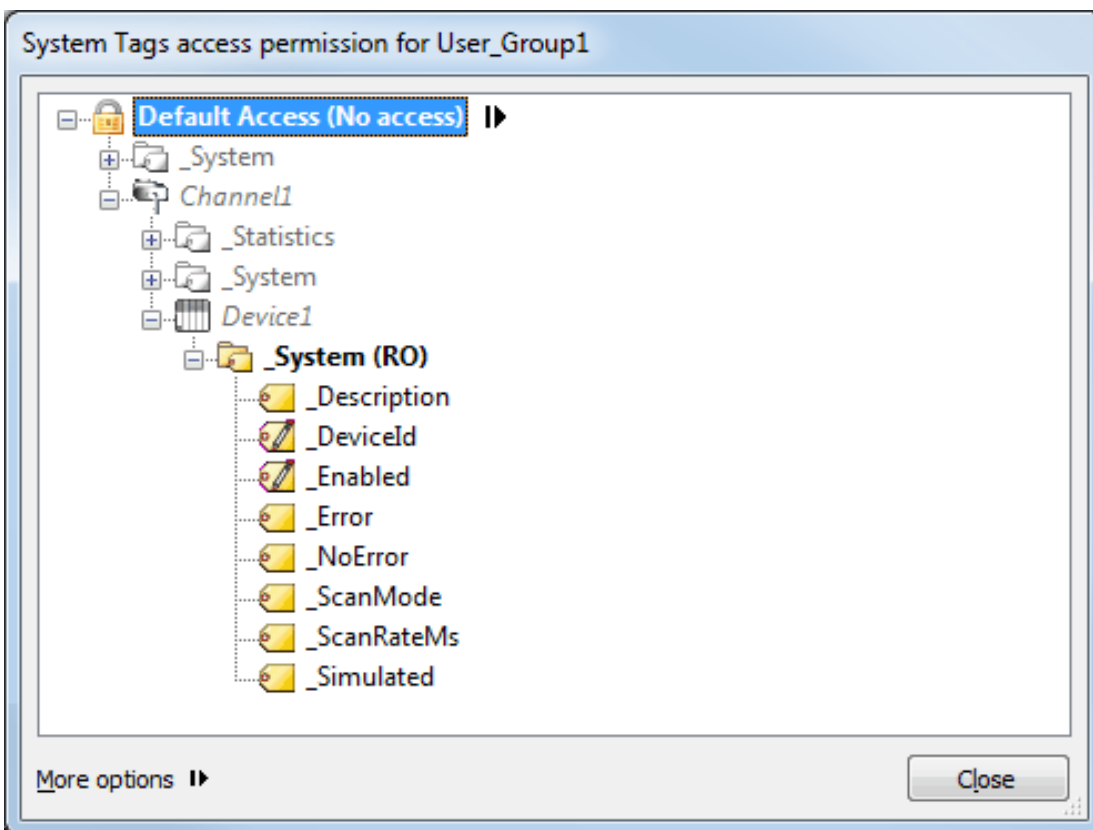
The access permission dialogs depend on the category that is selected. To accommodate projects of different size, the dialog is formatted into a browse tree. Users can locate and set permissions for lower-level objects by expanding the branches. Folders that contain tags will display a message that indicates the number of tags so that users may decide whether to expand it.



The permissions that are available depend on the object selected. Descriptions of the options are as follows:

- **Allow:** This allows Dynamic Addressing or browsing.
- **Deny:** This denies Dynamic Addressing or browsing.
- **No access:** This denies read and write access.
- **Read only:** This allows read access but denies write access.
- **Read/write:** This allows read access and write access.

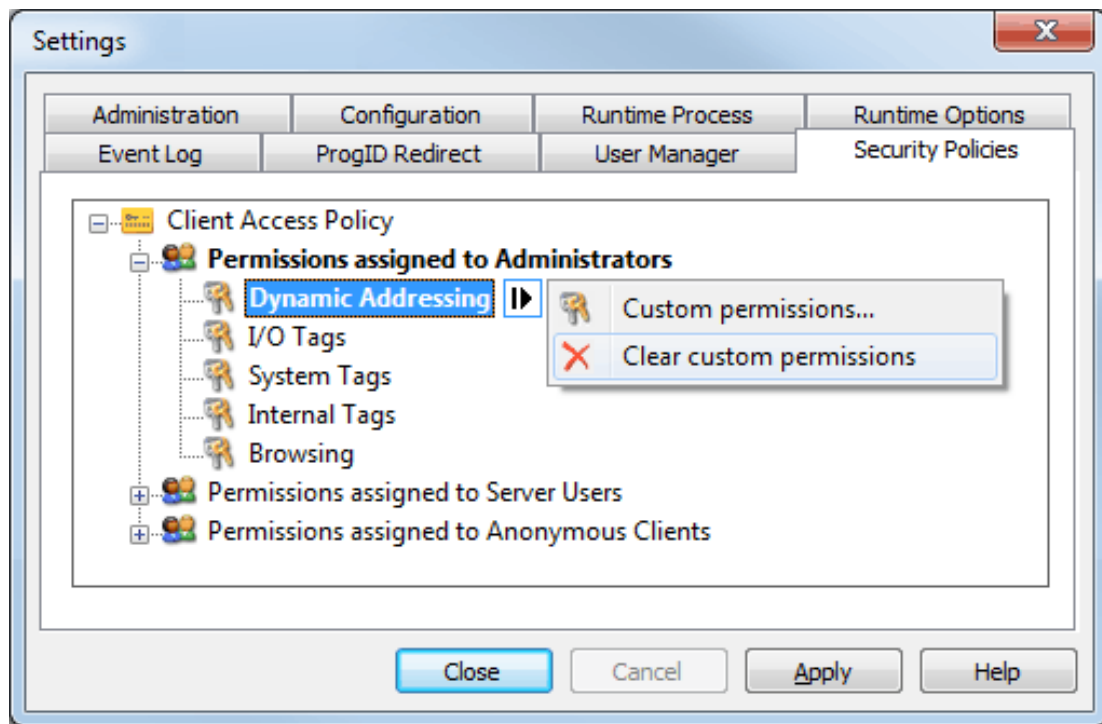
● **Note:** Access can be granted to individual branches or objects that have been denied for user groups through the Security Policies Plug-In. Any overridden permission will be indicated by bold styled text. Parts of the tree that are disabled or denied will be indicated by grey text. For more information, refer to [Navigating the Security Policies Tab](#).



Removing Custom Permissions

Font styling will persist until the custom permissions are removed.

- To remove all custom permissions assigned to a user group, select the user group. Then, click the actuator and select **Clear custom permissions**.
- To remove all custom permissions assigned to an access category, select the access category. Then, click the actuator and select **Clear custom permissions**.





● **Note:** Once custom permissions have been removed, the font styling will be regular.

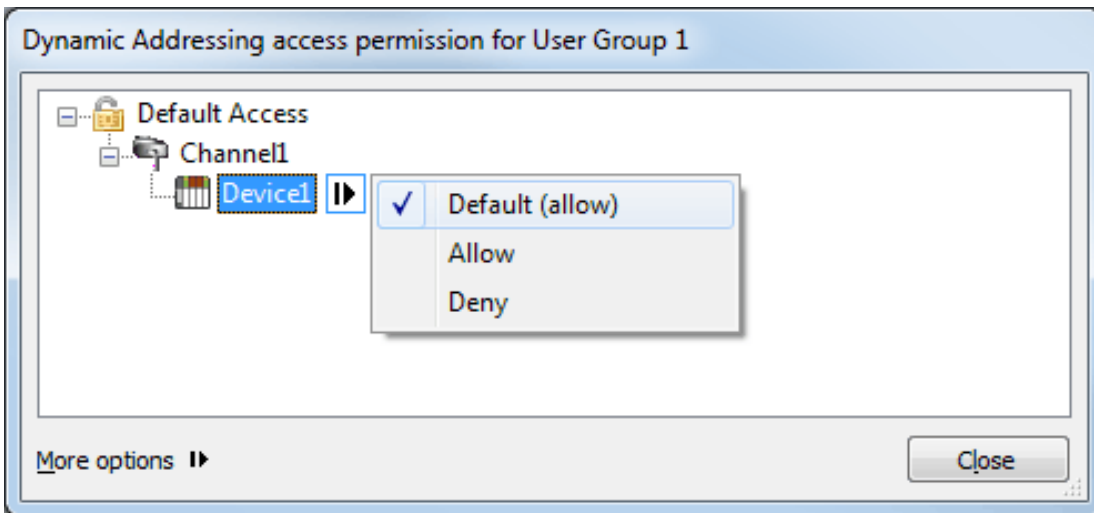
● **See Also:** [More Options](#)

Navigating the Access Categories

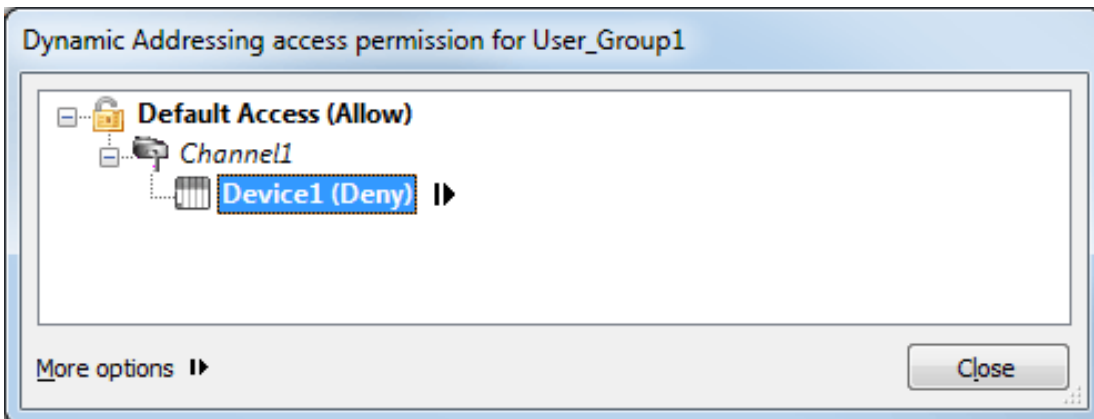
In the access categories' permission dialogs, users can assign permissions at the top level or to individual objects. To do so, right-click on the object and then select **Allow** or **Deny**. The Default option will display the permissions inherited from the user group.

● **Note:** The access permission dialogs' Default Access branch will display an icon to allow users to quickly determine its inherited permission.

-  The unlocked lock indicates that the permission is set to Allow.
-  The locked lock indicates that the permission is set to Deny.



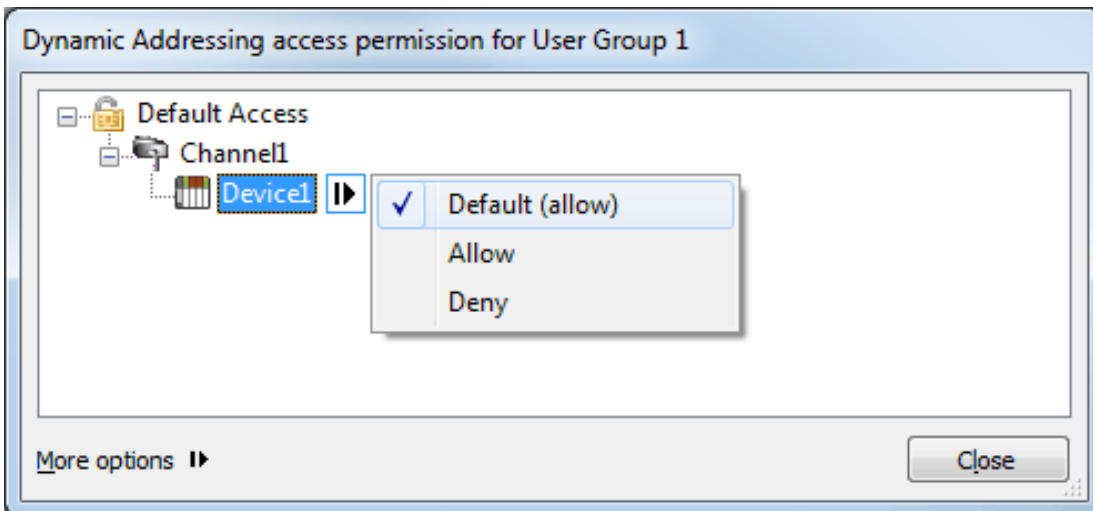
● **Note:** The text displayed in parentheses indicates the default condition inherited from the user group. The text will be bold when an object's default permission is overridden.



● **Note:** In the example above, Default Access indicates "Allow" in order to display the permission that would have been inherited if not overridden.

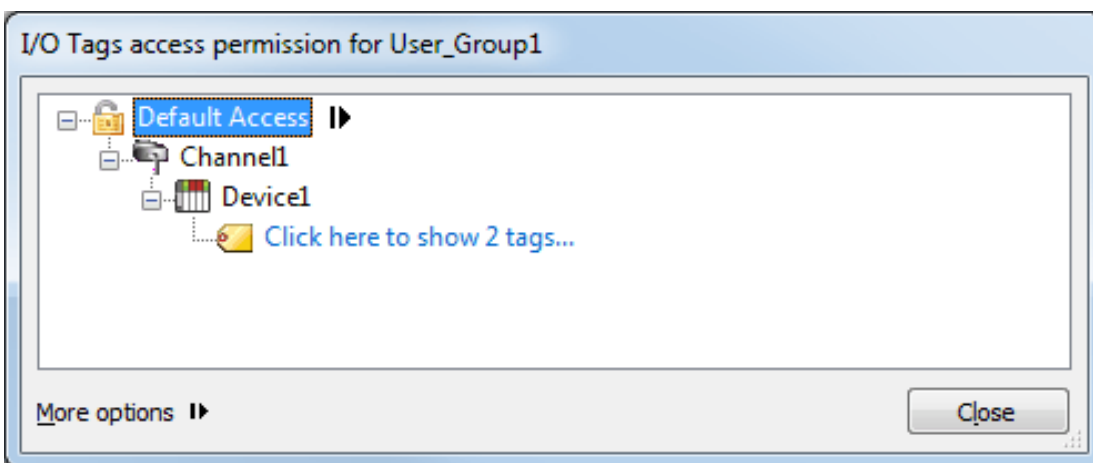
Dynamic Addressing

Dynamic Addressing must be enabled at the user group level in order for it to be available for permissions through the Security Policies Plug-In. For information on specifying permissions during server installation, refer to [Installation](#).



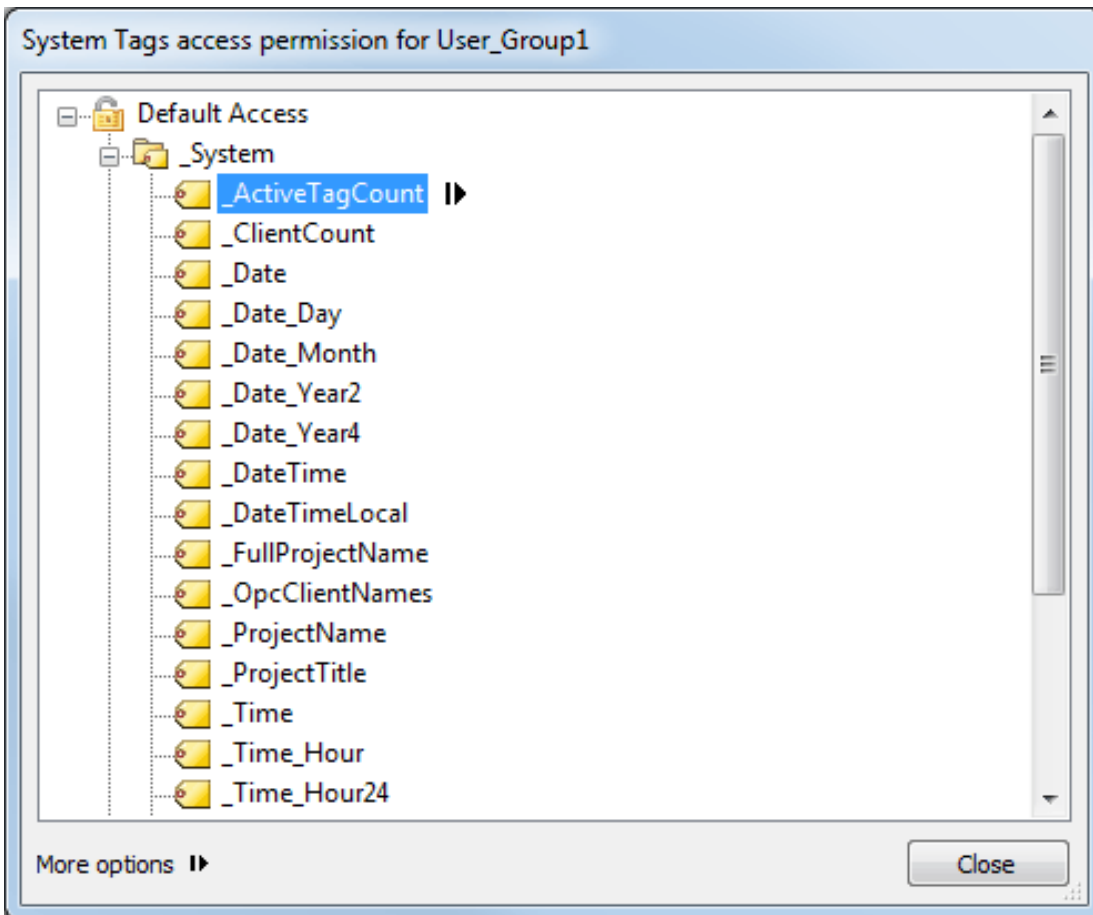
I/O Tags

The I/O Tags access category's browser displays and provides access to branches from the channel level to the device level that do not lead to System Tags or Internal Tags. It will only display channels, devices, user-defined tag groups, and Static Tags. For more information on its access permissions, refer to [Custom Permissions](#).



System Tags

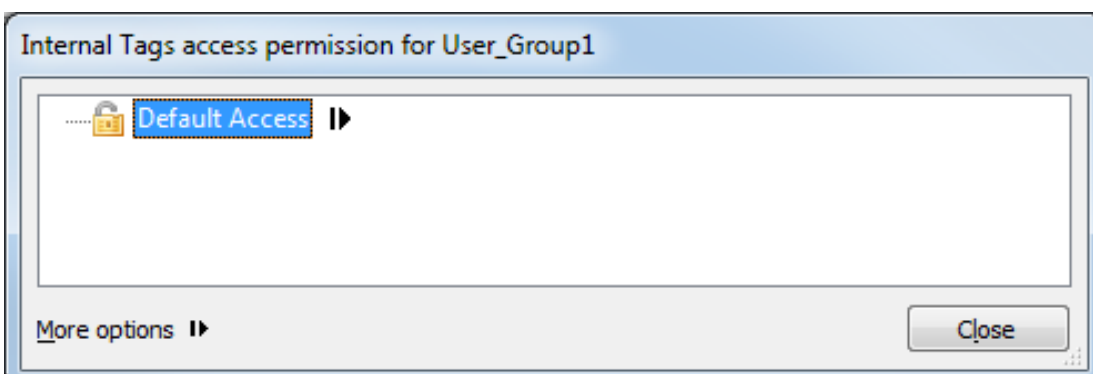
The System Tags access category's browser displays and provides access to branches of the project namespace that lead to one or more System Tags. For more information on its access permissions, refer to [Custom Permissions](#).



Internal Tags

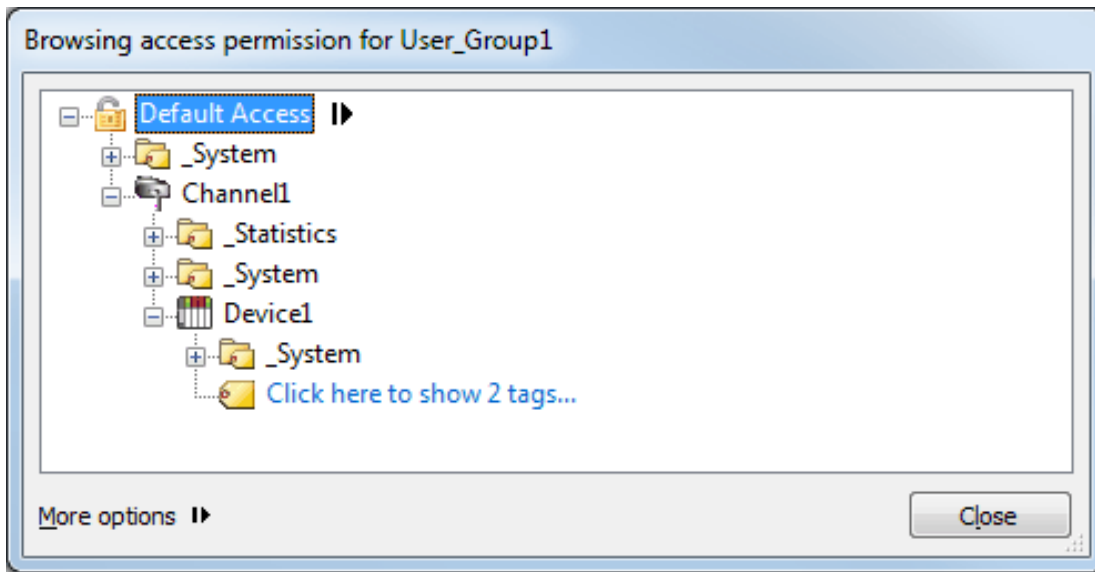
The Internal Tags access category's browser displays and provides access to branches of the project namespace that lead to one or more Internal Tags. For more information on its access permissions, refer to [Custom Permissions](#).

Note: Whether Internal Tags are displayed in the browse tree will depend on the device.



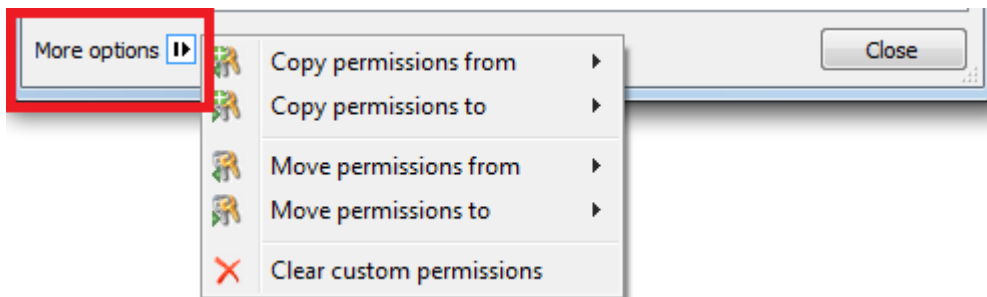
Browsing

The Browsing access category displays and provides access to the entire project namespace.



More Options

Each access category contains additional settings. To access those settings, locate **More Options** at the bottom of the dialog and then select the actuator.



Descriptions of the options are as follows:

- **Copy permissions from:** This option displays a list of user groups from which users can choose. Once selected, the permissions assigned to that user group for the current access category will be copied to the browse tree.
- **Copy permissions to:** This option displays a list of user groups from which users can choose. Once selected, the permissions shown in the browse tree will be copied and assigned to that group.
- **Move permissions from:** This option displays a list of user groups from which users can choose. Once selected, the permissions assigned to that user group for the current access category will be copied to the browse tree and then cleared from the source user group.
- **Move permissions to:** This option displays a list of user groups from which users can choose. Once selected, the permissions shown in the browse tree will be copied, assigned to that user group, and removed from the browse tree.
- **Clear custom permissions:** This option removes all custom permissions from the access category. This option is only available when custom permissions have been assigned.

Error Descriptions

The following error/warning messages may be generated. Click on the link for a description of the message.

[Custom <access category> access control permissions will not be applied to <object path> because it does not exist.](#)

[Failed to load client access permissions: Unable to map client access permissions for all user groups.](#)

[Failed to load client access permissions: User group <name> does not exist.](#)

[Policy defined for user group <user group name> does not match any existing user group.](#)

Custom <access category> access control permissions will not be applied to <object path> because it does not exist.

Error Type:

Warning

Possible Cause:

An attempt was made to apply access permissions to an object that does not exist in the project.

Solution:

1. Add the missing object and then re-attempt to load the client access permissions.
2. Re-assign the access permissions to an object that exists in the project.

Failed to load client access permissions: Unable to map client access permissions for all user groups.

Error Type:

Error

Possible Cause:

An attempt was made to load access permissions for user groups, but the information got merged by duplication.

Solution:

Re-attempt to load the client access permissions.

Failed to load client access permissions: User group <name> does not exist.

Error Type:

Error

Possible Cause:

Access permissions were defined for a group that does not exist in the project.

Solution:

Add the missing user group to the User Manager tab located in the server's Administration Settings dialog. Then, re-attempt to load the client access permissions.

Policy defined for user group <user group name> does not match any existing user group.

Error Type:

Error

Possible Cause:

The user group information that was present at the time the project was configured does not match what is defined in the User Manager.

Solution:

1. Add the specified group to the User Manager.
2. Open the Security Policies tab and delete the permissions assigned to the specified group.

Index

A

- Accessing the Security Policies Tab 5
- Administration 5
- Allow 11
- Allow anonymous login for UA Client Sessions 4

B

- Browsing 15

C

- Clear custom permissions 16
- Client Access Policy 8
- Copy permissions 16
- Custom <access category> access control permissions will not be applied to <object path> because it does not exist. 17
- Custom Permissions 9

D

- Default Access 12
- Default Application Settings 4
- Deny 11
- double-key 6
- Dynamic Addressing 13

E

- Error Descriptions 17

F

- Failed to load client access permissions: Unable to map client access permissions for all user groups. 17

Failed to load client access permissions: User group <name> does not exist. 17

G

group <name> does not exist 17

H

Help Contents 3

I

I/O Tags 14

Installation 4

Internal Tags 15

L

lock 6, 12

M

merged by duplication 17

missing user group 18

Move permissions 16

N

Navigating the Access Categories 12

Navigating the Security Policies Tab 6

No access 11

O

object that does not exist 17

Options 16

Overview 3

P

Policy defined for user group <user group name> does not match any existing user group. 18

R

Read only 11

Read/write 11

Removing Custom Permissions 11

S

Security Policies 8

Static Tags 14

System Tags 14

U

Unable to map client access 17

unlock 12

user-defined tag groups 14

User Manager 6