



# Gemini Permissions Quick Guide

Product Release 3.6

© 2009 CounterSoft Limited. All rights reserved.

## Scenario 1 – Using Global Groups

Global Groups will be used to group related users and their permissions. For example:

- Issue Workers: this group will contain people who work on issues.
- Issue Administrators: this group will contain people who control all aspects of an issue.
- Project Administrators: this group will contain people who can administer projects (the highest permission possible at the project level).

By using Global Groups you define group membership globally – group membership does not vary by project (it is the same for all projects).

The following table defines the steps required to configure security using Global Groups whereby user group membership is controlled by Gemini Administrators.

Step	Comments
<b>1 <u>Create Global Groups</u></b> <i>Administration → Security Settings → <b>Global Groups</b></i>	Group membership controlled globally by Gemini Administrators. Consider creating recognisable groups organised by functional area: <ul style="list-style-type: none"> <li>• Project Administrators, Managers, Developers, Testers, Customers</li> </ul>
<b>2 <u>Create Users</u></b> <i>Administration → Security Settings → <b>Users</b></i>	Add your users to Gemini.
<b>2 <u>Assign Users to Global Groups</u></b> <i>Administration → Security Settings → <b>Global Groups</b></i>	Add users to Global Groups (define group membership).  Edit each Global Group and select the members for that group. Each user can be assigned can belong to more than one group.  For your organization you should already be aware of which users belong to each group.
<b>At this point you should have defined Groups, Users, and assigned group membership.</b>	
<b>3 <u>Create Security Schemes</u></b> <i>Administration → Security Settings → <b>Schemes</b></i>	Security Schemes allow to define user permissions and then apply them to multiple projects.  Start by creating a single security scheme.  Determine how many Security Schemes are required before you start this project. If you need to define different permissions per project, then you may wish to either create multiple schemes or follow Scenario 2.
<b>4 <u>Assign Users &amp; Global Groups to Security Schemes</u></b> <i>Administration → Security Settings → <b>Schemes</b></i>	Edit Security Scheme and select which users/groups can perform what role.  You can type in user names into the “User” dropdown box and Gemini will automatically find matching users for you.  You should ideally be assigned Groups to permissions to simplify on-going administration, but you can still assign individual users.
<b>5 <u>Apply Security Schemes to Projects</u></b> <i>Administration → Projects → <b>Project</b></i>	Each project is assigned a Security Scheme.  Edit a Project and assign Security Scheme to a Project.

## Scenario 2 – Using Project Groups

Project Groups allows administrators to vary group membership. Project Groups enable are very useful when you have one or two Security Schemes and you want to vary who can do what per project. For example:

- Bob & Sarah are part of Developers group for Project X.
- Sarah & Tim are part of Developers group for Project Y.

As you can see from the above example, the membership of the Developers group is different for each project.

The following table defines the steps required to configure security using Project Groups whereby user group membership is controlled by Gemini Administrators and Project Administrators.

Step	Comments
<b>1 <u>Create Project Groups</u></b> <i>Administration → Security Settings → <b>Project Groups</b></i>	Group membership varies per project. Consider creating recognisable groups organised by functional area: <ul style="list-style-type: none"> <li>• Project Administrators, Managers, Developers, Testers, Customers</li> </ul>
<b>2 <u>Create Users</u></b> <i>Administration → Security Settings → <b>Users</b></i>	Add your users to Gemini.
<b>2 <u>Assign Users to Project Groups</u></b>	<i>Administration → Security Settings → <b>Project Groups</b></i> Edit each Project Group and select the members for that group for each project. The key thing to understand is that you select a Project first (dropdown) and then decide who is part of that group for the selected project.  <i>[Project Home Page] → Project Administration → <b>Project Groups</b></i> You can also go to each Project and define who is belongs to each Project Group for that project.
<b><i>At this point you should have defined Groups, Users, and assigned group membership.</i></b>	
<b>3 <u>Create Security Schemes</u></b> <i>Administration → Security Settings → <b>Schemes</b></i>	Security Schemes allow to define user permissions and then apply them to multiple projects.  Start by creating a single security scheme.  Determine how many Security Schemes are required before you start this project. If you need to define different permissions per project, then you may wish to either create multiple schemes or follow Scenario 2.
<b>4 <u>Assign Users &amp; Project Groups to Security Schemes</u></b> <i>Administration → Security Settings → <b>Schemes</b></i>	Edit Security Scheme and select which users/groups can perform what role.  You can type in user names into the “User” dropdown box and Gemini will automatically find matching users for you.  You should ideally be assigned Groups to permissions to simplify on-going administration, but you can still assign individual users.
<b>5 <u>Apply Security Schemes to Projects</u></b> <i>Administration → Projects → <b>Project</b></i>	Each project is assigned a Security Scheme.  Edit a Project and assign Security Scheme to a Project.

## Common Issue Field Visibility Related Configuration Steps

Decide, who can see which issue field and when (e.g. “Developers” can see “Affected Versions” field when looking at “Bugs”).

1	<b><u>Create Issue Field Visibility Schemes</u></b>  <i>Administration → Issue Settings → <b>Field Visibility Schemes</b></i>	Issue Field Visibility Schemes determine who sees which issue field. Each issue field can be enabled or disabled.  Groups can be assigned to determine which users can see the issue field.  Issue Field Visibility Schemes are applied to Issue Types. Therefore, you can decide which issue fields are available for Bugs, Change Requests, Enhancements, etc.  Just remember to perform Step 3 below – Define Project Default Values!
2	<b><u>Apply Issue Field Visibility Schemes to Issue Types</u></b>  <i>Administration → Issue Settings → <b>Issue Type</b></i>	Issue Field Visibility Schemes are applied to Issue Types. Therefore, you can decide which issue fields are available for Bugs, Change Requests, Enhancements, etc.  You are advised to map out:  <ol style="list-style-type: none"><li>1. What issue fields are applicable to each Issue Type;</li><li>2. Who can see which issue field (e.g. only Managers can amend the “Reported By” field).</li></ol>
3	<b><u>Define Project Default Values</u></b>  <i>[Project Home Page] → Project Administration → <b>Default Values</b></i>	Each project can be assigned Default Values for issue fields (e.g. Components). This is essential where Issue Field Visibility schemes are applied as certain issue fields may not be visible to users. In such scenarios the default values will be used when creating and editing issues.
4	<b><u>Set Issues List Field Visibility</u></b>  <i>Administration → Projects → <b>Project</b></i>	You can also control what issue fields are displayed on the Issues list page (Issues.aspx). Simply apply an Issue Field Visibility Scheme to each project. Edit a Project and assign a default Field Visibility Scheme that affects Issues List.

## Common Global Security Options

1	<b><u>Set Global Administration Options</u></b> <i>Administration → Security Settings → <b>General</b></i>	There are several global options that also affect user security:  <i>Administration → Security Settings → General → Allow User Registrations</i> <i>Administration → Security Settings → General → Allow Anonymous Users</i> <i>Administration → Security Settings → General → Show All Projects</i> <i>Administration → Security Settings → General → Show Gemini Statistics</i> <i>Administration → Security Settings → General → Portal Mode User Group</i>
2	<b><u>Portal Mode Setup</u></b> <i>Administration → Security Settings → <b>General</b></i>	Users in a specified Global Group can be marked as being Portal Mode users. Any users in this group will only issue their own issues and are directed straight to the Issues list post-login.  Such users can only see a single project.