



Understanding Permissions

BlueStep™ Permission Structure

One of the important features of BlueStep™ products is the unequalled caliber of security that can be applied to the system in flexible ways. At virtually every level of Connect™, Relate™, Team™ and HQ™, the administrator has the option of restricting or allowing use of data or any functions/features at multiple points. Anything from a single field to the entire system may be included or excluded for entire groups or individual users. By selecting the Permissions tab

Permissions

on any screen where it appears, you can access five levels of permission:

- **No Access** – no admission of any sort to the item
- **Reader** – permission to view contents only
- **Participant** – permission to respond to content
- **Author** – permission to create and add content, plus edit data in their own creations
- **Editor** – full permission to add, edit and delete content in any way

As administrator, you make the decision as to what permission level to allow any groups or individual users. Since all BlueStep™ products are hierarchical, decisions by those administrators at the top of the organization flow down to other levels. However, other supervisors and team leads have additional limited authority to allow or disallow permissions for those on their own level, their own team or subgroups under their leadership, without overriding the decisions made by top management.

Associated with permissions is the concept of explicit, implicit and "flow down". In the hierarchical structure, if permissions are expressly or **explicitly** set on any object, those permissions will flow down to objects below them in the structure. The objects below would then have implied or **implicit** permissions from the parent container.

If you move an object from one position to another, it will retain the permissions assigned to it in its old location *if* the permissions on that container were explicit. If they were inherited or implicit, the moved object will inherit the new permissions of the unit to which they have been moved.

There are two guidelines for good security management. The first is to establish security as high as practicable in the organization structure and let it flow down from there. The second is to create groups that will assign security levels to large numbers of users. It is by far easier to add users to groups and thereby allow them access to resources than it is to individually assign those rights to all of the possible users in all possible places.



Users or groups may be added or deleted as needed or their permission levels changed at any time. Please heed the warnings concerning edit and deletion powers granted by permission, and the serious consequences they can have to the site, Team, management system and database in the hands of unknowledgeable individuals.

Setting Permissions

Wherever you locate a permissions screen, a set of default permissions will already be in effect. The default permissions that appear are those that are set at higher-up administrative levels within your organization. You may wish to preserve those permission settings or change them to meet your needs.

To change permissions, use the column radio buttons and grant permissions to the users or groups identified on the screen. If you have specific users or groups who are not listed, you may add them to the list using the Add Group [Add Group](#) and Add Users [Add User](#) buttons. Once they appear on the screen, you may set permissions as desired. Always remember to click the Save [Save](#) button when permissions are complete.

Report Permissions

* Required

Permissions

Use this page to control the level of access to content and functionality.

[Add Group](#) [Add User](#)

Group/User	No Access	Reader	Participant	Author	Editor	Remove
Everyone	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Registered Users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Relate Licensees	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Permission Rules

- "Readers" can view content, "Participants" can respond to the content, "Authors" can create new content and modify their own content, and "Editors" can modify or remove all content. "No Access" revokes permission granted at a higher level.
- Permissions granted to individual users take precedence over permissions granted to groups of users. If a user has access through multiple groups, the least restrictive permission applies.

Default Permission Overridden Permission Reset to Default Remove
 New Permission Cannot Remove

The Report Permissions example above is a simplified permissions screen. The Group/Users column contains those entities pertinent to the BlueStep™ product you are using **and** to the position within your organization where the screen is located.



Each BlueStep™ product has specific Group/Users that will automatically appear in the Group/Users column. For instance, Everyone and Registered Users are seen throughout Relate™ and Connect™, but not in Team™.

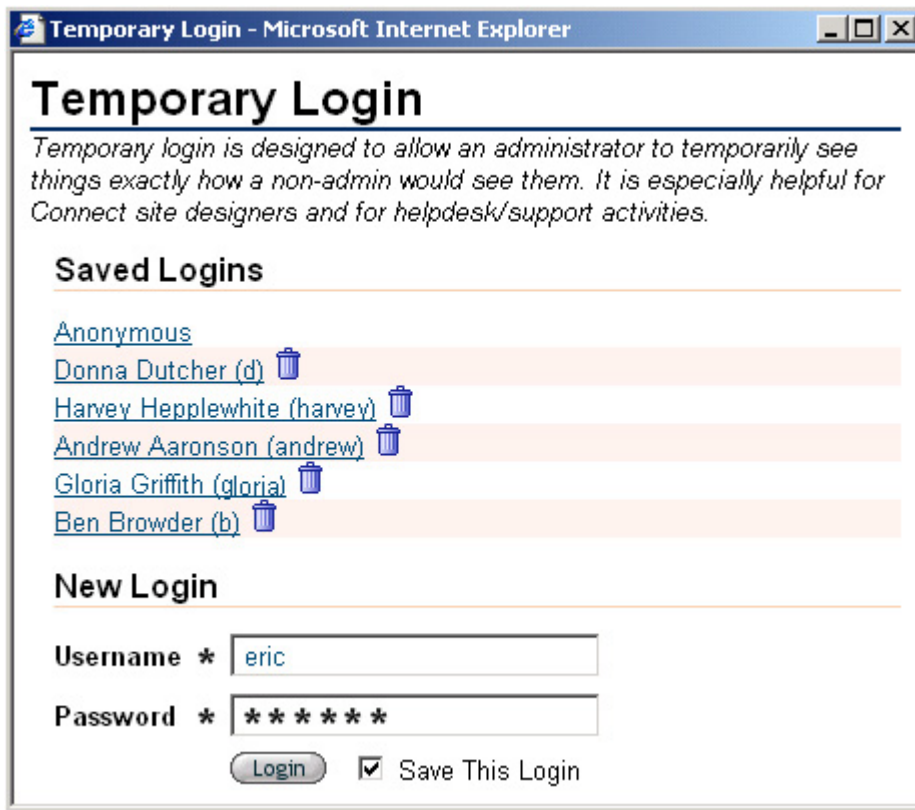
The default groups for BlueStep™ products are:

Relate™	Team™	Connect™	HQ™
Everyone	Team Members	Everyone	All Staff
Registered Users	Team Guests	Registered Users	HQ Licensees
Relate Licensees			Unit Admins
Unit Admins			
Relate Self			

Additionally, any Group/Users that have been added to a permissions screen at a point higher up in the hierarchical structure of your organization will also appear in the Group/Users column. These include such entities as Team Leads, Staff, Clients, Committees or any group/individual available through the Add Group and Add User buttons.


Temporary Login

Administrators (Org Admins, Relate Admins, HQ Admins, Site Admins and Team Leads) have access to a useful tool for verifying permissions and the appearance of pages available to users within their organization. It is called Temporary Login and is available through the Tools drop-down on the dashboard. Mouse over the Tools button and select Temporary Login from the list.






Any logins that have been saved in the Temporary Login list will appear on the pop-up, along with the username for that login. To use one of the listed logins, click on the underlined name. Clicking anonymous displays the site or screen as if you were a not-logged-in individual.

To login as a user not on the list, enter the username and password for that individual in the fields provided. If you would like the login saved for future use, check the Save This Login checkbox. Click the Login button . Whether a recalled temp login or a new temp login, you will be entered into the system as the temporary user when the screen repaints.

To cancel the temporary login, return to the Temporary Login Screen through the Tools drop-down and click the Cancel Login link. This cancel will leave you on the current screen. A second method is to click the Logout link on the dashboard. This method will attempt to move you back to the original page where the temporary login took over, insofar as possible.

 You may use the Temporary Login while on any screen within any BlueStep™ product. However, in a very few instances, because of the wide customization possibilities on Connect™ sites and/or the formatting of various entries in Team™, the login *process* (not the username/password, but the actual logging-in code) may not be compatible with the specific page you are viewing. If you receive an error message, use the back button to navigate to another page. Check the login line on the dashboard. You may be successfully logged in as the temp user or you may need to use the Temporary Login again. Once you have access as the temp user, there should be no errors as you navigate through any of the pages. You will be seeing the site, team or screen just as the temp user does, including the permissions they have been granted.

Permissions Rules

- **Rule 1: Permissions are set at one of five levels per group/individual.** As noted above, Readers can view content; Participants can respond to the content; Authors can create new content and Editors can add, modify or remove any content. No Access can block all access or view of the specified item, *if* the individuals in the group do not have access through another permissions group that would grant less restrictive access. (See third rule, below.)
- **Rule 2: Permissions granted (or restricted) to individual users take precedence over permissions granted to groups of users.** For instance, if a user is added to the permissions list by name (using the Add User button), that permission level will supersede permissions the individual received or was denied as part of a group.
- **Rule 3: If a user has access through multiple groups, the least restrictive permission applies.** For instance, if a user is a Licensee and also a Registered User (which is always the case), the permission that grants the user the highest level of access is in force.
- **Rule 4: Permissions of administrative users, such as organization administrators, site admins and team leads, cannot be restricted.** As is necessary for administrators to perform their assigned tasks, permission level assignments do not override administrator privileges, which are set to Editor permission.
- **Rule 5: New permissions and inherited permissions have equal dominance.** New permissions do not automatically override inherited permissions and vice versa.



The second, third and fourth rules apply and settings under these rules become the inherited permissions from this level downwards in the organization structure.

General Information
Permissions

Permissions

Use this page to control the level of access to content and functionality.

Add Committee
Add User

Group/User	No Access	Reader	Participant	Author	Editor	Remove
Team Guests	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Team Members	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
2005 Planning Committee	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Management Committee	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Permission Rules

- "Readers" can view content, "Participants" can respond to the content, "Authors" can create new content and modify their own content, and "Editors" can modify or remove all content. "No Access" revokes permission granted at a higher level.
- Permissions granted to individual users take precedence over permissions granted to groups of users. If a user has access through multiple groups, the least restrictive permission applies.

Default Permission
 Overridden Permission

Reset to Default
 Remove
 Cannot Remove

In the example above, from BlueStep's Team™ product, permissions are being set on a specific document intended for committee use only. Inherited permissions were overridden to allow No Access for Team members or Guests. Then explicit permission was set for the Planning Committee to have Editor privileges and the Management Committee to have Reader privileges. In this way, access to the document was controlled by blocking the Team members entirely and giving the committees the least restrictive permission level, as described by the third rule, above.

Relate™ Permissions

The permissions for BlueStep's Relate™ product have several special-case conditions that may also affect the access users have to data that is stored in Relate™, even if the data is being presented in Connect™, Team™ or HQ™.

- **Field Permissions in Relate™ take precedence over other permissions.** If permissions on a field have been set using a Relate™ permissions screen, then every place or situation in which that field is used will reflect those permissions. This is true even if other permissions have been set on the screen, pagelet, form, report, discussion, document, merge report, etc. while in Team™, Connect™ or HQ™. The exception is that names and e-mail addresses as seen in surveys, discussions and the Team roster/e-mail screens may not be hidden using Relate™ field permissions.

- **Permissions set on Relate™ forms have effect through the inherited access of the fields on that form.** If access is granted to any field on the form, then the form is visible, without displaying any fields that may have been set to no access. If access is denied to all fields, the form is not displayed. Form permissions have more effect on multi-entry forms, where the form permission governs the access to creating or removing entries.



- **Those with Author permissions on a specific Relate™ field may not edit any data that is contained in that field, even if it is data the Author created.** This differs from the way Author permissions apply to non-Relate data, where Authors may add and create content, plus edit content of their own creation.
- **Relate Self grants special permission to users when creating or editing their own record.** In terms of precedence, Relate Self is treated as group permission and, therefore, may be overridden by setting permissions for specific users.

Basic Permission Screens

Relate™

Permissions

Use this page to control the level of access to content and functionality.

[Add Group](#) [Add User](#)

Group/User	No Access	Reader	Author	Editor	Remove
* Everyone	<input checked="" type="radio"/>	<input type="radio"/>			
* Registered Users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
* Relate Licensees	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
* Relate Self	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
* Unit Admins	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	

Permission Rules

- "Readers" can view data, "Authors" can create data, and "Editors" can modify or remove data. "No Access" revokes permission granted at a higher level.
- Permissions granted to individual users take precedence over permissions granted to groups of users. If a user has access through multiple groups, the least restrictive permission applies.
- "Relate Self" defines the permissions users have to their own record.

Default Permission
 Overridden Permission
 Reset to Default
 Remove

New Permission
 Cannot Remove

[Save](#) [Cancel](#)

Team™

Permissions

Use this page to control the level of access to content and functionality.

[Add Committee](#) [Add User](#)

Group/User	No Access	Reader	Participant	Author	Editor	Remove
* Team Guests	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
* Team Members	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	

Permission Rules

- "Readers" can view content, "Participants" can respond to the content, "Authors" can create new content and modify their own content, and "Editors" can modify or remove all content. "No Access" revokes permission granted at a higher level.
- Permissions granted to individual users take precedence over permissions granted to groups of users. If a user has access through multiple groups, the least restrictive permission applies.

Default Permission
 Overridden Permission
 Reset to Default
 Remove

New Permission
 Cannot Remove

[Save](#) [Cancel](#)



Connect™

Permissions

Use this page to control the level of access to content and functionality.

Add Group Add User

Group/User	No Access	Reader	Participant	Author	Editor	Remove
Everyone	<input type="radio"/>	<input checked="" type="radio"/>				
Registered Users	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Permission Rules

- "Readers" can view content, "Participants" can respond to the content, "Authors" can create new content and modify their own content, and "Editors" can modify or remove all content. "No Access" revokes permission granted at a higher level.
- Permissions granted to individual users take precedence over permissions granted to groups of users. If a user has access through multiple groups, the least restrictive permission applies.

Default Permission
 Overridden Permission
 Reset to Default
 Remove
 New Permission
 Cannot Remove

Save Cancel

HQ™

Permissions

Use this page to control the level of access to content and functionality.

Add Group Add User

Group/User	No Access	Reader	Participant	Author	Editor	Remove
All Staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
HQ Licensees	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
Unit Admins	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	

Permission Rules

- "Readers" can view content, "Participants" can respond to the content, "Authors" can create new content and modify their own content, and "Editors" can modify or remove all content. "No Access" revokes permission granted at a higher level.
- Permissions granted to individual users take precedence over permissions granted to groups of users. If a user has access through multiple groups, the least restrictive permission applies.

Default Permission
 Overridden Permission
 Reset to Default
 Remove
 New Permission
 Cannot Remove

Save and Close Cancel