Using Record Groups in Protege GX

Application Note

Last Published: 15-Sep-21 5:06 PM

Contents

Introduction

Record groups provide the ability to divide a site into functional groups such as building, branch or region. This can be used to streamline reporting, floor plans and status pages, but is primarily designed to customize an operator's user interface to display only the records they are required (or authorized) to access.

For example, a single status list can be created which includes all doors in the system. Each door is then assigned the appropriate record group, such as its building. When an operator views the list in the user interface, they will only see the doors that are included in record groups assigned to their operator role.

Record groups are not used for user access control.

Hierarchical Record Groups

Creating a hierarchy of record groups allows you to easily structure layers of operator access where some operators, such as managers, need access to a broader range of records.

Each record group can be assigned a parent record group, which has access to everything within the child record group. A parent record group can be assigned to multiple record groups, which provides the operator with access to the records included in all of those groups.

In the example below, a record group has been created for each building so that operators can see only the records applicable to the building they are authorized for.

A regional record group is assigned as the parent record group for each of the region's building record groups. This allows a regional manager or other regional operators to access all records within the combined groups.

The global record group is assigned as the parent record group for the regional groups, giving global operators access to records for all buildings.
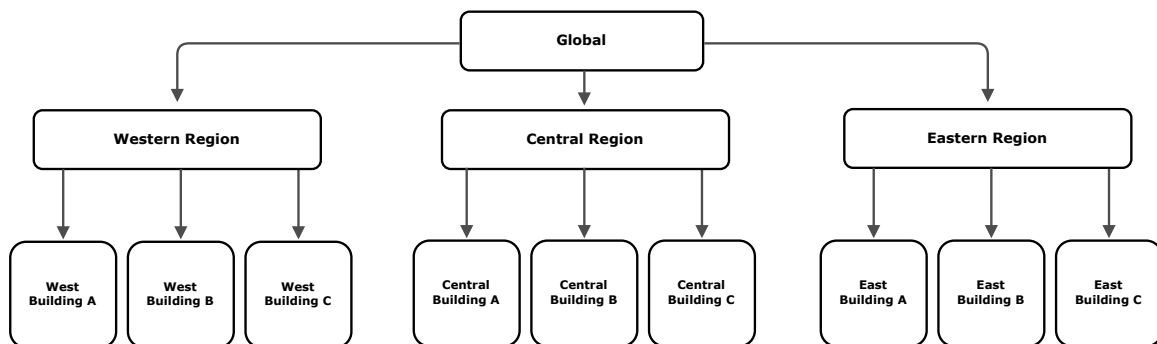
An operator working in multiple buildings across different regions can have as many record groups assigned to their role as is required for them to access, or additional layers can be created in the hierarchy structure.

Which Records Can Be Grouped?

The following Protege GX record types can be filtered by record groups:

- Schedules
- Calendar actions
- Controllers*
- Credential types
- Function codes
- Users
- Access levels
- Custom fields and custom field tabs
- Card templates
- Reports
- Floor plans
- Status pages
- Salto doors, Salto door groups and Salto calendars
- Doors and door types
- Areas
- Elevator cars
- Floors
- Phone numbers
- Apartment areas and apartment users
- Door groups
- Area groups
- Keypad groups
- Menu groups
- Output groups
- Elevator groups
- Floor groups

* Records which cannot be assigned a record group - such as inputs, trouble inputs and outputs - automatically follow the controller they are associated with. This includes the controller record group being <Not set>. Records which can be assigned a record group are not affected by the record group settings of controllers.

Record Groups and Security Levels

The Protege GX system allows administrators to customize operator access and visibility to provide controlled access to records, relevant to the role of each staff member.

Security levels define the types of records the operator can access within the Protege GX system, and their level of control for each record type.

Assigning security levels to operator roles allows you to more precisely control which functions operators can perform. Some record types they may have full access to, others they may only be permitted to view, and some they may not see at all.

Record groups determine which specific records operators can see and control, within the parts of the system that their security levels permit them to access.

Summary

- Each operator is assigned a role to determine what access they have to the Protege GX system and records.
- Each role is configured at the global level and includes:
    - A global **Preset** which defines the operator's default access.
    - The operator's level of access to specific Protege GX **Tables**, which can be inherited from the preset or customized as required.
    - The **Sites** the operator can access records for.
    - Optionally, site-specific **Security levels** (see below).
    - Optionally, the site-specific **Record groups** the operator can access.

        A record group can only be assigned to an operator role in conjunction with a site-specific security level.

- Security levels determine which types of records an operator can access, and what level of access and control they have for each record type. Each security level is configured at the site level and includes:
    - The operator's level of access to specific Protege GX **Tables** for the site, which can be inherited from the role or customized as required.

        Permissions granted in a security level will override those granted in the role.

    - The **Manual commands** the operator can perform on the site.
- Record groups determine which specific records the operator can see and control, within the record types that their access level grants them access to.

Only one security level per site may be assigned to each operator role. Multiple record groups with the same security level can be included, but record groups with different security levels are not supported. If multiple security levels for the same site are assigned to a role, the user interface may not behave as expected.

Programming Operator Access

To effectively control operator access using record groups, the following steps are required:

- Create record groups
- If hierarchical grouping is required, assign parent record groups
- Assign record groups to records
- Create security levels
- Create roles
- Assign security levels and record groups to operator roles
- Assign roles to operators

Creating a Record Group

1. Navigate to **Sites | Record groups**. In the toolbar, select the **Site** this record group will apply to.
2. Add a record group with a **Name** that identifies the grouping, such as the building, branch or region.
3. Click **Save**.

Assigning a Parent Record Group

To create hierarchical filtering of records (see page 4), a parent record group needs to be assigned to each of the record groups that you want it to include.

1. Add the record group that will be the parent record group, such as a regional or global group.
2. Add or select the child record group, and set the **Parent record group** as required.

   You can also multi-select (**Ctrl + click**) all the child record groups and set the parent collectively.

3. Click **Save**.

Assigning a Record Group to a Record

The records that you assign record groups to determines what each operator has access to in the user interface.

1. To assign a record group, navigate to the programming page for the record (e.g. **Programming | Doors**).
2. Select (or multi-select) the record(s) to include in the record group.
3. Select the appropriate **Record group**.
4. Click **Save**.

When a record group is assigned to a controller, operators who have access to that record group also have access to the unassignable records associated with the controller. Operators without that record group assigned to their role will have no access to those records. If the controller has no record group assigned, only operators with no record groups or <Not set> assigned will be able to access the controller and its associated unassignable records.

For more information, see Which Records Can Be Grouped? (page 5).

Creating Security Levels

1. Navigate to **Sites | Security levels**. In the toolbar, select the **Site** where this security level will be used.

2. Add a security level with a **Name** that identifies its purpose, such as the level of access or operator role.

3. In the **Tables** tab, set the permissions this security level has for the various database tables.
   - Inherit from role to retain the permissions from the role that this security level is assigned to.
   - Deny to prevent access to the data contained in the table. This hides any functions and menu options for that table from the operator.
   - Grant full access to grant full read/write permissions to the table.
   - Grant read only access to grant access to view but not to update data in the table. The operator will be able to view the relevant settings but the options for updating them are disabled.

4. In the **Manual commands** tab, define the specific manual commands that are available to operators with this security level assigned. For each command, choose from Inherit (from the role), Allow or Deny.

5. Click **Save**.

For more information on security levels, see the Protege GX Operator Reference Manual.

Creating Roles

1. Navigate to **Global | Roles**.

2. Add an operator role with a **Name** that identifies the operator level or job title.

3. Select the **Preset** that this role will be based on.
   - Administrator: Can perform all actions in all sites without any restrictions.
   - Installer: Can perform actions required to install and configure the system.
   - End user: Can perform reporting and limited system configuration of users.
   - Guard: Can monitor the system and view events only.

4. In the **Sites** tab, define which sites this role will have access to. If they are denied access to a site, operators will be able to see that the site exists, but not view or edit any of its records. The default is access to all sites.

5. Click **Save**.

An operator role will be required for each level of access, and also for each record grouping. An organization may grant the same level of access to guards in all of its buildings, but if record grouping is to be used each building will need its own guard operator role with the appropriate record group assigned.

For more information on roles, including preset permissions, see the Protege GX Operator Reference Manual.

Assigning Security Levels and Record Groups to Roles

1. Select or add the role to assign the security level and record group to.

2. In the **Security levels** tab, click **Add**.

3. Select the **Site** this configuration will apply to.

4. Select the **Security level** to define the required access permissions of this role for the selected site.

5. Define the **record group** access for this role.

   - Check Access all record groups to grant access to all records (based on the security level permissions).

   - Select the <Not set> record group to grant access to all records with <Not set> or no record group assigned.

   - Select the required record group(s) to grant access to records within the selected group(s).

   Click **Ok**.

6. Click **Save**.

Only one security level per site may be assigned to each operator role. Multiple record groups with the same security level can be included, but record groups with different security levels for the same site are not supported.

Operators can only access records which have the same record group assignment as their operator role, as illustrated below.

Operator Record Group	Record Group <Not set> for Record	Record Group Assigned to Record
No record group assigned to operator role	✅	❌
<Not set> record group assigned to operator role	✅	❌
Same record group assigned to operator role	❌	✅
Other record group assigned to operator role	❌	❌

Note that when assigning a security level to an operator role, <Not set> can be assigned as the record group. This can be used to restrict operator access to only those records with no record group assigned, or to provide access to those records in addition to records with selected assigned record groups.

Assigning Roles to Operators

1. Navigate to **Global | Operators**.

2. Add or select the required operator(s) and assign the appropriate **Role**.

   When new operators are added, the default role setting is No access until a role is selected.

3. Click **Save**.

Programming Scenario

In this scenario there is a single site with two buildings in the Eastern region. Building managers only have access to records for the building they manage, while regional managers have access to all records for the region.

We will create record groups for East Building A and East Building B, with a parent record group for the Eastern Region. The record groups will be assigned to some records for each building, and security levels and operator roles created and assigned to the relevant operators. Each manager will have full administrative permissions for the records in their record group (using the Administrator role preset).

We will also create a basic status list and status page to help demonstrate the operation of the record groups.

Before You Begin

To test this programming scenario you will need an operational Protege GX system with at least two controllers online. The following records must be programmed before you begin:

- **Controllers**: East A Ctrl, East B Ctrl
- **Areas**: East A Office, East B Office
- **Doors**: East A Door, East B Door
- **Outputs**: East A Lights, East B Lights
- **Operators**: East A Manager, East B Manager, Eastern Manager

Create the Record Groups

1. Navigate to **Sites | Record groups**. In the toolbar, select the **Site**.
2. First, add the Eastern Region parent record group. Click **Save**.
3. Add the East Building A record group and set the **Parent record group** to Eastern Region. Click **Save**.
4. Add the East Building B record group and set the **Parent record group** to Eastern Region. Click **Save**.

Assign the Record Groups to Records

1. Navigate to **Programming | Areas**.
   - Select East A Office and set the **Record group** to East Building A, then **Save**.
   - Select East B Office and set the **Record group** to East Building B, then **Save**.
2. Navigate to **Programming | Doors**.
   - Select East A Door and set the **Record group** to East Building A, then **Save**.
   - Select East B Door and set the **Record group** to East Building B, then **Save**.

For now, we will not assign any record groups to controllers.

Create the Security Levels

1. Navigate to **Sites | Security levels**. In the toolbar, select the **Site**.
2. Add the East A Manager security level and **Save**.
3. Add the East B Manager security level and **Save**.
4. Add the Eastern Manager security level and **Save**.

Create the Roles

1. Navigate to **Global | Roles**.

2. Add the East A Manager role and set the **Preset** to Administrator.
   - In the **Security levels** tab, click **Add**.
   - Select the **Site**.
   - Set the **Security level** to East A Manager.
   - Select the East Building A record group, then click **Ok**.

3. Add the East B Manager role and set the **Preset** to Administrator.
   - In the **Security levels** tab, click **Add**.
   - Select the **Site**.
   - Set the **Security level** to East B Manager.
   - Select the East Building B record group, then click **Ok**.

4. Add the Eastern Manager role and set the **Preset** to Administrator.
   - In the **Security levels** tab, click **Add**.
   - Select the **Site**.
   - Set the **Security level** to Eastern Manager.
   - Select the Eastern Region record group, then click **Ok**.

Assign Roles to The Operators

1. Navigate to **Global | Operators**.

2. Select the East A Manager operator and assign the East A Manager **Role**.

3. Select the East B Manager operator and assign the East B Manager **Role**.

4. Select the Eastern Manager operator and assign the Eastern Manager **Role**.

5. Click **Save**.

Configure the Status Page

1. Navigate to **Monitoring | Setup | Status lists**. In the toolbar, select the **Site**.

2. Add the Eastern Status List.

3. In the **Devices** section, click **Add**.
   - Set the **Device type** to Door, select East A Door and East B Door, then click **Ok**.
   - Set the **Device type** to Output, select East A Lights and East B Lights, then click **Ok**.
   - Set the **Device type** to Area, select East A Office and East B Office, then click **Ok**.

4. Click **Save**.

5. Navigate to **Monitoring | Setup | Status page editor**.

6. Add the Eastern Status Page, select your preferred **Default layout**, then click **Ok**.

7. Select a tile and set the **Type** to Status list and the **Record** to the Eastern Status List.

8. Set the configuration for columns and rows as desired, then **Save**.

Testing

Once the scenario configuration is complete, you can now test your programming.

1. Log out or close the Protege GX user interface.
2. Log in as East A Manager.
   - Navigate to **Programming | Doors**. You should be able to see East A Door only.
   - Navigate to **Programming | Areas**. You should be able to see East A Office only.
   - Navigate to **Programming | Outputs**. You should not be able to see any outputs.
   - Navigate to **Monitoring | Status page view** and select the Eastern Status Page. You should be able to see the status of East A Door and East A Office only.
3. Log out, then log in as East B Manager.
   - Navigate to **Programming | Doors**. You should be able to see East B Door only.
   - Navigate to **Programming | Areas**. You should be able to see East B Office only.
   - Navigate to **Programming | Outputs**. You should not be able to see any outputs.
   - Navigate to **Monitoring | Status page view** and select the Eastern Status Page. You should be able to see the status of East B Door and East B Office only.
4. Log out, then log in as Eastern Manager.
   - Navigate to **Programming | Doors**. You should be able to see both East A Door and East B Door.
   - Navigate to **Programming | Areas**. You should be able to see both East A Office and East B Office.
   - Navigate to **Programming | Outputs**. You should not be able to see any outputs.
   - Navigate to **Monitoring | Status page view** and select the Eastern Status Page. You should be able to see the status of East A Door, East B Door, East A Office and East B Office.
5. Now assign the record groups to their respective controllers.
   - Log out, then log in as an admin operator with access to all records.
   - Navigate to **Sites | Controllers**. In the toolbar, select the **Site**.
   - Select the East A Ctrl controller record and set the **Record group** to East Building A.
   - Select the East B Ctrl controller record and set the **Record group** to East Building B.
   - Click **Save**.
6. You should now be able to access the East A Lights and East B Lights outputs, as these are associated with the controllers which are now part of the Eastern record groups.
   - Navigate to **Programming | Outputs**. These outputs should now be visible, and accessible for the operator to view and edit.
   - Navigate to **Monitoring | Status page view** and select the Eastern Status Page. You should be able to view the status and control the East A Lights and East B Lights outputs.
   - This can be repeated for the East A Manager and East B Manager operators to test their access to the outputs for their respective buildings.

Additional Record Group Usage

Using the Find Tool

Records in the Protege GX interface can easily be filtered to display only the records with, or without, the selected record group(s) assigned.

1. Navigate to the relevant programming page (e.g. **Programming | Doors**).

2. In the toolbar, click **Find**.

3. Set the search **Field** to Record group.

4. Set the search **Values** to either Contains the following or Does not contain the following.

5. Select the record group(s) to find/exclude records for, then click **Ok**.

The programming page will filter the records to display only those which meet the search criteria.

Filtering User Records

User records can be viewed in Protege GX in **Tree View** (organized by record group) by clicking the icon in the toolbar. List view is the default, but you can set the default to tree view by enabling the **Display users in groups** option (**Global | Sites | Display**).

User records can also be filtered using the find tool.

User Search

The user search feature (**Users | User Search**) allows you to generate one-off temporary user reports that can be printed, exported or emailed. It is ideal for creating ad hoc reports that do not need to be repeated frequently.

User search offers the following record group options:

- **Report type**: Select All users by record group for a user report which automatically groups users by record group.
- **Sort column**: Set to Record group to sort the search results by record group.
- **Group by**: Set to Record group to group the search results by record group.
- **Columns**: Add the Record group column to include each user's assigned record group in the search results.

Filtering Reports

Record groups can be used to easily and conveniently customize reports to include results for selected record groups only. This is ideal for streamlining reporting for installations with many buildings, departments or regions.

Event Reports

1. Navigate to **Reports | Setup | Event** and select or add an event report to customize.

2. Select a **Record group** to restrict access to this report. When a record group is selected, only operators with the selected record group assigned to their role will be able to view this report.

3. Click **Add** to add an **Event filter**, and select the **record group** to filter the records by. The report will only include records in the selected record group(s).

Muster Reports

1. Navigate to **Reports | Setup | Muster** and select or add a muster report to customize.

2. Select a **Record group** to restrict access to this report. When a record group is selected, only operators with the selected record group assigned to their role will be able to view this report.

3. In the **Columns** tab, click **Add** and select the Record group column to include each user's assigned record group in the report results.

User Reports

1. Navigate to **Reports | Setup | User** and select or add a user report to customize.

2. Select a **Record group** to restrict access to this report. When a record group is selected, only operators with the selected record group assigned to their role will be able to view this report.

3. Set the following options related to record groups as required:
   - **Report type**: Select All users by record group for a user report which automatically groups users by record group.
   - **Sort column**: Set to Record group to sort the report results by record group.
   - **Group by**: Set to Record group to group the report results by record group.

4. In the **Columns** tab, **Add** the Record group column to include each user's assigned record group in the report.

For more information on reports setup, see the Protege GX Operator Reference Manual.

Custom Third-Party Integrations

Record groups can be referenced in custom third-party integrations, by defining a value that is included in the integration XML schema. To define the value that a record group will be identified by in custom third-party integrations:

1. Navigate to **Sites | Record groups**. In the toolbar, select the **Site**.

2. Select the record group to define the identifier value for.

3. In the **Custom data** tab, set the value which will identify this record group. This information is included in the XML schema for record groups.
   - **Numeric Data**: A number that identifies the record group.
   - **Text Data**: A text string that identifies the record group.