AN-191

Preset Roles within Protege GX

Application Note

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

Last Published: 04-Jul-24 9:02 AM

Contents

Introduction

Roles in Protege GX determine what each operator has permission to see and do in the software. They define which items in the Protege GX menu are visible, enabling you to limit access to specific functions and records based on the requirements of the operator.

For example, operators in an HR position are typically granted full access to view and edit users and run reports on access data, but denied permission to records related to the physical operation of the site such as doors and outputs.

When creating a role in **Global | Roles**, you start by assigning one of the four presets:

- **Administrator** or **Installer**: Can perform all actions in the system without any restrictions.
- **End user**: Can perform most actions related to user access and scheduling. Can view status pages and floor plans and run reports.
- **Guard**: Can view status pages and floor plans and run event reports.

The preset for the role determines which permissions are enabled and disabled by default. This document contains a reference guide for the default permissions for each preset.

You can then refine the permissions for that specific role by adjusting the settings in the other tabs:

- **Tables**: The menu items and functions available to the operator. By default these are set to Inherit from default. You can modify each table to Deny, Grant full access or Grant read only access.
- **Sites**: By default the operator has access to all sites. You can enable or disable access to each site individually.
- **Security levels**: To further refine the operator's permissions, you can set the security level within a site or record group. Security levels (**Sites | Security levels**) provide a more granular breakdown of the functions that are available to the operator. This also allows you to restrict the operator to one or more record groups, which may represent different regions or companies within the Protege GX system.

This document also includes an example of role and security level programming to provide a starting point for customizing your own roles.

Role Presets

Each role in Protege GX must be based on a specific preset which has predefined access parameters. The **Tables** and **Security levels** tabs allow you to customize what access each role has, using the preset as a starting point.

= Full Access

= Read Only

= Denied

Description	Admin	Installer	End User	Guard
Access Levels	✓	✓	✓	✗
Alarms	✓	✓	✗	✗
Analog Expanders	✓	✓	✗	✗
Apartments	✓	✓	✗	✗
Areas	✓	✓	✗	✗
Area Groups	✓	✓	✗	✗
Attendance	✓	✓	✗	✗
Automation	✓	✓	✗	✗
BitData Values	✓	✓	✗	✗
Calendar Actions	✓	✓	✗	✗
Cameras	✓	✓	✗	✗
Controllers	✓	✓	✗	✗
Credential Types	✓	✓	✓	✗
Custom Fields	✓	✓	✓	✗
Custom Field Tabs	✓	✓	✓	✗
Data Values	✓	✓	✗	✗
Daylight Savings	✓	✓	✓	✗
Device States	✓	✓	✗	✗
Doors	✓	✓	✗	✗
Door Groups	✓	✓	✗	✗
Door Types	✓	✓	✗	✗

Description	Admin	Installer	End User	Guard
Download Servers	✓	✓	✗	✗
DVRs	✓	✓	✗	✗
Elevator Cars	✓	✓	✗	✗
Elevator Groups	✓	✓	✗	✗
Event Filters	✓	✓	✗	✗
Event Reports	✓	✓	✓	✓
Event Servers	✓	✓	✗	✗
Floors	✓	✓	✗	✗
Floor Groups	✓	✓	✗	✗
Floor Plans	✓	✓	✓	✓
Health Status	✓	✓	✓	✓
Holidays	✓	✓	✓	✗
Holiday Groups	✓	✓	✓	✗
Inputs	✓	✓	✗	✗
Input Expanders	✓	✓	✗	✗
Input Types	✓	✓	✗	✗
Intercoms	✓	✓	✗	✗
Jobs	✓	✓	✗	✗
Kaba Lock Groups	✓	✓	✗	✗
Keypads	✓	✓	✗	✗
Keypad Groups	✓	✓	✗	✗
Licensing	✓	✓	✓	✓
Menu Groups	✓	✓	✗	✗
Modems	✓	✓	✗	✗
Muster Reports	✓	✓	✗	✗
Operators	✓	✓	✗	✗

Description	Admin	Installer	End User	Guard
Outputs	✓	✓	✗	✗
Output Expanders	✓	✓	✗	✗
Output Groups	✓	✓	✗	✗
Phone Numbers	✓	✓	✗	✗
Photo ID Templates	✓	✓	✓	✗
Programmable Functions	✓	✓	✗	✗
Reader Expanders	✓	✓	✗	✗
Record Groups	✓	✓	✓	✗
Record History	✓	✓	✓	✗
Roles	✓	✓	✗	✗
Salto Calendars	✓	✓	✗	✗
Salto Doors	✓	✓	✗	✗
Salto Door Groups	✓	✓	✗	✗
Salto Outputs	✓	✓	✗	✗
Salto Time Periods	✓	✓	✗	✗
Schedules	✓	✓	✓	✗
Scripts	✓	✓	✗	✗
Security Levels	✓	✓	✗	✗
Security Options	✓	✓	✗	✗
Server Event Log	✓	✓	✓	✓
Services	✓	✓	✗	✗
Sites	✓	✓	✗	✗
Smart Readers	✓	✓	✗	✗
Status Definitions	✓	✓	✗	✗
Status Lists	✓	✓	✓	✓
Status Pages	✓	✓	✓	✓

Description	Admin	Installer	End User	Guard
System	✓	✓	✗	✗
Trouble Inputs	✓	✓	✗	✗
Users	✓	✓	✓	✗
User Images	✓	✓	✓	✗
User Import	✓	✓	✗	✗
User Reports	✓	✓	✓	✗
Variables	✓	✓	✗	✗
Variable History	✓	✓	✓	✗
VMS	✓	✓	✓	✓
VMS Cards	✓	✓	✓	✓
VMS Images	✓	✓	✓	✓
VMS Pages	✓	✓	✓	✓
VMS Workstations	✓	✓	✓	✓
Web Links	✓	✓	✗	✗

Example: Security Guard Operator

As an example, we will demonstrate how to program an operator record for use by a security guard.

First, we must assess how the security guard will be using Protege GX, and therefore what records they need access to.

- The guard is employed by ACME Incorporated, and should therefore be restricted to viewing records on the ACME site.
- The guard is responsible for monitoring only ACME's Singapore location. They should be restricted to viewing records in the Singapore record group.
- The guard's duties include:
  - Monitoring door and area status from a floor plan or status page.
  - Monitoring events and security camera footage.
  - Controlling doors and areas from the Protege GX software. However, they are not permitted to bypass inputs.
  - Comparing user photos to the users entering the building. However, they are not permitted to add or edit user records.

As a starting point, we will use the Guard role preset. The role presets table (see page 5) indicates that this preset has permission to view status pages, floor plans and event reports, but few other permissions. This allows us to add only what is required for this particular operator.

Programming Steps

Before we begin, it is assumed that the ACME site and Singapore record group already existed, and that the record group has been applied to the relevant records (including status pages and floor plans).

Because the guard's access must be restricted to a specific record group, we need to create a security level. The security level also determines how this operator's access differs from the standard Guard preset.

1. In Protege GX, navigate to **Sites | Security levels**.
2. In the toolbar, set the **Site** to ACME.
3. Add a new security level with the name Security Guard (ACME).
4. The **Tables** tab allows you to set the access individually for each record type.
   - Most records can be left as Inherit from role to retain the settings from the Guard preset.
   - The **Users** table should be set to Grant Read Only Access. This overrides the setting from the role preset (no user access permitted).
5. The **Manual commands** tab allows you to set whether the guard can control each type of device.
   - Most records can be left as Inherit from role. The Guard preset is permitted to control doors and areas from a status page by default.
   - Set **Input control** to Deny. This will prevent the guard from bypassing inputs.
6. Click **Save**.

Now we can apply the security level to a role:

1. Navigate to **Global | Roles** and add a new role with the name Security Guard (ACME Singapore).
2. Set the **Preset** to Guard.
3. Open the **Sites** tab and uncheck **Has access to all sites**.
4. Check the box next to the ACME site. This ensures that the operator only has access to records in this site.
5. Open the **Security levels** tab and click **Add**.

- Set the **Site** to ACME.
- Set the **Security level** to Security Guard (ACME).
- Select the Singapore record group.
- Click **Ok**.

6. Click **Save**.

Finally, we must create an operator who uses the new role:

1. Navigate to **Global | Operators** and add a new operator called Zhang San (ACME Singapore).
2. Set the **Username** and **Password** to unique values. Ensure that you use a strong password or pass phrase.
3. Set the **Role** to Security Guard (ACME Singapore).
4. Set the **Time Zone** to GMT+08:00 Singapore Standard Time Singapore.
5. Ensure that **Show PIN numbers for users** is disabled. This ensures that the guard cannot see users' PIN codes.
6. Check **Enable operator timeout** and set the **Operator timeout in seconds** to 600 (10 minutes). If the operator is not active for this length of time, the Protege GX client will give a 30 second warning and then close.
7. Click **Save**.

To test the programming, open a new Protege GX client and log in as the guard operator. Ensure that you can see and control only the records which have been specified in the job description above. For example, the guard should be able to view only user records in the Singapore record group (excluding their PIN codes), and should not be able to edit them.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.