Proficy CIMPLICITY 11.1

Security

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:
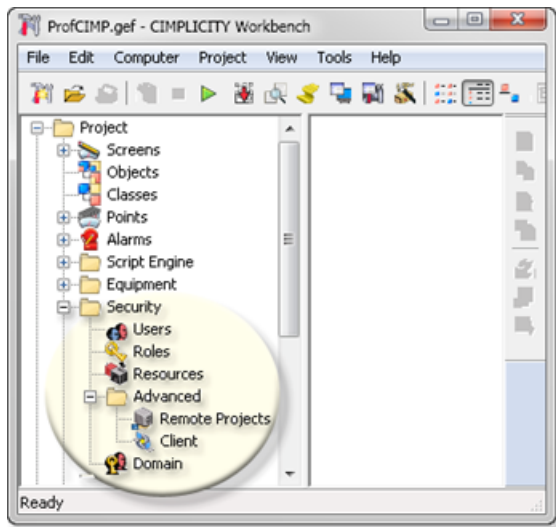
doc@ge.com

Chapter 1. About Security and Routing

CIMPLICITY security features in the Workbench left pane include the following.

rect 40, 191, 128, 208 [About Users *(page 29)*](#)
rect 40, 206, 128, 223 [About Roles *(page 11)*](#)
rect 40, 221, 128, 238 [About Resources *(page 6)*](#)
rect 66, 264, 162, 279 [About Client Configuration *(page 51)*](#)
rect 53, 277, 127, 292 [Windows Authentication Configuration *(page 30)*](#)

Feature	Description
Users	Configure users for a CIMPLICITY project.
Roles	Create roles with assigned privileges. The role that is assigned to a user determines what the user can do in a CIMPLICITY project.
Resources	Physical or conceptual units that comprise a facility.
Remote projects	Defined to retrieve point information from projects running on other computers.
Client	Configure default log ins for CIMPLICITY viewers on client computers.

Chapter 2. Resource Configuration

About Resources

Resources are the physical or conceptual units that comprise your facility. They can be devices, machines, or stations where work is performed, or areas where several tasks are carried out. Resource configuration plays an important role in your CIMPLICITY project by routing alarms to specific users and filtering the data users receive.

CIMPLICITY software uses resources in the following ways:

- Each CIMPLICITY device and point is associated with a resource.
- Each user has a view of the facility. The view is defined by the resources configured for that user. CIMPLICITY software alarms are generated against resources and routed (displayed) to users who have those resources in their view.
- Many base system functions (such as Alarm Viewer) and product option functions filter data by resource. For example, a user can create an Alarm Viewer display that only contains alarm data for a specific resource.

Resource Configuration

Resource Configuration

The Workbench displays a project's existing resources in the right pane.

- Create and configure resources.
- View a project's existing resources.

Create and configure resources

Step 1 (page 8)	Create a new resource.
Step 2 (page 9)	Configure a resource definition.

View a project's existing resources

Select Project>Security>Resources in the Workbench left pane.

The Workbench right pane displays the following attributes for each Resource.
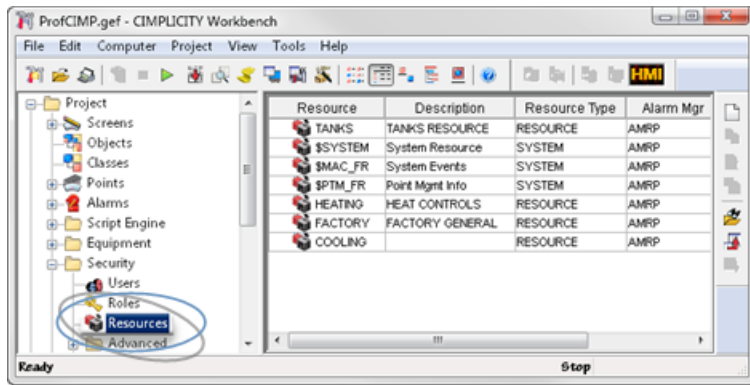
Attribute	Description
Resource	A name that uniquely identifies each resource.
Description	Text that gives users more information about the resource.
Resource Type	Identifies the type of resource. CIMPLICITY software currently supports two resource types: SYSTEM, and RESOURCE. This is a display-only field and cannot be modified. Any resources you create are automatically given a **Resource Type** of RESOURCE.
Alarm Mgr	Identifies the Alarm Manager process that receives alarms for this resource. This is a display-only field and cannot be modified.

📄 **Note:** Use the Workbench Field Chooser to remove or re-display any of the fields, except the Resource. The Resource is required.

The Resource list is initially sorted by **Resource**. You can click on any of the other column titles at the top of the list to sort the list by that attribute.

Step 1. Open a Resource Definition Dialog Box

Step 1. Open a Resource Definition Dialog Box

Option 1.1 *(page 8)*	Create a new resource.
Option 1.2 *(page 9)*	Open an existing Resource Definition dialog box.

Option 1.1. Create a New Resource

1. Select **Project>Security>Resources** in the Workbench left pane.
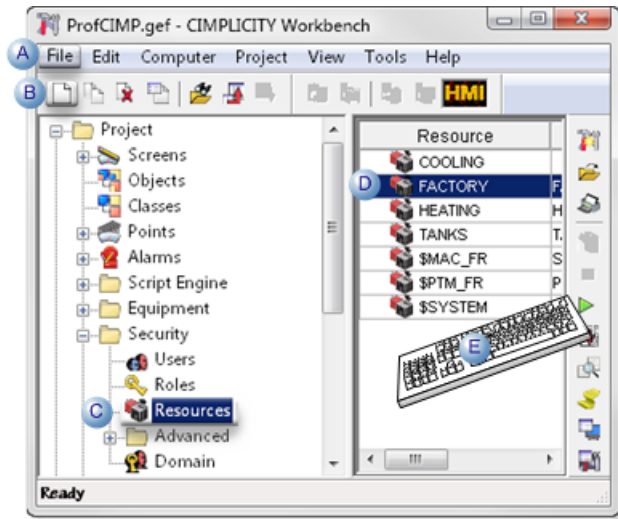
2. Do one of the following.

Item	Description
A	Click File>New on the Workbench menu bar.
B	Click the New Object button on the Workbench toolbar.
C	In the Workbench left pane, either double-click **Resources**, or right-click **Resources** and select New on the Popup menu.
D	In the Workbench right pane, right-click any resource and select New on the Popup menu.
E	Press Ctrl+N on the keyboard.

A New Resource dialog box opens when you use any method.

3. Enter the name of the new resource in the **Resource ID** field.

4. Click OK.

The system verifies that the Resource ID does not already exist, and that no invalid characters have been used. If the Resource ID you entered is valid, the Resource Definition *(page 9)* dialog box for the new resource opens.

Option 1.2. Open an Existing Resource Definition Dialog Box

1. Select **Project>Security>Resources** in the Workbench left pane.

2. Select a resource in the Workbench right pane.
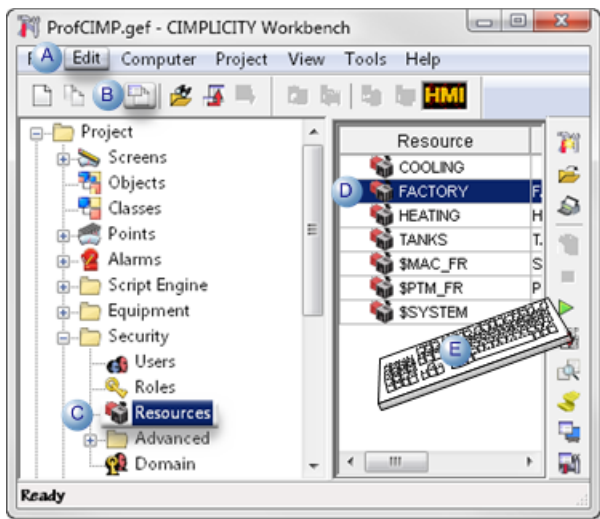
3. Do one of the following.

Action	Description
A	Click Edit>Properties on the Workbench menu bar.
B	Click the Properties button on the Workbench toolbar.
C	In the Workbench left pane: a. Right-click **Resources**. b. Select Properties on the Popup menu.
D	In the Workbench right pane, either double-click a resource, or right-click a resource and select Properties on the Popup menu.
E	Press Alt+Enter on the keyboard.

The Resource Definition dialog box for the selected resource opens.

Step 2. Configure a Resource Definition

Description

Up to 40 characters of explanatory text describing the resource.

⚠️ **Important:** You cannot use the $ or | characters in a resource name.

Add

1. Select the user in the **Available users** box.
2. Select **Add**.

The user is moved to the **Users for this resource** box.

Remove

1. Select the user in the **Users for this resource** box.
2. Select **Remove**.

The user is removed to the **Available users** box.

Properties

1. Select the user in either the **Available users** or **Users for this resource** box.
2. Select **Properties**.

A **User Properties** window for the selected user opens.

New

1. Create a new user.
2. Do a project configuration update.

The new user is added to the **Available users** or **Users for this resource** box for the selected resource.

Chapter 3. Role Configuration

About Roles

Each user in CIMPLICITY is assigned a role.

A role specifies what privileges its users have when they work in CIMPLICITY . Types of privileges include:

📒 **Note:** The CIMPLICITY default configuration includes the following three roles:

- SYSMGR
- USER
- OPER

Role Configuration

Role Configuration

Step 1 (page 11)	Open a role's Role Properties dialog box.
Step 2 (page 14)	Assign role privileges.

Procedure to View a Project's Existing Roles

1. Expand the Security folder in the left pane of the Workbench.
2. Select 🔑 Roles.

The Workbench right pane displays the Role ID for each Role.

Step 1. Open a Role's Role Properties Dialog Box

Step 1. Open a Role's Role Properties Dialog Box

Option 1.1 *(page 12)*	Create a new role.
Option 1.2 *(page 13)*	Open a Role Properties dialog box for an existing role.

Option 1.1. Create a New Role

1. Select **Project>Security>Roles** in the Workbench left pane.
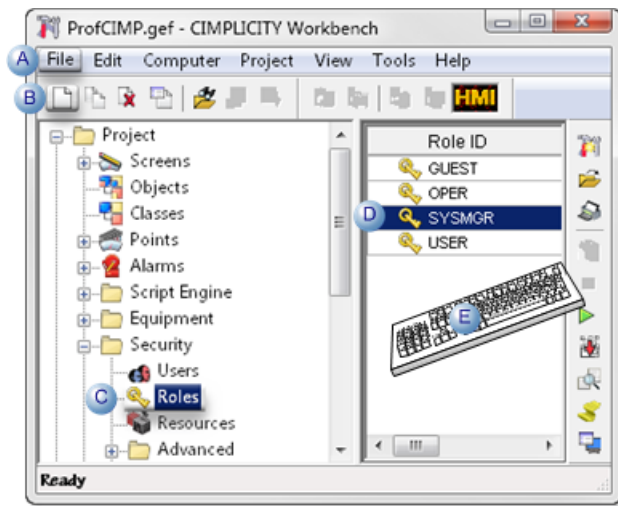
2. Do one of the following.

Action	Description
A	Click File>New on the Workbench menu bar.
B	Click the **New Object** button on the Workbench toolbar.
C	In the Workbench left pane, either double-click **Roles**, or right-click **Roles** and select New on the Popup menu.
D	In the Workbench right pane, right-click any role, and select New on the Popup menu.
E	Press Ctrl+N on the keyboard.

The new role dialog box opens when you use any method.

3. Enter the name of the new role in the **Role ID** field.

4. Click **OK**.

The system verifies that the Role ID does not already exist, and that no invalid characters have been used. If the Role ID you entered is valid, the Role Properties dialog box for the new role will open.

ⓘ Tip: You can also open the Role Properties dialog box through the Point Properties dialog box.

Option 1.2. Open a Properties Dialog Box for an Existing Role

1. Select **Project>Security>Roles** in the Workbench left pane.

2. Select a role in the Workbench right pane.
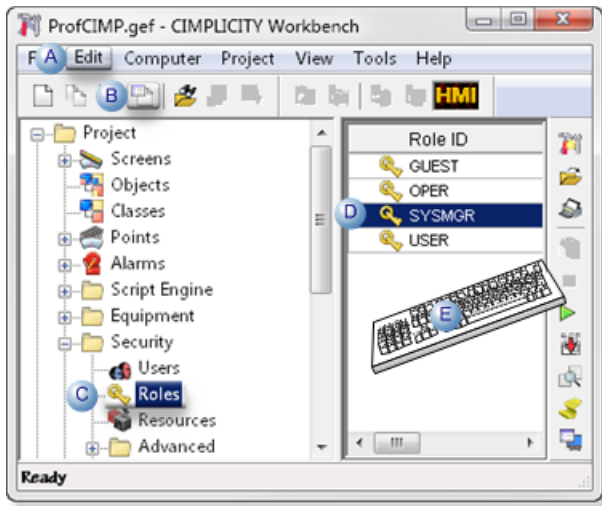
3. Do one of the following.

Item	Description
A	Click Edit>Properties on the Workbench menu bar.
B	Click the **Properties** button on the Workbench toolbar.
C	In the Workbench left pane: a. Right-click **Roles**. b. Select Properties on the Popup menu.
D	In the Workbench right pane, either double-click a role, or right-click a role and select Properties on the Popup menu.
E	Press Alt+Enter on the keyboard.

4. Click the **Properties** button on the Workbench toolbar.
   The Role Properties dialog box associated with the selected role opens.

ⓘ Tip: You can also open a Role Properties dialog box for an existing role through the Point Properties dialog box.

Step 2. Assign Role Privileges

Step 2. Assign Role Privileges

You can assign privileges to each role in each of the following categories.

📝 **Note:** Many of the tabs that can be available in the Roles Properties dialog box display only when the option they apply to is enabled.

Option 2.1 *(page 14)*	Assign role application privileges.
Option 2.2 *(page 20)*	Assign role calendar privileges.
Option 2.3 *(page 21)*	Assign role configuration privileges.
Option 2.4 *(page 22)*	Assign role Broadcast privileges.
Option 2.5 *(page 23)*	Assign role Query Engine privileges.
Option 2.6 *(page 24)*	Assign role TADB privileges.
Option 2.7 *(page 24)*	Assign role Tracker UI privileges.
Option 2.8 *(page 27)*	Assign role RCO UI privileges.

Option 2.1 Assign Role Application Privileges

The Privileges tab on the Role Properties dialog box let you define the application privileges for a new role.
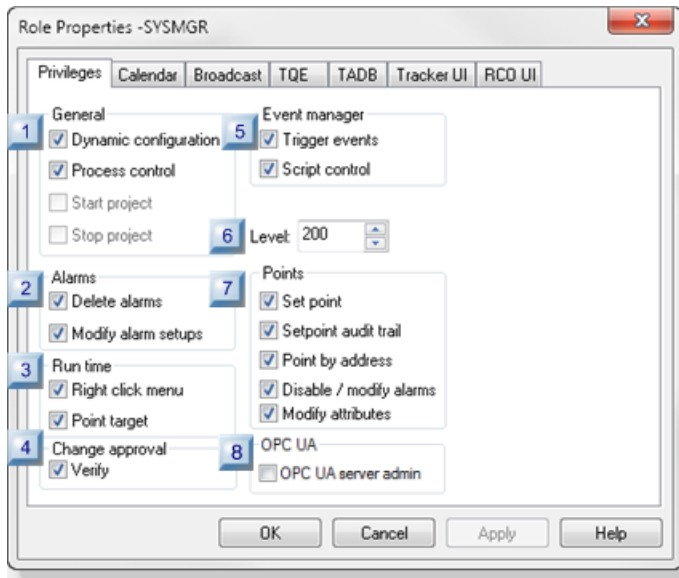
Step	Description
	General.
	Alarms.
	Runtime.
	Change approval.
	Event manager.
	Level.
	Points.
	OPC UA.

1. General

Check the check box for each privilege you want to assign to a role.

Privilege	Description
Dynamic configuration	Enable Dynamic Configuration from functions in the Workbench.
Process Control	Use the CPC (CIMPLICITY Program Control) utility to start and stop CIMPLICITY processes.
Start Project	Start a project.
Stop Project	Stop a project.

2. Alarms

Check the check box for each privilege you want to assign to a role.

Privilege	Description
Delete alarms	Delete alarms from the Alarm Viewer.
Modify alarm setups	Modify alarm setups in Alarm Viewer.

3. Run time
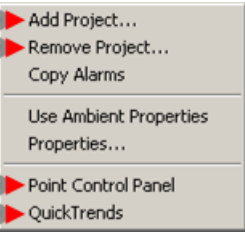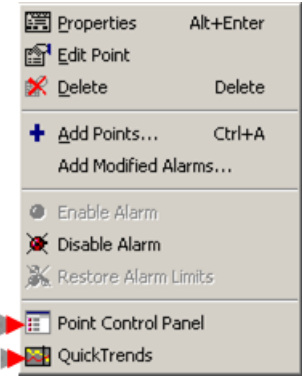
A role's ability to open processes through the following windows can be limited, based on whether or not you check **Right-click menu** and/or **Point Target**.

- Alarm Viewer OCX
- CimView (including Point View)
- Point Control Panel
- System Sentry

Richt-click menu

Right-click menu authorizes the role to display Popup menus, as follows.

Item	Description	Menu
Alarm Viewer OCX		

Item	Description	Menu
Checked	A Popup menu displays. Processes that can be opened through the Popup menu include: • Add a project. • Remove a project. • Open the Point Control Panel. • Open a quick trend. 📋 **Note:** Point Target must also be checked for Point Control Panel and quick trend.	Add Project... Remove Project... Copy Alarms Use Ambient Properties Properties... Point Control Panel QuickTrends
Clear	No Popup menu displays.	
CimView		
Checked	A Popup menu displays. Processes that can be opened through the Popup menu include: • Open a Point View window. • Open the Point Control Panel. • Open a quick trend. 📋 **Note:** Point Target must also be checked for Point Control Panel and quick trend.	✓ Menu Full Screen Point View Point Control Panel QuickTrends Help Properties
Clear	No Popup menu displays.	
Point Control Panel		
Checked	A Popup menu displays. Processes that can be opened through the Popup menu include: • Open an additional Point Control Panel that displays selected points. • Open a quick trend. 📋 **Note:** Point Target must also be checked for Point Control Panel and quick trend.	Properties Alt+Enter Edit Point Delete Delete Add Points... Ctrl+A Add Modified Alarms... Enable Alarm Disable Alarm Restore Alarm Limits Point Control Panel QuickTrends
Clear	No Popup menu displays.	

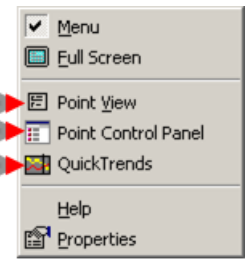📋 **Note:** System Sentry displays Popup options the same as other CimView screens.

⚠️ **Important:** If you are connected to multiple projects, e.g. through the Point Control Panel, you can display the Popup menu only if your role is authorized to do so in all of the projects.

For projects that are in CIMPLICITY versions less than 7.0, the authorization is assumed to be True.
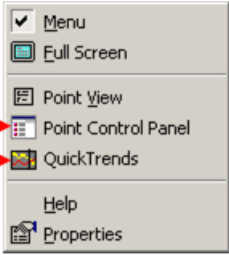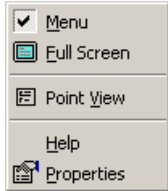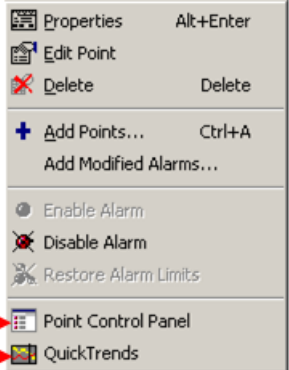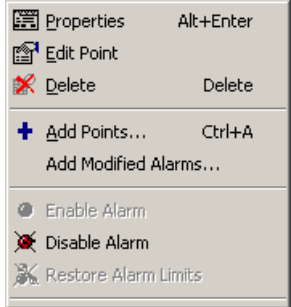
Point target

Checking **Point target** enables users to display the Point Control Panel and Quick Trends.

Popup menus and toolbar buttons that provide access to these features display based on whether **Point target** is checked or clear are as follows.

- When **Point target** is checked Point Control Panel and QuickTrends are listed on the right-click Popup menus in:
    ◦ Alarm Viewer OCX
    ◦ CimView
    ◦ Point Control Panel
    ◦ System Sentry

    📋 **Note: Right-click menu** must also be checked.

Point target Checked	Clear
CimView	
Point Control Panel	

- When **Point target** is checked **Point Control Panel** and **Quick Trends** buttons display on the Point View toolbar when Point View *(page   )* is opened through a CimView screen.

Point target Checked	Clear
Point View	
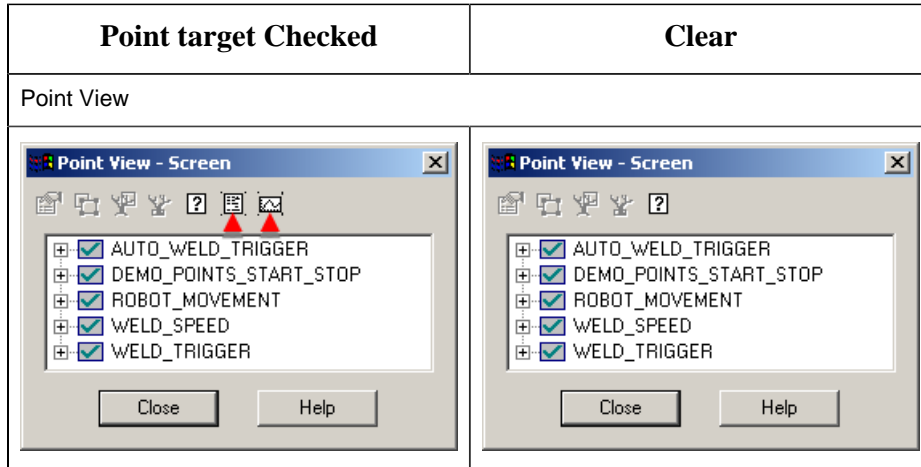
4. Change approval

Privilege	Description
Verify	Electronically verify a setpoint action for points and/or alarms that require electronic signatures for both the setpoint performer and a verifier.

5. Event Manager

Privilege	Description
Trigger Event	Trigger Event Manager events from the Basic Control Engine user interface.
Script Control	Stop, pause, or resume scripts in the Event Manager from the Basic Control Engine user interface.

6. Level

Enter a number to indicate the level at which the role can set points.

Level security affects all writable attributes of the point, including alarm limits, quality attributes, raw value, etc.

Each point can be assigned a level on the advanced General tab in the Point Properties dialog box. A role with a level equal to or higher than a point level can set the point.

The SYSMGR role:

- Has been assigned a level of 100.
- Can set any points with a level that is lower or equal to 100.

The OPER role:

- Has been assigned a level of 10.

• Can set any points with a level that is lower or equal to 10.

7. Points

Privilege	Description
Set point	Perform setpoints from CimView screens that contain Setpoint actions.
Setpoint Audit Trail	Have a $DOWNLOAD event recorded in the Event Log for each setpoint that is generated. When you enable the Setpoint Audit Trail, the information sent to your Event Log can provide a detailed audit trail of which users set which setpoints. However, the audit trail imposes significant overhead (20 times slower) since a record is logged in the database for each setpoint. This is particularly noticeable when a user performs setpoints in a loop in the Program Editor. If you do not require an audit trail for setpoints, it is recommended that you disable the **Setpoint Audit Trail** option. 📝 **Note:** The audit trail logs data in device units. You can use the global parameter **EU_AUDIT_TRAIL** to have CIMPLICITY log the data in EU and measurement unit converted values.

	Default	Disabled
Point by Address	Use point by address points in CimEdit expressions.	
Disable / modify alarms	Disable or modify a point's alarms in the Point Control Panel.	
Modify Attributes	Change the MANUAL_MODE point quality attribute. Change the QUALITY.DISABLE_WRITE point attribute. Write to a user defined field attribute if **Restrict write by role** is checked in the Field Attribute dialog box.	

8. OPC UA

Privilege	Description
OPC UA server admin	Select this option to allow an admin user to remotely manage the OPC UA security configuration for CIMPLICITY projects. This includes: configuring server certificates, updating trust lists, restarting the OPC UA Server, shutting down the OPC UA Server, and viewing diagnostic information about the OPC UA Server. When you select this option, you will need to restart your CIMPLICITY project.
	Default	Disabled

Option 2.2. Assign Role Calendar Privileges

The Calendar tab in the Role Properties dialog box is available if your CIMPLICITY product has the Action Calendar option enabled.

Check the check box for each privilege you want to assign to a role.
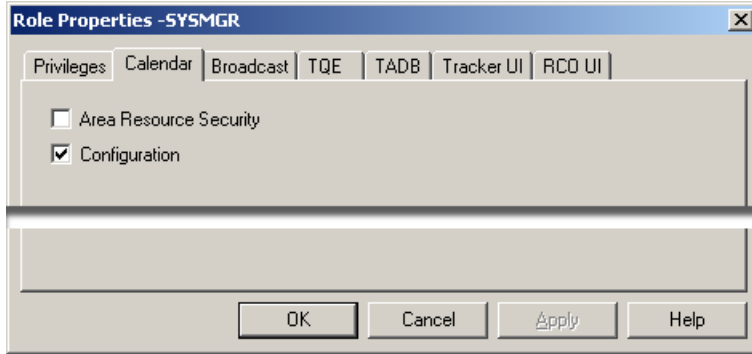
Privilege	Option	Description
Area Resource Security	Checked	Only see areas whose Resource ID is assigned to the user
	Unchecked	See all areas.
Configuration	Checked	Configure a schedule for any areas that can be seen
	Unchecked	View schedules, but no configuration is possible.

Option 2.3. Assign Role Configuration Privileges

⚠️ **Important:** You need to activate configuration security to display the Configuration tab in the Role Properties window. Configuration security will require users to logon to a CIMPLICITY project. Therefore, their privileges will be affected by the roles to which they are assigned.

You activate security by selecting the Configuration Security check box in the Options tab of the Project Properties window. The Configuration tab in the Role Properties window enables you to specify the type of configuration privileges available to users who are assigned to the role. Select the check box for each privilege you want to assign to a role.
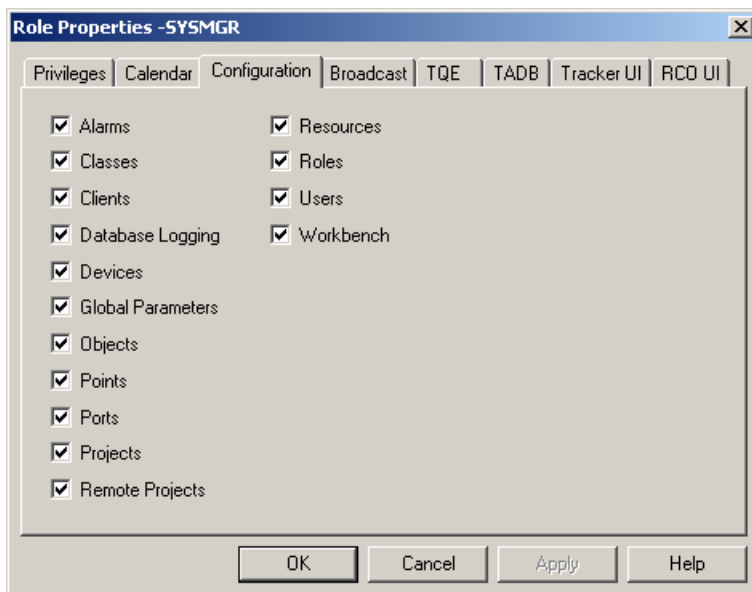
📄 **Note:** If you clear the Alarms check box and select the Points check box, you cannot configure and modify alarms from Alarm Navigation. However, since you have the privilege to create points, you can configure and modify alarms from the Point Properties window.

Option 2.4. Assign Role Broadcast Privileges

The Broadcast tab in the Role Properties dialog box is available if your CIMPLICITY product has the Order Execution Mgt. Broadcast option enabled.

Check the check box for each privilege you want to assign to a role.
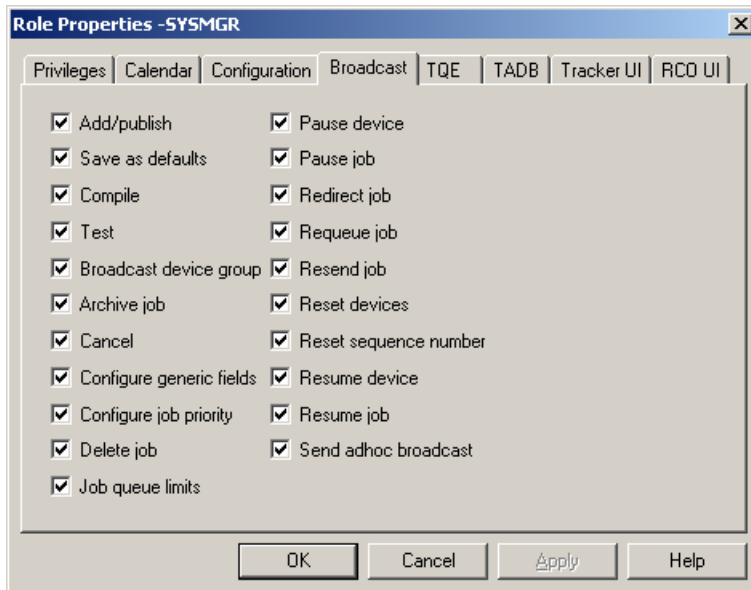
Privilege	Description
Add/Publish	Add/publish a WYSIWYG, ASCII or Control Character Token (CCT) form to the list of available Broadcast forms.
Save As Defaults	Save WYSIWYG form object configurations as defaults for objects that are placed on a form after the defaults are saved.
Compile	Compile a Control Character Token file, ASCII form or WYSIWYG form.
Test	Test an ASCII or WYSIWYG form with data to make sure it has the correct layout and configuration.
Broadcast device group	Configure a Broadcast device group
Archive job	Archive a job from the history queue.
Cancel	Cancel a job.
Configure generic fields	Configure job fields in the Broadcast Queue Manager.

Privilege	Description
Configure job priority	Specify priority among the following job types. • Ad Hoc broadcast • Redirect • Resend • Normal broadcast • Test broadcast
Delete job	Delete jobs in the Broadcast Queue Manager.
Job Queue limits	Set queue limits in the Broadcast Queue Manager.
Pause device	Pause a device in the Broadcast Queue Manager
Pause job	Pause selected active jobs that are in the Broadcast Queue Manager printing queue.
Redirect job	Redirect selected jobs in the Broadcast Queue Manager
Requeue job	Re-queue selected archived jobs in the Broadcast Queue Manager
Resend job	Resend selected history jobs in the Broadcast Queue Manager
Reset devices	Reset devices, after they have been paused, so the Broadcast Queue Manager will send them forms.
Reset sequence number	Reset the device group sequence number in the Broadcast Queue Manager.
Resume device	Resume a device after it has been paused in the Broadcast Queue Manager.
Resume job	Resume printing of jobs that have been paused in the Broadcast Queue Manager.
Send adhoc broadcast	Send an adhoc broadcast through the Broadcast Queue Manager.

Option 2.5. Assign Role Query Engine Privileges

The TQE tab in the Role Properties dialog box is available if your CIMPLICITY product has the Order Execution Mgt. Query Engine option enabled.

Check the check box for each privilege you want to assign to a role.

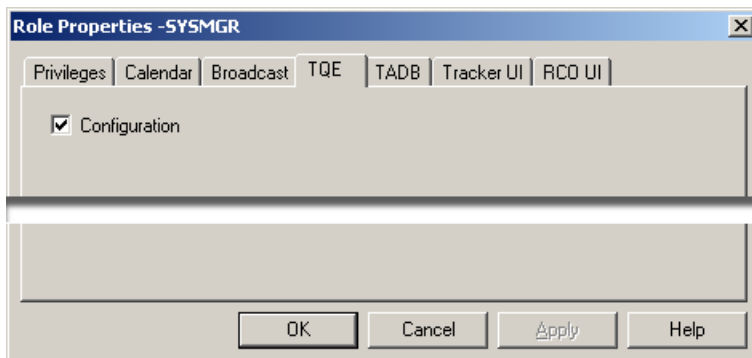| Privilege	Description
Configuration	Create or modify expressions.

Option 2.6. Assign Role TADB Privileges

The TADB tab in the Role Properties dialog box is available if your CIMPLICITY product has the Order Execution Mgt. TADB option enabled.

Check the check box for each privilege you want to assign to a role.
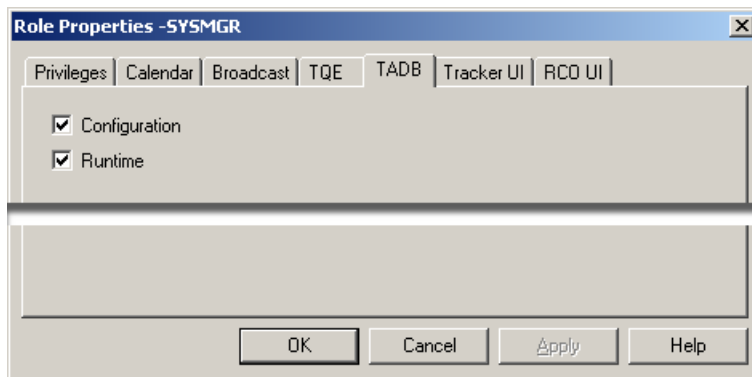
Privilege	Description
Configuration	Create or modify Tracker item types, groups and/or attributes in the TrackerCfg UI
Runtime	Create or modify attributes in the PRT UI or through a CimView screen.

Option 2.7. Assign Role Tracker UI Privileges

The Tracker UI tab in the Role Properties dialog box is available if your CIMPLICITY product has the Tracker option enabled.

- Privileges that can be assigned to a role.
- Role privileges and scripting for PRT_UI

Note: In some versions previous to CIMPLICITY v7.0, Role privileges for Tracker UI and RCO UI were incorrectly recorded. This has been corrected in CIMPLICITY 7.0. However, it would be prudent to double-check that the privileges have are correctly checked or clear for each role.

Privileges that can be Assigned to a Role

Check the check box for each privilege you want to assign to a role.

Disabling privileges applies to GE Digital client applications.
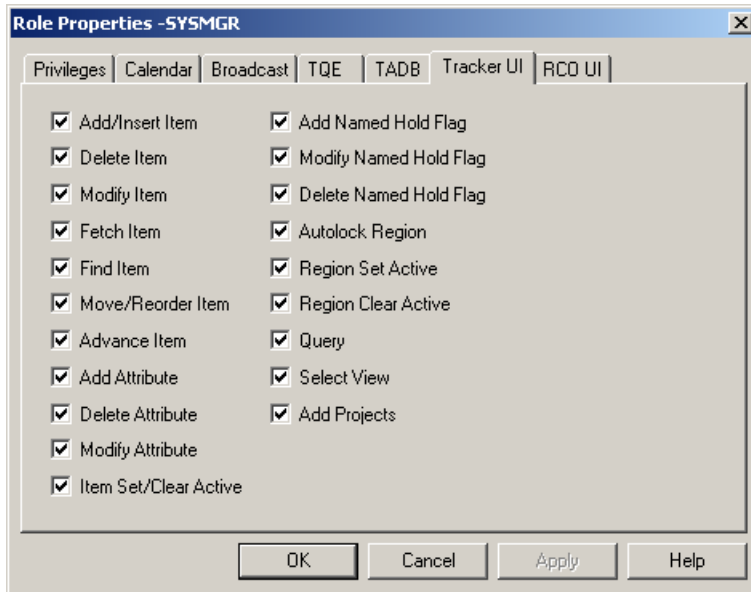
rect 22, 63, 126, 82 *(page 25)*
rect 22, 82, 127, 101 *(page 25)*
rect 21, 103, 124, 126 *(page 26)*
rect 21, 125, 128, 153 *(page 26)*
rect 21, 152, 126, 173 *(page 26)*
rect 23, 172, 146, 197 *(page 26)*
rect 21, 196, 144, 222 *(page 26)*
rect 20, 220, 143, 242 *(page 26)*
rect 21, 239, 142, 266 *(page 26)*
rect 22, 266, 140, 287 *(page 26)*
rect 25, 285, 151, 314 *(page 26)*
rect 159, 56, 300, 84 *(page 26)*
rect 158, 82, 301, 107 *(page 26)*
rect 159, 107, 303, 132 *(page 26)*
rect 159, 132, 302, 154 *(page 26)*
rect 160, 154, 299, 177 *(page 26)*
rect 160, 176, 298, 199 *(page 26)*
rect 161, 196, 299, 222 *(page 26)*
rect 162, 220, 297, 242 *(page 26)*
rect 162, 241, 298, 268 *(page 26)*

Privilege	Description
Add/Insert Item	Add or Insert an item to a region.
Delete Item	Delete an item into a region.

Privilege	Description
Modify Item	Modify an item into a region. Important: If you clear Modify Item the following privileges will also be unavailable (even if they are checked in the Roles Properties dialog box). • Add Attribute • Delete Attribute • Modify Attribute • Item Set/Clear Active
Fetch Item	Fetch an item.
Find Item	Find an item in the PRT database using the PRT_UI
Move/ Reorder Item	Move or Reorder an item to another region using the PRT_UI.
Advance Item	Advance an item to the next region using the PRT_UI.
Add Attribute	Add a PRT standard or extended attribute.
Delete Attribute	Delete a PRT standard or extended attribute.
Modify Attribute	Modify a PRT standard or extended attribute.
Item Set/ Clear Active	Activate or de-activate an item's status in a region, e.g. delayed, external hold, internal hold and normal.
Add Named Hold Flag	Add named hold flags through Object Model scripting
Modify Named Hold Flag	Modify named hold flags through Object Model scripting
Delete Named Hold Flag	Delete named hold flags through Object Model scripting.
Autolock region	Automatically lock the region so you can perform operations on items within the region whenever you want.
Region Set active	Activate a region's status.
Region Clear active	De-activate a region's status.
Query	NA
Select View	Select a configured view.
Add Projects	Connect to multiple projects.

Role Privileges and Scripting for PRT_UI

Scripts can be written to automate activity in the PRT_UI, e.g. add attributes to blocks, set or clear an internal hold.

- When the script is run the first time it adheres to the role privileges that have been set in the Roles dialog box.
- When the script has run once in the CimBasic Editor it is added to the cache. Even if the role privileges are changed dynamically, the script will continue to run as written adhering to the role privileges that were assigned when it was first run. While the script is in the cache, it does not honor the dynamically changed role privileges.

A script is written that includes Modify Named Hold Flag.

Dynamic configuration is on while the project is running.

The Modify Named Hold Flag privilege is removed dynamically.

The script will continue to perform Modify Named Hold Flag, as specified, while it is in the cache.

Option 2.8. Assign Role RCO UI Privileges

The RCO UI tab in the Role Properties dialog box is available if your CIMPLICITY product has the Tracker RCO UI option enabled.

Check the check box for each privilege you want to assign to a role.

📝 **Note:** In some versions previous to CIMPLICITY v7.0, Role privileges for Tracker UI and RCO UI were incorrectly recorded. This has been corrected in CIMPLICITY 7.0. However, it would be prudent to double-check that the privileges have are correctly checked or clear for each role.

Each of these features has a related menu item in the RCO_UI, which will be disabled if the corresponding check box is clear.
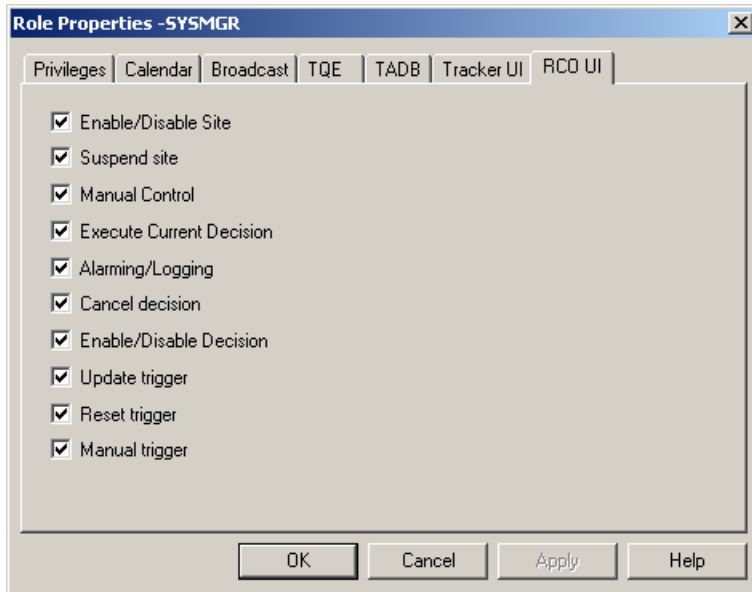
rect 21, 59, 147, 85 *(page 28)*
rect 20, 85, 147, 105 *(page 28)*
rect 22, 104, 146, 128 *(page 28)*
rect 23, 129, 171, 154 *(page 28)*
rect 25, 152, 169, 177 *(page 28)*
rect 24, 174, 168, 198 *(page 28)*
rect 26, 197, 171, 222 *(page 28)*
rect 25, 223, 166, 244 *(page 28)*
rect 23, 243, 164, 264 *(page 28)*
rect 19, 263, 164, 287 *(page 28)*

Privilege	Description
Enable/Disable site	Enable or Disable control sites.
Suspend site	Suspend control sites.
Manual Control	Perform manual decisions.
Execute Current Decision	Complete current decisions.
Alarming/Logging	Set alarming and logging through the RCOUI
Cancel decision	Cancel RCO decisions.
Enable decision	Enable or Disable manual control decisions.
Update trigger	Refresh the status of triggers.
Reset trigger	Reset triggers manually.
Manual trigger	Manually trip a trigger.

Chapter 4. User Configuration

About Users

The Users application enables you to configure users for your CIMPLICITY project.

A User is an individual person working with a CIMPLICITY project.

The privileges and resources that CIMPLICITY offers a user is determined by one of the following.

Windows Authentication
Authenticated Windows groups can be selected and assigned roles and resources.

CIMPLICITY verifies the user's Windows password to allow access.

CIMPLICITY user configuration

A user can be created in CIMPLICITY and assigned a password, roles and resources.

📝 **Note:** The first user you create when starting a new project is assigned the SYSMGR role. Beginning with CIMPLICITY 9.5, this user must be assigned a password. See About Cimplicity Passwords *(page 29)* for details on password complexity.

The default user requires a password to access CIMPLICITY project functions.

⚠️ **Important:** CIMPLICITY does not support Windows XP Fast user Switching.

About CIMPLICITY Passwords

Beginning in CIMPLICITY 9.5, the user with the SYSMGR role can determine whether or not passwords are case-sensitive. If you choose case sensitivity, the system will not recognize apple123, APPLE123 and ApplE123 as the same password. When setting up a new project carefully consider if you want the passwords for the project to be case-sensitive or case-insensitive. Switching between the two can cause complications once you have built a project and assigned multiple user roles, user names, and passwords.

Note the following about CIMPLICITY passwords:

- Password complexity rules are set for the entire project, not on a user-by-user basis.
- Case-sensitive passwords must have a least one uppercase letter and one lower case letter.

- If you have a project that has case-insensitive passwords and you change the project to case-sensitive passwords, those existing passwords must now be entered in all uppercase letters. Numerals and special characters do not change.
- When creating a project and creating user accounts, you must assign each account a password. However, when logging in at a later time with SYSMGR privileges, you can create new users without passwords. This is not recommended.
- If you set up a project with case-sensitive passwords and then change to case-insensitive passwords, your existing mixed case passwords must be entered in mixed case as they were originally created. However, any new passwords you create are case insensitive.
- It may be best to leave already existing projects with case-insensitive passwords.

Windows Authentication Configuration

Windows Authentication Configuration

Windows authenticated users can use their Windows user name and password when logging into CIMPLICITY if they are members of selected Windows groups.

Do the following to select and configure the groups that CIMPLICITY will use for authentication.
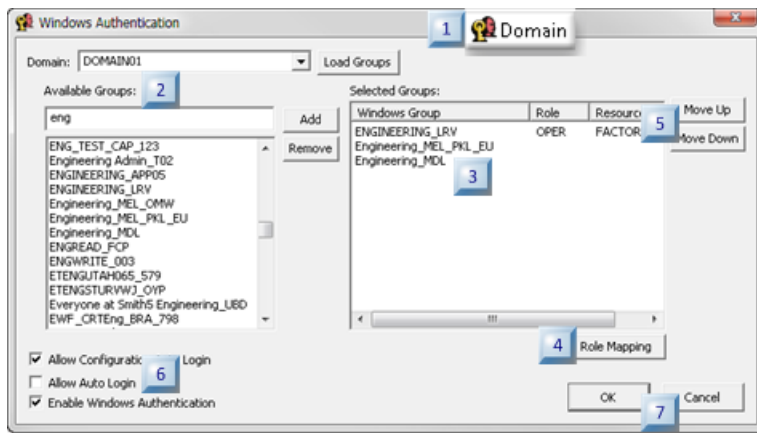
rect 81, 36, 110, 64 Step 2. List Groups in a Selected Domain *(page 32)*
rect 81, 213, 110, 241 Step 6. Enable Automatic Log Ins *(page 37)*
rect 259, 0, 288, 28 Step 1. Open the Windows Authentication Window *(page 31)*
rect 276, 91, 305, 119 Step 3. Select Groups that will be Authenticated for CIMPLICITY *(page 34)*
rect 394, 57, 423, 85 Step 5. Prioritize Groups *(page 36)*
rect 331, 194, 360, 222 Step 4. Map a Role for each Group *(page 35)*
rect 393, 238, 422, 266 Step 7. Save or Cancel the Windows Authentication Configuration *(page 40)*

Step	Description
	Open the Windows Authentication window.
	List Windows groups in a selected domain.
	Select groups that will be authenticated for CIMPLICITY.
	Map a role for each group.
	Prioritize groups.
	Enable automatic log ins.
	Save or Cancel the Windows Authentication Configuration

Step 1. Open the Windows Authentication Window

1. Select Project>Security>Domain in the Workbench left-pane.

2. Select **Domain** in the right-pane.

3. Do one of the following.

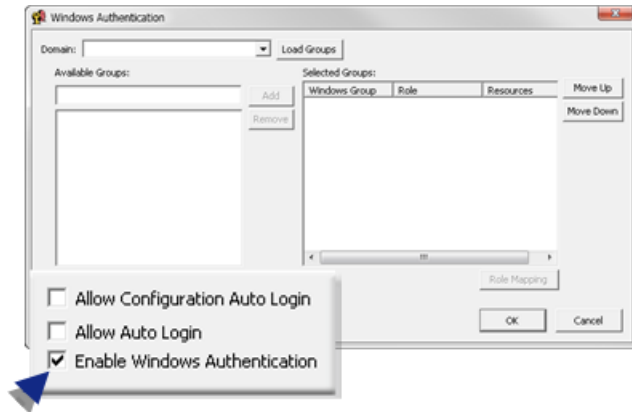| Action	Description
A	Click Edit>Properties on the Workbench menu bar.
B	Click the Properties button on the Workbench toolbar.
C	In the Workbench left-pane either double-click **Domain**, or right-click **Domain** and select Properties on the popup menu.
D	In the Workbench left-pane either double-click **Domain**, or right-click **Domain** and select Properties on the popup menu.
E	Press Alt+Enter on the keyboard.

The Windows Authentication window opens when you use any method.

Step 2. List Groups in a Selected Domain

• Enable Windows Authentication
• Load Groups: In a Selected Domain
• Load Groups: Guidelines

Enable Windows Authentication

Check Enable Windows Authentication.

Load Groups: In a Selected Domain

Do the following.
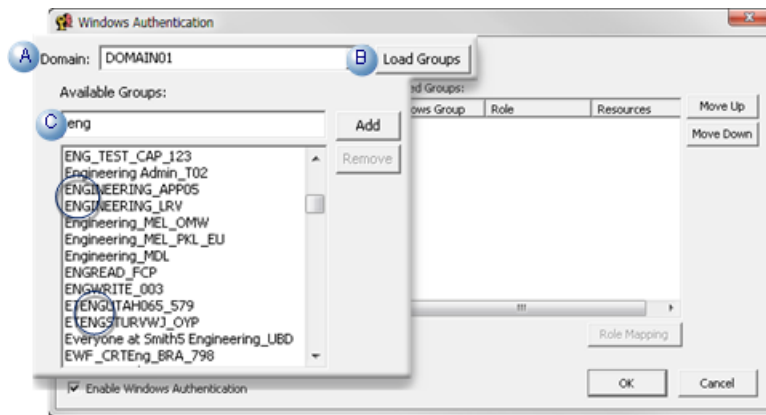
Item	Name	Description
A	Domain	Select a domain from the drop-down list.
B	Load Groups	Click **Load Groups**. Domain groups are listed in the **Available Groups** box.
C	Available Groups	(Optional) Enter a string in the field to list only groups that contain the string in some part of the name.

Windows users groups that have been defined for the selected domain are listed in the Available Groups list. If a string has been entered to filter the list, only the groups that include the string are listed.

Load Groups: Guidelines

You must have a valid domain User name/Password to list a domain's groups.

If you have not logged into windows with a valid domain username/password,
a Windows Authentication error message box opens reporting the issue, as
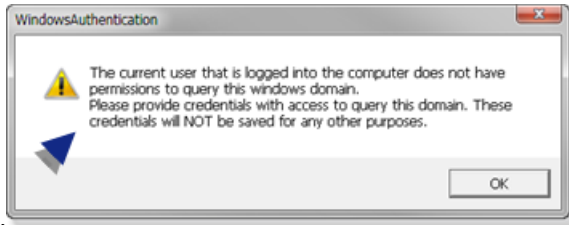
follows.

The current user that is logged into the computer does not have permission to query the windows
domain.

Please provide credentials, with access to query the domain. These credentials will NOT be saved for
any other purpose.

1. Select **OK**.
   The **Windows Authentication** error message window closes. A **Login** window opens.

2. Enter valid **Username** and **Password** credentials for the selected domain.

3. Select **OK**.
   The following occurs based on whether or not the entered domain login credentials are valid.

Login	Result
Valid	The domain's available groups are listed.
Invalid	a. An error message reports that the login is invalid. b. A blank **Login** window opens. 📝 **Note:** Select **Cancel** if you do not have valid login credentials.

- The speed at which the groups load depends on the domain size and your network speed.
- While CIMPLICITY is loading the groups, the window will be gray.

Step 3. Select Groups that will be Authenticated for CIMPLICITY

Available Groups

1. Select an available group.

2. Select **Add**.
   The group is added to the selected groups list.

Selected Groups

1. Select a selected group.

2. Select **Remove**.
   The group is removed from the Selected Groups list.

Step 4. Map a Role for each Group

1. Select a group in the Selected Groups list.

2. Click **Role Mapping**.
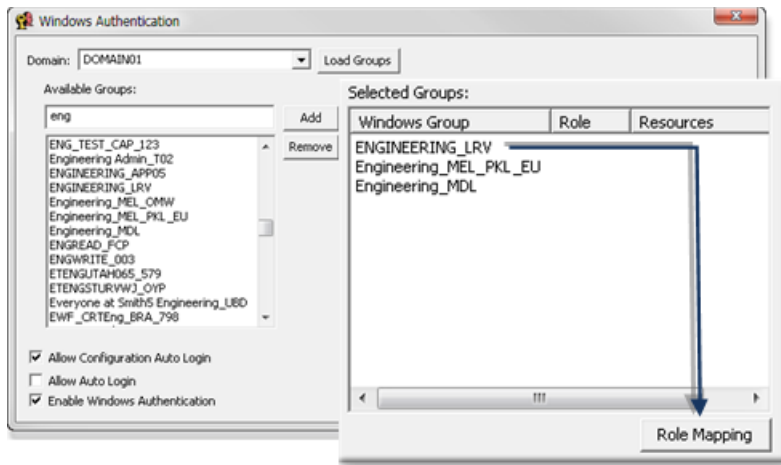
A Mapping dialog box opens displaying the roles that are currently in the project configuration.

3. Do the following.
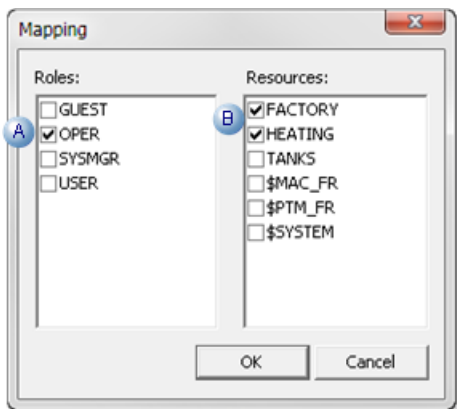
   a. Check one role.
   b. Check the resources to which the role will have access.

4. Click one of the buttons:

Name	Description
OK	Saves your selections
Cancel	Cancels the selections or changes to an existing group

The Mapping dialog box closes. The Role and resource selections are listed in the Windows
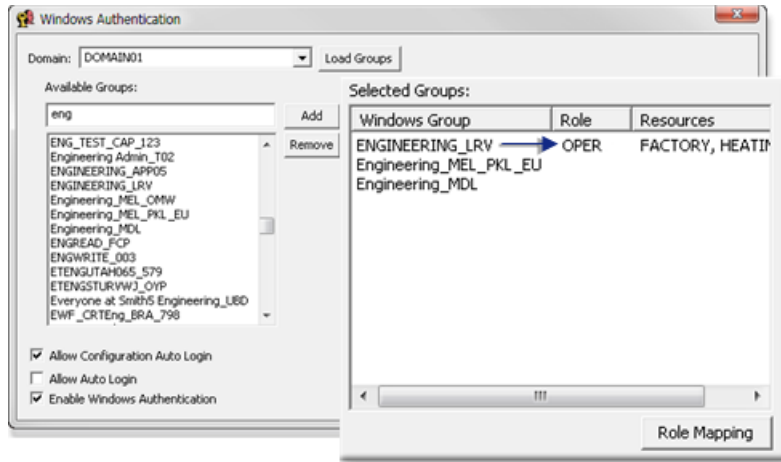
group's row.

Step 5. Prioritize Groups

Users can belong to more than one Windows group.

CIMPLICITY:

- Looks for the user starting with the first group in the Selected Groups list and moving down.
- Assigns the role/resources to the user that are assigned to the first group in which the user is found.

List the groups in the order of priority; the first group is the highest priority.

Select a group and click **Move Up** or **Move Down** to change its order in the list.

Step 6. Enable Automatic Log Ins

Windows authentication can be enabled or disabled whether or not Windows groups have been selected in the Windows Authentication window.

Enable/Disable Windows Authentication

The following steps describe how to enable Windows Authentication in CIMPLICITY, and the options available when you do (**Allow Configuration Auto Login** and **Allow Auto Login**).
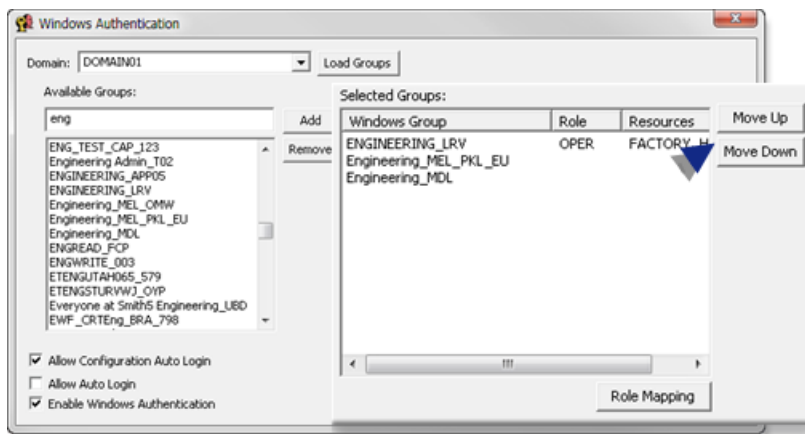
1. Open the Windows Authentication dialog box.

2. Select **Enable Windows Authentication**.
   The following options become available: **Allow Configuration Auto Login** and **Allow Auto Login**.

   📝 **Note:** If only **Enable Windows Authentication** is selected and if the Windows user is a member of a selected group, CIMPLICITY will:
   - Open a CIMPLICITY Login dialog box.
   - Check the Windows/password credentials.
   - Look for the user in the Selected Groups.
   - Give the user CIMPLICITY/Proficy Change Management (PCM) access based on the first group in which the user is found.

3. Select one of the following configurations:

Allow Auto Login	Allow Configuration Auto Login	Description
Checked	Clear	If the Windows user is a member of a selected group, CIMPLICITY will: • Look for the user in the Selected Groups. • Automatically log in the user to CIMPLICITY based on the first group in which the user is found. • Assign the user the role/ resources assigned to that group. Users have to manually log into CIMPLICITY to do configuration if CIMPLICITY Configuration Security is enabled and to manually log into Proficy Change Management (PCM). Users have to: • Manually log into CIMPLICITY to do configuration if CIMPLICITY Configuration Security *(page)* is enabled. • Manually log into Proficy Change Management
Checked	Checked	Users can potentially be automatically logged into: • CIMPLICITY configuration. • CIMPLICITY runtime. • Proficy Change Managements (PCM) projects.

Allow Auto Login	Allow Configuration Auto Login	Description

Clear	Checked	When Windows Authentication is enabled, Windows Authentication:
		• Reads the current logged in Windows user.
		• Does the following if the user is new to CIMPLICITY/not listed in the project:
		  ◦ Prompts the user for a CIMPLICITY valid name/password.
		  ◦ Creates a CIMPLICITY user based on the valid name/password.
		  ◦ Assigns the user the role/resources assigned to the Windows Authentication group that the user is in.
		  ◦ Automatically logs the user into CIMPLICITY based on the first Windows Authentication group in which the user is found.
		  ◦ Automatically logs the user into CIMPLICITY based on the first Windows Authnetication group in which the user is found.
		Users are:
		• Automatically logged into CIMPLICITY to do configuration even if CIMPLICITY Configuration Security *(page)* is enabled.
		
		A failure message may display for a user who does not have Workbench privileges; a Configuration Login dialog box will open to prompt the user for valid credentials.
		
		A Valid user can enter either of the following in the Configuration Login dialog box:
		  ◦ `<domain>/<username>`
		  ◦ `<username>`
		• Automatically logged into a Proficy Change Management (PCM) project.
		  ◦ The automatic logon applies only to PCM project properties, not to PCM computer properties.
		  ◦ An automatic PCM logon can occur based on selections in the Project Properties dialog box>Change Management tab:
		    ▪ As soon as the Workbecnh starts up if **Logon at Workbench startup** is checked.
		    ▪ If **Prompt for user name and password**

Windows Authentication Guidelines

- When a user:
  - ◦ Attempts to log into CIMPLICITY, if the Windows user name/password are not valid or CIMPLICITY does not find the user in any of the groups, the user is denied CIMPLICITY access.
  - ◦ Logs into CIMPLICITY for the first time using Windows authentication, that user is automatically added to CIMPLICITY's list of users.
  - ◦ Is listed in the CIMPLICITY list, user specifications can be modified the same way as for any other user.
- When the new Windows Authentication module tries to validate a user with auto log in, If Windows Authentication does not have a valid user/password to use to query the domain controller, it uses the current user that the process is running under.

  On a default installation Windows authentication runs as a system user; depending on how the domain is set up there is a good chance that the system user will not have the ability to query the domain.

  To make sure Windows authentication can query the domain:

1. Open the Services control panel.
2. Make the CIMPLICITY HMI service run under a domain account that has privileges to query the domain.

Step 7. Save or Cancel the Windows Authentication Configuration

Click one of the following in the Windows Authentication window.

Button	Description
OK	• Saves this session's configuration • Closes the Windows Authentication window.
Cancel	• Cancels this session's configuration • Closes the Windows Authentication window. **Note:** If Windows Authentication was previously configured, the previous configuration is used.

User Configuration

User Configuration

User configuration steps

The following steps describe how to enter specifications for a user.

1. Open a **User Properties** window. *(page 42)*
2. Configure user general (security) properties. *(page 44)*
3. Configure user resource availability. *(page 47)*

Review existing users

1. To review exiting users, expand the Security folder in the left pane of the Workbench.

2. Select **Users**.
   The Workbench right pane can display the following attributes for each
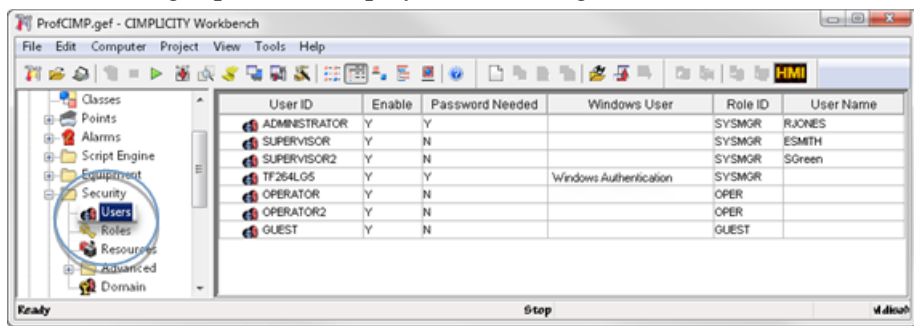
User.

Attributes	Description
User ID	A name that uniquely identifies each user.
Enable	Indicates if the account is enabled or disabled.
Password Needed	If a password is needed for the selected user.
Windows User	Identifies users who are authorized by Windows authentication.
Role ID	The role assigned to the user. This determines the privileges assigned to the user.
User Name	The user's name.

📝 **Note:** Use the Workbench Field Chooser to remove or re-display any of the fields, except the User ID. The User ID is required.

The User list is initially sorted by User ID. You can click any of the other column titles at the top of the list to sort the list by that attribute.

Step 1. Open a User Properties Dialog Box

Step 1. Open a User Properties Dialog Box

You can begin user configuration by:

	Create a new user.
	Open the Properties dialog box for an existing user.

Option 1.1. Create a New CIMPLICITY User

• New CIMPLICITY user
• New Windows authenticated user

📄 **Note:** Beginning with CIMPLICITY 9.5, you must assign a user name to the first user you create when beginning a new project. This first user is assigned to the SYSMGR by default. By default, the SYSMGR role is granted the most privileges.

New CIMPLICITY User

1. To add a new user, select **Project>Security>Users** in the Workbench left pane.
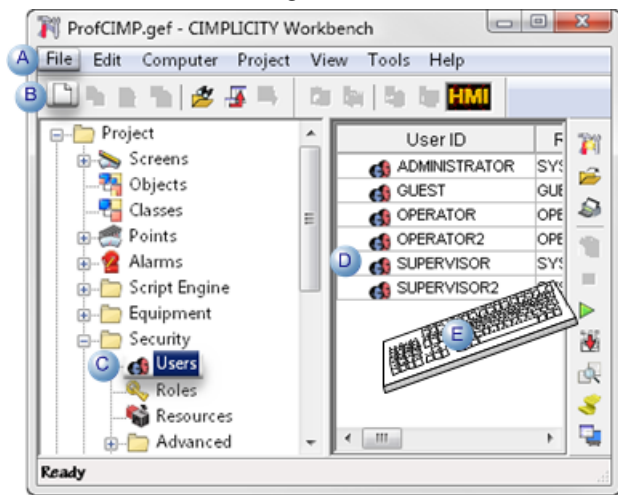
2. Do one of the following.

Action	Description
A	Click File>New on the Workbench menu bar.
B	Click the New Object button on the Workbench toolbar.
C	In the Workbench left pane, either double-click **Users**, or right-click **Users** and select New on the Popup menu.

D	In the Workbench right pane:
	  a. Right-click any user.
	  b. Select New on the Popup menu.

E	Press Ctrl+N on the keyboard.

The New User dialog box opens when you use any method.

3. Enter the name of the new user in the **User ID** field.

⚠️ **Important:** CIMPLICITY user ID's can be 32 characters, however, Change Management limits user ID's to 20 characters. If your project and/or system uses Change Management and If the same user ID's will be used for CIMPLICITY and Change Management, limit the length to 20 characters.

4. Click **OK**.
   The system verifies that the User ID does not already exist, and that no invalid characters have been used. The User Properties dialog box opens is the User ID is approved.

New Windows Authenticated User

1. Enable *(page 37)* and configure *(page 30)* Windows Authentication.
   CIMPLICITY adds an authenticated user to the CIMPLICITY user list after the first log in.

2. Open the Properties dialog box for the existing *(page 43)* user.

Option 1.2. Open a Properties Dialog Box for an Existing User

CIMPLICITY provides several methods to open an existing **User Properties** window.

1. Select **Project>Security>Users** in the Workbench left pane.

2. Select a user in the Workbench right pane.
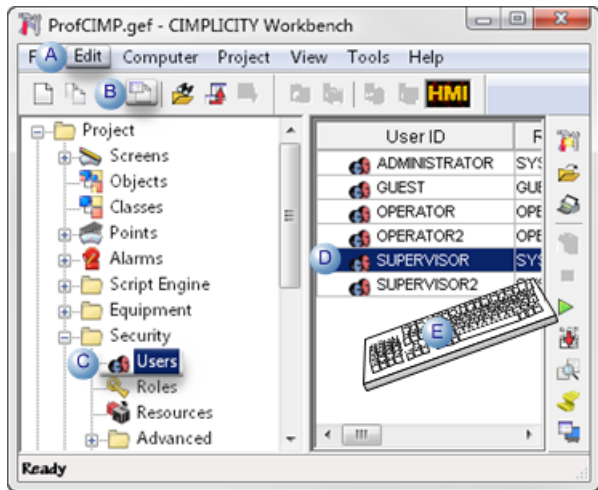
3. Do one of the following.

Action	Description
A	Click Edit>Properties on the Workbench menu bar.
B	Click the Properties button on the Workbench toolbar.
C	In the Workbench left pane: a. Right-click **Users**. b. Select Properties on the Popup menu.
D	In the Workbench right pane, either double-click a user or right-click a user and select Properties on the popup menu.
E	Press Alt+Enter on the keyboard.

A User Properties dialog box associated with the selected user opens when you use any method.

Step 2. Configure User General Properties

The **General** tab on the **User Properties** dialog box lets you define the following for a new user:

1. Role
2. Authentication Type
3. Password/Confirm password
4. User name
5. Enabled
6. Password expires

📄 **Note:** If you change a user's configuration dynamically, the user must log out then log back in for the changes to take effect.

rect 120, 230, 346, 274 *(page   )*
rect 1, 231, 122, 275 *(page   )*
rect -2, 188, 360, 232 *(page   )*
rect 67, 112, 349, 184 *(page   )*
rect -1, 85, 354, 114 *(page   )*
rect -2, 52, 353, 87 *(page   )*

Role

1. Select ![icon] to the right of the input field to display the **Select A Role** window and use it to select the role.

2. **Optional:** Select ![icon] to create a new role, edit the current role, or browse for another role.

Authentication Type

Select one of the following procedures that CIMPLICITY should perform to authenticate a user when the user logs in:

Selection	CIMPLICITY allows access
None	With no password.
CIMPLICITY	When the user enters the name and password that are in the Users dialog box.
	The user's role and other specifications are also defined.

Selection	CIMPLICITY allows access
Windows Domain	Available when both: • The user is a member of a selected Windows Authentication group. • Enable Windows Authentication is checked in the Windows Authentication window. The user's assigned role and name may be different from the role assigned to the group.
Windows Domain with Group Mapping	Available when both: • The user is a member of a selected Windows Authentication group. • Enable Windows Authentication is checked in the Windows Authentication window. CIMPLICITY assigns the user a role for the first selected group in which the user is found.

Password and Confirm Password

1. When CIMPLICITY is selected as the Authentication Type, enter the user's password in the **Password** box.

   ⚠️ **Important:** The password length can be a maximum of 16 characters.

2. Re-enter the password in the **Confirm Password** box.
   Asterisks are displayed in place of the characters you type.

   The following runtime rules also apply to user passwords:

   During runtime, a user:

   • Is prompted to change the password when the current password expires.
   • Can change the password from the CIMPLICITY Login Panel.
   • Can use the Change Password command in the Basic Control Engine to change the password in CimView.
   • (In a Server Redundancy configuration) can only change the password when the Primary computer is running.

   The new password must comply with the password complexity rules (page 29) set up for the entire project.

   The user is not prompted to change his or her password at runtime when the following are selected as the Authenticated Type:

Selection	CIMPLICITY allows access when the user enters:
None	No password.
Windows Domain	The user's authorized Windows password.
Windows Domain with Group Mapping	The user's authorized Windows password.

User Name

Optional: Enter the user's name or descriptive text about the user.

Enabled

Either:

- • Check to enable the user account.
- • Clear to disable the account.

When **Enabled** is unchecked, the account is not available for user login.

📒 **Note:** If you disable an account dynamically, currently logged in users will not be logged out; however, new log in attempts will be rejected.

Password expires

Enter the number of days until the user's password expires.

📒 **Note:** Zero indicates that the password never expires.

After the elapsed number of days, the user will be required to change the password prior to logging in.

📒 **Note:** In a Server Redundancy configuration, automatic password expiration is not supported.

Step 3. Configure User Resource Availability

The Resources tab in the User Properties dialog box enables you to define the resources for which the user can view alarms. The resources currently assigned to the user are displayed on the Resources tab in the User Properties dialog box. You can add or remove resources for the selected user.

Add

1. Select a resource in the **Available** box.

2. Select **Add**.

The new resource moves to the **Configured** box.

Add All

Select **Add All**.

All the resources move to the **Configured** box.

Remove

1. Select a resource in the **Configured** box.
2. Select **Remove**.

The resource is removed back to the **Available** box.

Notes

- If you change a user's resources dynamically, the user must log out then log back in to access the changed resources.
- You can also use the **Shift** and **Ctrl** keys in combination with the mouse to select more than one resource for deletion.

User Runtime Properties

You can use the User Setup dialog box to change the runtime user log in properties in your project.

- Open the **User Setup** dialog box
- Configure user runtime account access
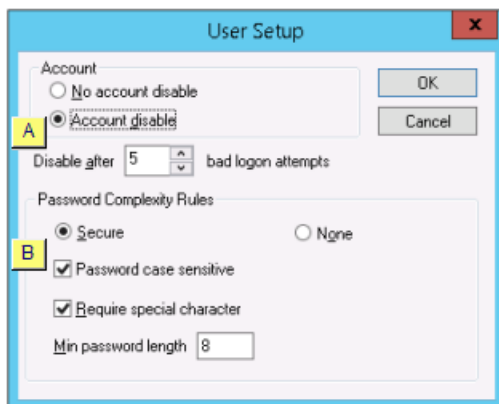
Open the User Setup dialog box

1. Do one of the following.
    - Select **Project > Properties** on the Workbench menu bar.
    - Select the **Project Properties**.
    The **Project Properties** dialog box opens.

2. Select the **Settings** tab.

3. Select **Users**.

4. Select **Settings**.
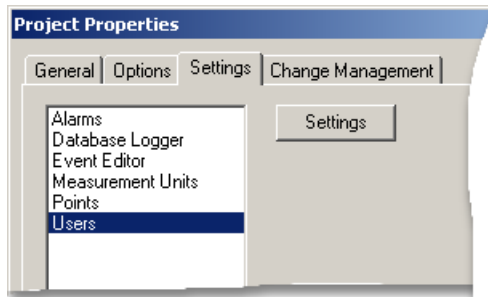
The **User Setup** dialog box opens.

Configure user runtime account access

- Automatic account disable
- Password Complexity Rules

Automatic account disable

CIMPLICITY can be configured to automatically disable a user account after a selected number of failed log in attempts.

Check one of the following.

- **No account disable**

  Disables automatic account disabling.

  Users will be allowed unlimited log in attempts.

- **Account disable**

  Enables:
  ◦ Automatic account disabling

◦ **Disable after n bad logon attempts** box.

Enter the number of log in attempts that can fail before CIMPLICITY disables the account.

Users will be allowed the specified number of log in attempts. If the number is exceeded CIMPLICITY disables the user account and generates a $LOGIN_FAILURES event.

To re-enable the account, the system administrator needs to dynamically re-enable the user account.

a. Select on the Workbench toolbar.
b. Open *(page 43)* the User's **User Properties** dialog box.
c. Re-enable *(page   )* the user account.

Note: Automatic account disabling is not supported on Servers using Server Redundancy.

Password Complexity Rules

Checked

When Secure is selected, CIMPLICITY will require users to create passwords with the rules you select:

- Password Case Sensitive
- Require Special Character
- Minimum Password Length

Chapter 5. Client Configuration

About Client Configuration

The Client Configuration utility enables you to configure default logins for CIMPLICITY Viewers on Client computers.

You can configure a CIMPLICITY Viewer on a Client computer to:

- Automatically log in to a Server project for specified users.
- Use the Windows Logon Username as the default user for logging in to a CIMPLICITY project.
- Only have access for an associated CIMPLICITY User ID if it has the correct Authorization Code.

Configure Client Properties

Configure Client Properties

CIMPLICITY provides you with several options for configuring client properties that enable you to restrict access from a client location.

Follow the procedures for these steps to configure client properties.

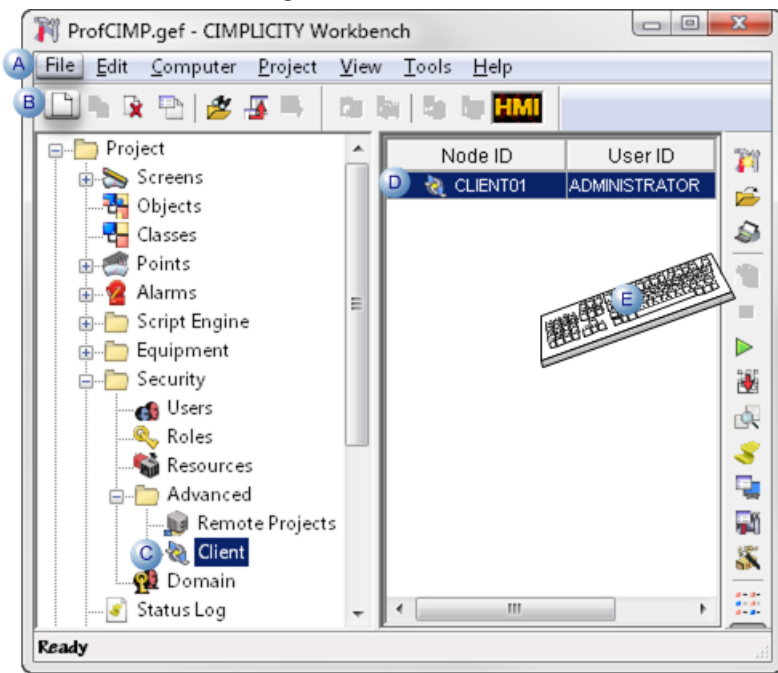| Step	Description
Step 1 (page 52)	Open a Node ID's Client Properties dialog box.
Step 2 (page 54)	Specify automatic access capability based on User Identification.
Step 3 (page 55)	(Optional) Enter a unique client Authorization Code.
Step 4 (page 56)	Close the Client Properties dialog box.

Step 1. Open a Client Properties dialog box

Step 1. Open a Client Properties Dialog Box

Option 1.1 *(page 52)*	Create a new client.
Option 1.2 *(page 53)*	Open an existing Client Properties dialog box.

Option 1.1. Create a new Client
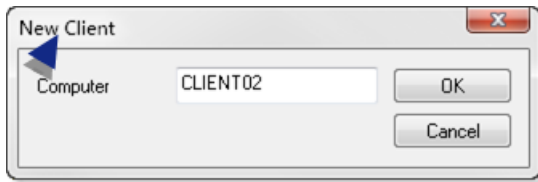
1. Select **Project>Security>Advanced>Client** in the Workbench left pane.

2. Do one of the following.

Action	Description
A	Click File>New on the Workbench menu bar.
B	Click the New Object button on the Workbench toolbar.
C	In the Workbench left pane either double-click **Client**, or right-click **Client** and select New on the Popup menu.

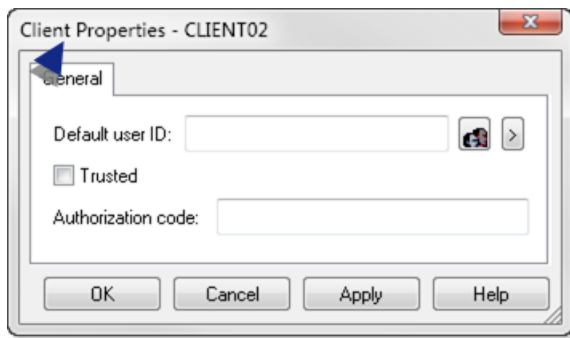| Action	Description
D	In the Workbench right pane, a. Right-click any client. b. Select New on the Popup menu.
E	Press Ctrl+N on the keyboard.

3. Enter the name of the computer for the new client.
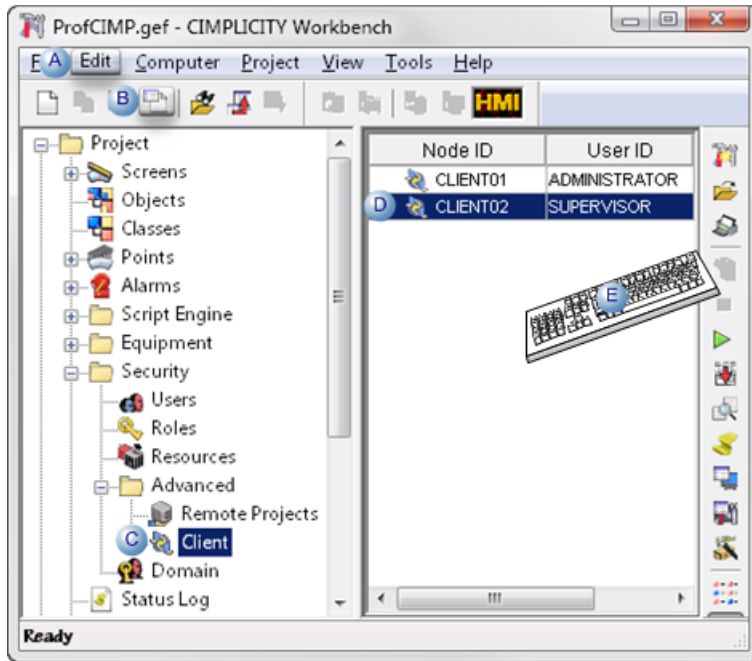
4. Click **OK**.

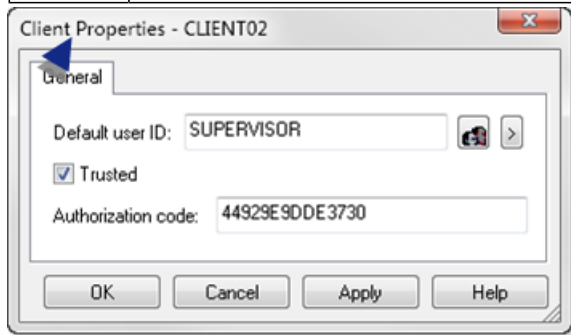The Client Properties dialog box opens.

Option 1.2. Open an existing Client Properties Dialog Box

CIMPLICITY provides several methods to open an existing Client Properties dialog box.

1. Select **Project>Security>Advanced>Client** in the Workbench left pane.

2. Select a client in the Workbench right pane.

3. Do one of the following.

Action	Description
A	Click Edit>Properties on the Workbench menu bar.
B	Click the Properties button on the Workbench toolbar.
C	In the Workbench left pane: a. Right-click **Client**. b. Select Properties on the Popup menu.
D	In the Workbench right pane, either double-click a client, or right-click a client and select Properties on the popup menu.
E	Press Alt+Enter on the keyboard.

The Client Properties dialog box for the selected client opens when you use any method.

Step 2. Specify Automatic Access Capability Based On User Identification

Choose one of the following four combinations of **Default User Id** field entries and **Trusted** check box to control client access based on user identification.

Option	In the Default User ID Field	Trusted Check Box	Client Access
1	Enter a User ID from the list of users available for the project.	Cleared	Users from the Client computer with the selected User ID are automatically logged in.
2	Leave User ID blank.	Selected	Users whose Windows Logon Username matches any CIMPLICITY User ID in the project are automatically logged in. All other users must enter a User ID and Password (if required) in the CIMPLICITY Login dialog box.
3	Enter a User ID from the list of users available for the project.	Selected	Users whose Windows Logon Username matches the specified CIMPLICITY User ID in the project are automatically logged in with that User ID. All other users must enter a User ID and Password (if required) in the CIMPLICITY Login dialog box.
4	Leave User ID blank.	Cleared	All users from the Client computer must manually log into CIMPLICITY.

Tip: Click the Browser button to the right of the input field to open the Select A User Browser and use it to select the User ID.

You can also click the Popup button , that provides you with the options to create a new user or browse for an existing user.

Step 3. Enter a Unique Client Authorization Code

Important: The following is required to run the Generate Authorization Code utility.

Operating System	Logon
Windows XP	With administrative privileges
Windows Server 2003	With administrative privileges
Windows Server 2003 R2	As actual administrator
Vista	As actual administrator

1. Make sure a Proficy CIMPLICITY project is running.

2. Run the CIMPLICITY Genauthcode application on the client to find its unique Authorization Code.

Item	Description
A	Open a Cmd window on the client PC.
B	Type genauthcode at the prompt.
C	Code is generated.

3. Enter the code in the **Authorization Code** field on the server.

Only the PC with the entered Authorization Code will automatically be logged in with the User ID and/or Trusted specifications.

📝 **Note:** Genauthcode requires administrative privileges on Windows XP or 2003.

Step 4. Close the Client Properties Dialog Box

Either:

• Click **OK** to close the Client Properties dialog box and create the new client properties,

Or

• Click **Cancel** to close the dialog box without creating the new client properties.

Chapter 6. System Management

About System Management

There are several procedures that you may need to use over time to manage your CIMPLICITY projects.

Review:

- Base system logical names.

- Login information deleted.

- Remove HMI/SCADA CIMPLICITY 7.0 and higher.

- Remove HMI/SCADA CIMPLICITY updates and patches.

- Remove Registry Information.

- CIMPLICITY security features.

Base System Logical Names

Base System Logical Names

Logical names are used to override default values in the `log_names.cfg` file for the CIMPLICITY Base System and options.

📝 **Note:** Do not confuse logical names with environment variables. Logical names are found in the `log_names.cfg` file, while environment variables are accessed through the Control Panel.

The following Base System applications have logical names:

- Import/Export

- Point management logical names.

- Point management logical name operation.

- `Log_names.cfg` file.

Import/Export Logical Names

Import/Export has the following logical name:

CLIE_MAX_PTS

CLIE_MAX_PTS , in the **log_names.cfg** file, specifies the maximum number of Import/Export points.

The default or expected is **1000**.

An example entry in log_names.cfg is:

CLIE_MAX_PTS|S|default|5|5000

Point Management Logical Names

Point Management will accommodate "reasonable" periods of temporary growth in the use of system memory, yet try to keep an errant client from causing Point Management to consume all resources. You can use Point Management logical names to modify the parameters Point Management uses to determine what is "reasonable".

Logical name	Description
`BSM_PTM_APPQ`	Threshold limit at which the burst handling code will be initiated. The default is **25**.
`BSM_PTM_AQ_OF_DELAY` *(page 59)*	Number of seconds. If the number of seconds specified by this logical have transpired without any communication with a client and an attempt is made to queue another message to this application, messages will be dropped. Note: Setting the **BSM_PTM_AW_OF_DELAY** value to zero causes **BSM_PTM_APPQ** to be used as an absolute limit for dropping messages rather than as a threshold at which burst/growth monitoring is initiated. The default is **50**.
`BSM_PTM_DCQ` *(page 59)*	`BSM_PTM_DCQ` sets the number of messages from a devcom that will be queued for processing in Point Manager to 200 (default).
`BSM_PTM_AQ_PERIOD`	Number of seconds in a period. The default is **15**. 📄 **Note: BSM_PTM_AQ_PERIOD** and **BSM_PTM_AQ_CNT4DROP** work together.
`BSM_PTM_AQ_CNT4DROP` *(page 59)*	Count of periods. The default is **6**. 📄 **Note: BSM_PTM_AQ_PERIOD** and **BSM_PTM_AQ_CNT4DROP** work together.

📒 **Note:** Point Management may log the following messages:

Application queue threshold exceeded…

Application queue overflow occurred…

The logging of these messages and the behavior leading to this can be affected by the Point Management logical names.

Point Management Logical Name Operation

Point management logical names operate as follows:

BSM_PTM_APPQ	
If:	The internal threshold value for messages queued to a client is reached (possibly specified by `BSM_PTM_APPQ`),
Then:	Point Management first checks the approximate period of time since communication occurred with that application.
BSM_PTM_AQ_OF_DELAY	
If:	The period of time exceeds the number of seconds specified by `BSM_PTM_AQ_OF_DELAY`
Then:	Point Management drops messages.
If:	Communication has occurred within the allowed period of time,
Then:	Point Management begins watching for continued growth, by keeping track of the number of messages a client has consumed compared to the number of messages being queued for the client.
BSM_PTM_AQ_CNT4DROP	
If:	Point Management finds that growth has occurred in the number of periods specified by `BSM_PTM_AQ_CNT4DROP`,
Then:	Point Management will start dropping records. Note that these periods are not required to be time consecutive, that is, growth might be noted for three time consecutive periods, no growth for 2 periods, and then growth for another three periods. It is when the maximum number of periods is exceeded that dropping will occur.
If:	The system merely has encountered a burst,
Then:	It is expected that client applications will consume queued messages, and the internal lists will drop below the threshold.
BSM_PTM_DCQ	
If:	If Point Manger receives a larger volume of messages from a devcom than set by `BSM_PTM_DCQ.`
Then:	Increments of the System Sentry (performance) counter recording devcom queue overflows will periodically log messages identifying Device communications occurrence queue overflow - <device>.

When messages drop below that threshold, a reset for the periods of growth count occurs. Counting, therefore, starts over the next time the threshold is exceeded.

Log_names.cfg File

Entries in the **log_names.cfg** file are in the following format:

< logical_name >|< type >|**default**|< length >|< value >

Where:

<logical_name> is the name of the logical

<type> is the type of logical (usually set to P for project)

<length> is the number of characters in <value>

<value> is the value to be assigned to the logical name.

You may use Notepad to edit the file.

To change a logical name in the Logical Names file for a project:

1. Click Tools on the Workbench menu bar.

2. Select Command Prompt.
   An MS DOS window opens

3. Type **cd data** .

4. Type **notepad log_names.cfg** .

Log_Files Record Opened in Windows Notepad

Select a logical name to modify

Notepad opens displaying the log_names.cfg.

5. Find the parameter you want to change, and make the change.

6. Exit the Notepad.

7. Type **exit** to exit the Command Prompt window.

> 📝 **Note:** When you are ready to implement the change in the runtime system, you will have to stop and restart CIMPLICITY software.

Login Information Deleted

When a user logs in to a project, the user is given the opportunity to save the Username and Password used. When a user logs in to a project from a Viewer, the user is also given the opportunity to request that the login occur automatically when the system reboots.

You can use the Login Panel utility to delete saved login information from the System Registry.

Remove HMI/SCADA CIMPLICITY 7.0 and Higher

CIMPLICITY v7.0 and higher can be removed through the Microsoft Control Panel. If CIMPLICITY v8.2 is still installed before CIMPLICITY v9.0 is installed, a message will ask if you want it to be uninstalled. You can also uninstall it at any time through the Microsoft Control Panel.

Step	Description
1	Remove CIMPLICITY.
2	(Optional) Remove CIMPLICITY applications.
3	(Optional) Remove CIMPLICITY Historian
4	(Optional) Remove Microsoft SQL Server Express 2005
5	Restart the computer.

1. Remove CIMPLICITY

1. Open the Add or Remove Programs window in the Microsoft Windows Control Panel.
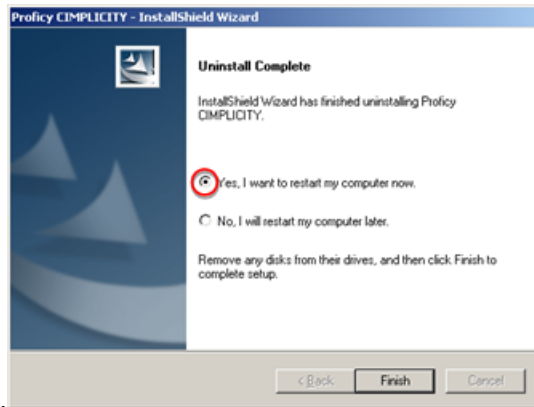2. Select HMI/SCADA - CIMPLICITY.
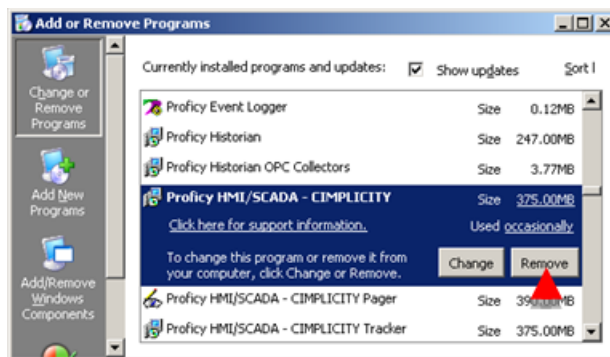
3. Click Remove.

A CIMPLICITY - InstallShield Wizard message opens asking:

Do you want to completely remove the selected application and all of its features?
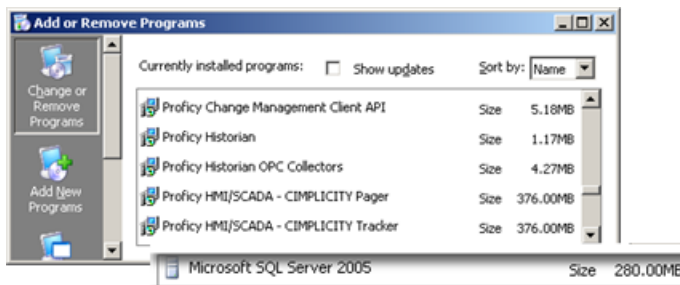
4. Click **Yes**.

A Setup Status window opens and reports the HMI/SCADA - CIMPLICITY removal; additional messages report details during removal. When un-install is complete an Uninstall Complete

window opens.

⚠️ **Important:**
- The following applications were removed.
  ◦ GE HMI/SCADA - CIMPLICITY
- The following applications were not removed.
  ◦ Microsoft SQL Server Express 2005
  ◦ Change Management Client API
  ◦ GE Historian Client
  ◦ GE HMI/SCADA - CIMPLICITY Pager
  ◦ GE HMI/SCADA - CIMPLICITY Tracker

5. Do the following.
   a. Check **Yes, I want to restart my computer now**.
   b. Click **Finish**.

📝 **Note:** You can wait until you remove remaining applications to reboot the computer. However, the HMI/SCADA CIMPLICITY features that were removed will not be completely uninstalled until you do reboot.

2. (Optional) Remove Remaining CIMPLICITY Applications

CIMPLICITY Pager and Tracker require CIMPLICITY to operate. If you do not plan to reinstall the same CIMPLICITY version, it is recommended that you remove these applications.

3. (Optional) Remove GE Historian Client

1. Open the Add or Remove Programs window in the Microsoft Windows Control Panel.
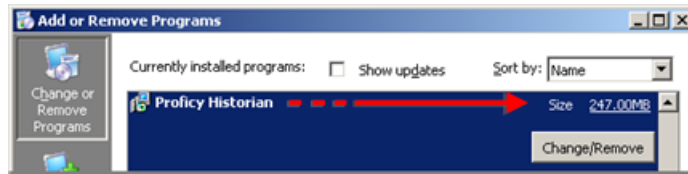
2. Find GE Historian.

   The size that is reported for GE Historian depends on whether Historian Client only or Historian with Historian Client are installed.

Size	Description
1.17MB	Historian Client only is installed.
247. 0MB	Historian with Historian Client is installed.

3. (If no other applications are using GE Historian or Historian Client) Click **Change/Remove** to start the removal process.

When removal is complete an Uninstall Complete window opens providing the option to reboot or not.

4. (Optional) Remove Microsoft SQL Server Express 2005

1. Open the Add or Remove Programs window in the Microsoft Windows Control Panel.
2. Find Microsoft SQL Server Express 2005.
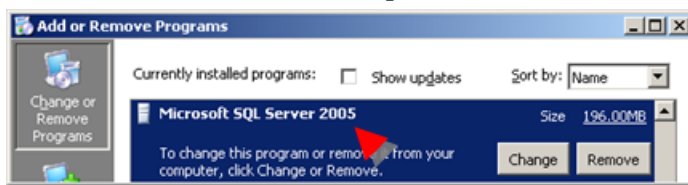
3. (If no other applications are using Microsoft SQL Server Express 2005) Click Remove to start the removal process.

When removal is complete an Uninstall Complete window opens providing the option to reboot or not.

5. Reboot the Computer

When all of the CIMPLICITY components have been removed, reboot the computer.

CIMPLICITY is removed from the computer.

Remove HMI/SCADA CIMPLICITY Updates and Patches

You can remove any CIMPLICITY updates or SIMs without removing the CIMPLICITY application.

1. Open the Add or Remove Programs window in the Microsoft Windows Control Panel.

2. Check Show updates.
   The installed CIMPLICITY updates and SIMs are listed under the CIMPLICITY entry.

3. Select any SIM or update.

4. Click **Remove**.

The selected SIM or update will be removed.

Remove Registry Information

⚠ **CAUTION:** It is possible to cause serious damage to your operating system by using RegEdit and RegEdt32. Be careful not to delete anything that is not listed in these instructions.

1. Run **Regedit.exe** .

2. Open HKEY_CURRENT_USERS

3. Open Software

4. Expand GE Fanuc.

5. Delete CIMPLICITY

6. Open HKEY_CLASSES_ROOT

7. Delete the following:
   - .amv
   - .cim

- .clg
- .gef
- CFGCab Document
- CimEdit
- CimEdit.Documents
- All file types starting with CIMPLICITY
- CimView
- CimView.Documents
- Default Device Property Sheet
- SNPDevice Property Sheet
- TCP IP Device Property Sheet
- VME Device Property Sheet

CIMPLICITY Security Features

CIMPLICITY Security Features

CIMPLICITY software provides you with the following security features to implement:

- Login passwords *(page 66)*
- Role privilege options *(page 66)*
- Setpoint security *(page 67)*
- Setpoint password *(page 67)*
- Security audit trail *(page 67)*

Login Passwords

When you configure a User in a CIMPLICITY project, you can:

- Select whether the user needs to enter a password in the CIMPLICITY Login dialog box. Passwords are stored in an encoded format and are not directly readable by users.
- Set the password to expire after a given number of days. When the password expires, the user will be required to change the password on the next login to CIMPLICITY.
- Configure a number of consecutive login failures. When this number is reached, the user's account is disabled and a **$LOGIN_FAILURE** alarm is generated.

Role Privilege Options

You can assign one Role to each User in a CIMPLICITY project. When you configure a Role in a CIMPLICITY project, you can grant users assigned the Role permission to:

- Perform setpoints on CimView or Point Control Panel screens.
- Enable Dynamic Configuration for functions in the Workbench.
- Delete alarms from the Alarm Viewer window.
- Access the CIMPLICITY Program Control utility.
- Modify alarm setups in the Alarm Viewer window.
- Log setpoint events to the Event Log.
- Create Point by Address points in CimEdit screens.
- Trigger events in the Basic Control Engine User Interface (BCEUI).
- Stop, pause or resume scripts in the BCEUI.

Setpoint Security

The Setpoint Security feature gives you the ability to enable or disable Setpoint capability for all users who access your project. If you enable Setpoint Security, a user can perform setpoints on only those points whose resources are in the user's view.

For an Enterprise Server project, Setpoint Security is enforced against the resource in the Enterprise Server project if that project contains the same resources as the provider of the point. If the resource is not configured on the Enterprise Server project, then Setpoint Security for the point is enforced against the remote project's resource.

Setpoint Password

By default, run-time users have unrestricted access to the setpoint functions used by CIMPLICITY software. If you enable the Setpoint Password option and enter a password, run-time users will be prompted for this password whenever they invoke a setpoint function.

Setpoint functions include:

- Setpoint entries from the Point Control Panel.
- Absolute, Ramp, static, Toggle and Variable setpoint actions on CimView screens.

If you include Setpoint functions in Basic Control Engine scripts, and you enable the Setpoint Password option, you must include the password in the function call.

Security Audit Trail Options

Security Audit Trail Options

The Security Audit Trail lets you monitor user actions in your project. It consists of a set of standard alarms.

Alarms report on the following types of events:

- [Point Control panel alarm changes](#) *(page 68)*
- [Setpoint downloads](#) *(page 68)*
- [Dynamic configuration changes](#) *(page 69)*
- [Project login/logout](#) *(page 72)*

These alarms are included in your project configuration. They are all configured for:

- Delete on Acknowledge
- No Manual Clear
- Log on Generate
- Acknowledge immediately
- No stacking

You can reconfigure the alarm characteristics to suit your needs.

By default, the Audit Trail alarms are logged in the Event Log table of the Database Logger. You can choose whether you want to log each alarm. You can also choose to log each alarm in the Event Log table or Alarm Log table. Finally, you can generate a report of Audit Trail alarms from the Database Logger table.

Point Control Panel Alarm Changes

The Point Control Panel alarm change alarms record the type of change, the Point ID being changed, the CIMPICITY login user name of the user, the computer login user name of the user and the computer name.

- `$ALARM_DISABLED` is generated when a user disables alarming for a point. The alarm message contains the following information: Alarm detection disabled for: <point_id> by <user_id> (<OS_user> @ <computer_name>)
- `$ALARM_ENABLED` is generated when a user enables alarming for a point. The alarm message contains the following information: Alarm detection enabled for: <point_id> by <user_id> (<OS_user> @ <computer_name>)
- `$ALARM_MODIFIED` is generated when a user modifies the alarm limits for a point. The alarm message contains the following information: Alarm limits modified for: <point_id> by <user_id> (<OS_user> @ <computer_name>)
- `$ALARM_RESTORED` is generated when a user restores the alarm limits for a point. The alarm message contains the following information: Alarm limits restored for: <point_id> by <user_id> (<OS_user> @ <computer_name>)

Setpoint Downloads

A user can download setpoints from:

   • CimView screens
   • The Point Control Panel
   • Recipes

Setpoints can also be downloaded from Basic Control Engine scripts

The **$DOWNLOAD** alarm is generated when a user downloads a setpoint or a recipe. The alarm message contains the following information:

```
<point_id> <value> <user_id> (<OS_user> @ <computer_name>)
```

Dynamic Configuration Changes

Dynamic Configuration Changes

When the `$DYN_CFG` alarm is routed to the correct role and configured for manual acknowledgement, it notifies the configured role(s) each time a user makes a configuration change while Dynamic Configuration is enabled.

The user, usually the administrator, to whom the alarm is routed will receive an alarm message.

The alarm message contains the following information:

```
<type> <name> changed by <user_id> (<OS_user> @ <computer_name>)
```

Where the parameters are as follows:

Parameter	Description
<type>	Entity type being changed.
<name>	Entity name being changed.
<user_id>	CIMPLICITY login user name of the user making the dynamic configuration change.
<OS_user>@<computer_name>	Computer login user name of the user making the dynamic configuration change.

⚠ **Important:** By default, `$DYN_CFG` is not routed to any role and is set to be automatically acknowledged and delete on acknowledgement. Therefore, configuration is required if you want it to be seen.

Steps to configure the `$DYN_CFG` alarm are:

Step	Description
Step 1 *(page 70)*	Make sure your role has alarm configuration privileges.
Step 2 *(page 70)*	Open the Alarm Definition - $DYN_CFG dialog box.
Step 3 *(page 71)*	Configure $DYN_CFG to notify the appropriate role(s).

Step 1. Make sure your Role has Alarm Configuration Privileges

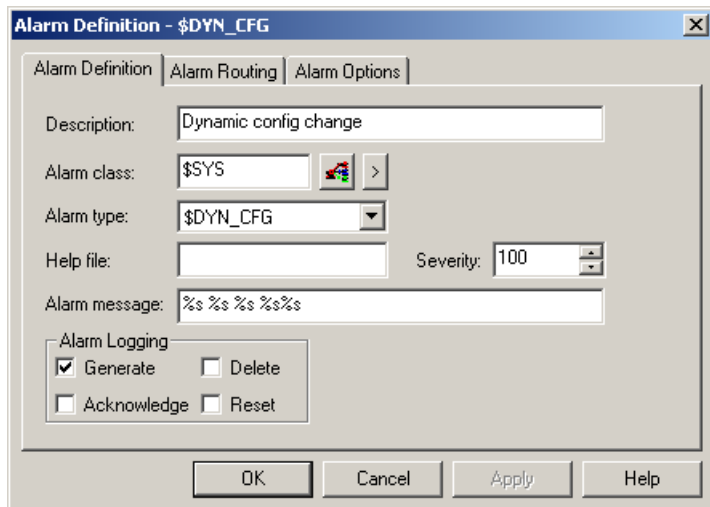**Note:** This step is important if you have Configuration Security enabled.

1. Expand the Security folder in the Workbench left pane.

2. Select ⚑ Roles in the Workbench left pane.

3. Double-click your role in the Workbench right pane.
   The Role Properties dialog box opens.

4. Select the Configuration tab.

5. Make sure that **Alarms** is checked.
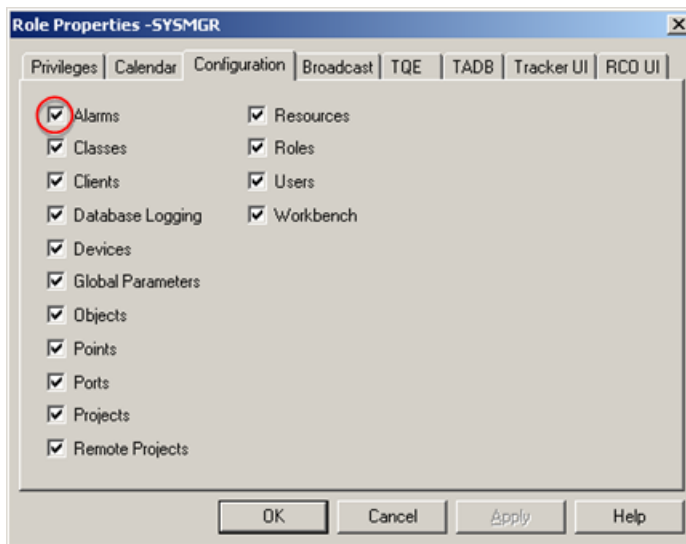
Step 2. Open the Alarm Definition - $DYN_CFG Dialog Box

1. Expand the Advanced folder in the Workbench left pane.

2. Select ⊟ 🚨 Alarms.

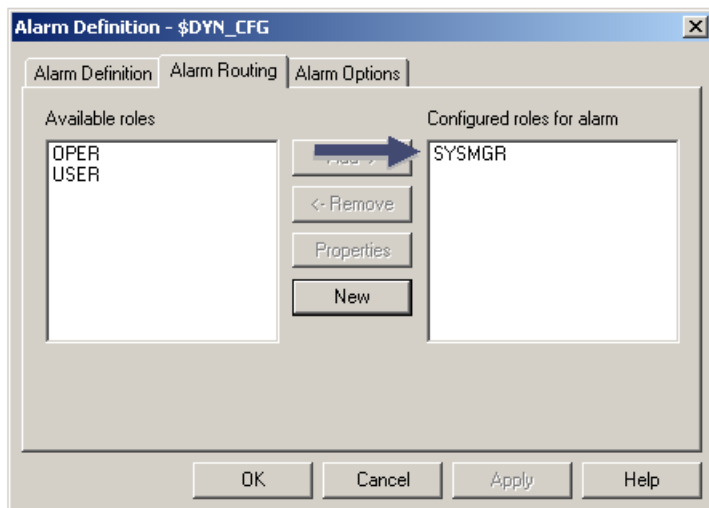3. Double-click $DYN_CFG in the Workbench right pane.
   The Alarm Definition $DYN_CFG dialog box

   opens.

Step 3. Configure $DYN_CFG to Notify the Appropriate Role(s)

1. Select the Alarm Routing tab in the Alarm Definition - $DYN_CFG dialog box.

2. Move your role to the **Configured roles for alarm** box.

3. Select the Alarm Options tab.

4. Change **Immediate** to **None** or **Timed** in the **Auto acknowledge** field.
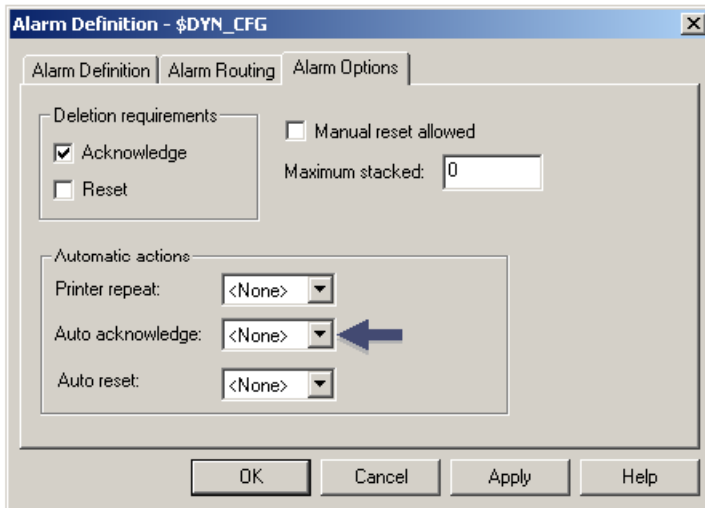
5. Click **OK**.

The next time a user performs a dynamic configuration $DYN_CONFIG will notify the selected roles.

Project Login/Logout

The **$LOGIN_FAILURE** alarm is generated when a user fails to log in to a CIMPLICITY project correctly and the number of consecutive login errors has been reached. The alarm message contains the following information:

User ID <user_id> **disabled, computer** <computer_name>

The **$LOGIN** alarm is generated when a user successfully logs in to a CIMPLICITY project. The alarm message contains the following information:

User ID <user_id> @ <computer_name> **logged on**

The **$LOGOUT** alarm is generated when a user logs out of a CIMPLICITY project. The alarm message contains the following information:

User ID <user_id> @ <computer_name> **logged out**