Proprietary Notice
The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

© 2023, General Electric Company. All rights reserved.

Trademark Notices
GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

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
Contents

Chapter 1. About Security and Routing.............................................................. 5

Chapter 2. Resource Configuration........................................................................ 6
   About Resources............................................................................................... 6
   Resource Configuration..................................................................................... 6
      Resource Configuration.................................................................................. 6
   Step 1. Open a Resource Definition Dialog Box............................................. 8
   Step 2. Configure a Resource Definition....................................................... 10
   Enable or Disable Alarm Counters (from Workbench)................................... 13

Chapter 3. Role Configuration............................................................................... 14
   About Roles...................................................................................................... 14
   Role Configuration.......................................................................................... 14
      Role Configuration....................................................................................... 14
   Procedure to View a Project's Existing Roles................................................. 14
   Step 1. Open a Role's Role Properties Dialog Box....................................... 14
   Step 2. Assign Role Privileges......................................................................... 17

Chapter 4. User Configuration.............................................................................. 37
   About Users.................................................................................................... 37
   About CIMPLICITY Passwords........................................................................ 37
   Windows Authentication Configuration....................................................... 38
      Windows Authentication Configuration....................................................... 38
   Step 1. Open the Windows Authentication Window.................................... 40
   Step 2. List Groups in a Selected Domain..................................................... 41
   Step 3. Select Groups that will be Authenticated for CIMPLICITY............... 44
   Step 4. Map a Role for each Group............................................................... 44
   Step 5. Prioritize Groups................................................................................ 46
   Step 6. Enable Automatic Log Ins................................................................. 47
   Step 7. Save or Cancel the Windows Authentication Configuration............. 54
Contents | iv

Login Passwords ........................................................................................................... 84
Role Privilege Options ................................................................................................. 84
Setpoint Security .......................................................................................................... 84
Setpoint Password ........................................................................................................ 85
Security Audit Trail Options ......................................................................................... 85
Chapter 1. About Security and Routing

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

1. About Users (on page 37)
2. About Roles (on page 14)
3. About Resources (on page 6)
4. About Client Configuration (on page 67)
5. Windows Authentication Configuration (on page 38)

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

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

<table>
<thead>
<tr>
<th>Step 1 (on page 8)</th>
<th>Create a new resource.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2 (on page 10)</td>
<td>Configure a resource definition.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>A name that uniquely identifies each resource.</td>
</tr>
<tr>
<td>Description</td>
<td>Text that gives users more information about the resource.</td>
</tr>
<tr>
<td>Resource Type</td>
<td>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.</td>
</tr>
<tr>
<td>Alarm Mgr</td>
<td>Identifies the Alarm Manager process that receives alarms for this resource. This is a display-only field and cannot be modified.</td>
</tr>
</tbody>
</table>

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

### Option 1.1. Create a New Resource

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click File&gt;<strong>New</strong> on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the <strong>New Object</strong> button on the Workbench toolbar.</td>
</tr>
<tr>
<td>C</td>
<td>In the Workbench left pane, either double-click <strong>Resources</strong>, or right-click <strong>Resources</strong> and select New on the Popup menu.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>D</td>
<td>In the Workbench right pane, right-click any resource and select New on the Popup menu.</td>
</tr>
<tr>
<td>E</td>
<td>Press Ctrl+N on the keyboard.</td>
</tr>
</tbody>
</table>

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

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

![New Resource dialog box]

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 (on page 10) 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.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click Edit&gt;Properties on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the Properties button on the Workbench toolbar.</td>
</tr>
</tbody>
</table>
| 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**

The Resource Definition window allows you to add a description for the resource, enable alarm counters, and add available users to the resource. Enabling alarm counters allow you to view total alarms, unacknowledged alarms, unreset alarms generated at a resource.

Perform the following steps to configure a resource definition for a resource:
1. Enter a description for the resource in the Description text box.

2. **Optional**: Select **Enable Alarm Counters** if you want to count or classify the alarms based on the resource.

**Note:**
You can also enable or disable the alarm counters for a resource from the Workbench Enable or Disable Alarm Counters (from Workbench) (on page 13)

**Important:**
- **Enable Alarm Counters** check box is not available in dynamic mode.
- If you disable the alarm counters of a resource, the existing alarm counter points of the resource are deleted.

3. To add a user for the resource, select the user from the **Available users** list, and select **Add->**. The user is moved to the **Users for this resource** list.

4. **Optional**: To remove a user, select the user from the **Users for this resource** list, and then select **Remove->**. The user is removed to the **Available users** list.
5. **Optional**: To view the properties of a resource, select the user from the *Available users* or *Users for this resource* list, and then select *Properties*. The *User Properties* window appears.

6. **Optional**: To create a new user:
   a. Select *New*.
   b. Enter a user ID, and then select *OK*.
   c. Enter user properties. Refer Step 2. Configure User General Properties (on page 59) and Step 3. Configure User Resource Availability (on page 63)
   d. Select *Apply*, and then select *OK*.

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

The resource is created and appears in the *Resources* list.

If you enabled alarm counters at step 2, the value of *Enable Alarm Counters* column is set to 1. Alarm points are generated for the resource which enable you to view the total alarms, unacknowledged alarms, unreset alarms generated at a resource.

If you disable alarm counters for a resource, the value of *Enable Alarm Counters* column is set to 0. The existing alarm points generated for the resource are deleted.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Enable Alarm Counters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COATING_AREA</td>
<td>1</td>
<td>This is coating area</td>
</tr>
<tr>
<td>PAINTING_AREA</td>
<td>1</td>
<td>this is painting area</td>
</tr>
<tr>
<td>WEILDING_AREA</td>
<td>0</td>
<td>This is weilding area</td>
</tr>
<tr>
<td>$MAC_FR</td>
<td>0</td>
<td>System Events</td>
</tr>
<tr>
<td>$PTM_FR</td>
<td>0</td>
<td>Point Mgmt Info</td>
</tr>
<tr>
<td>$SYSTEM</td>
<td>0</td>
<td>Systern Resource</td>
</tr>
</tbody>
</table>

**Note:**
In Performance Monitor, the *HMI Alarm Resource* category is added to the counters list which enables you monitor the alarm counters based on the resource.
Enable or Disable Alarm Counters (from Workbench)

You can classify the alarms based on the resource at which they are generated. When you enable the alarm counters you can view the total alarms, unacknowledged alarms, unreset alarms generated at a resource.

You can also watch the following video for detailed steps on Enabling/Disabling Alarm Counters:

https://www.youtube.com/embed/rH29zJzThdI

Note:
If you are using a script to create a resource, you must set the resource.EnableAlarmCounters parameter to True to enable the alarm counters while creating a resource using a script.

The following are the steps to Enable or Disable alarm counters from Workbench.

1. In the Workbench, select Resources from the Security drop-down list.

   Note:
   You can also enable/disable alarm counters from Resource Definition window. Refer Option 1.2. Open an Existing Resource Definition Dialog Box (on page 9).

   The list of resources appears.
2. Right-click the resource(s) for which you want to enable the alarm counters.
3. Select Enable Alarm Counter(s) to enable alarm counters for the resource(s) or select Disable Alarm Counter(s) to disable the alarm counters of the resource(s).

If you enable alarm counters for a resource, the value of Enable Alarm Counters column is set to 1. Alarm counter points are generated for the resource which enable you to view the total alarms, unacknowledged alarms, unreset alarms generated at a resource.

If you disable alarm counters for a resource, the value of Enable Alarm Counters column is set to 0. The existing alarm counter points of the resource are deleted.
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:

- SYSMGR
- USER
- OPER

Role Configuration

### 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
Option 1.1. Create a New Role

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click File-New on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the New Object button on the Workbench toolbar.</td>
</tr>
<tr>
<td>C</td>
<td>In the Workbench left pane, either double-click Roles, or right-click Roles and select New on the Popup menu.</td>
</tr>
<tr>
<td>D</td>
<td>In the Workbench right pane, right-click any role, and select New on the Popup menu.</td>
</tr>
<tr>
<td>E</td>
<td>Press Ctrl+N on the keyboard.</td>
</tr>
</tbody>
</table>
The new role dialog box opens when you use any method.

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

   ![New Role Dialog Box]

   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.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click Edit&gt;Properties on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the <strong>Properties</strong> button on the Workbench toolbar.</td>
</tr>
</tbody>
</table>
| 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**

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.

<table>
<thead>
<tr>
<th>Option 2.1 (on page 18)</th>
<th>Assign role application privileges.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 2.2 (on page 26)</td>
<td>Assign role calendar privileges.</td>
</tr>
<tr>
<td>Option 2.3 (on page 27)</td>
<td>Assign role configuration privileges.</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Option 2.4 (on page 28)</td>
<td>Assign role Broadcast privileges.</td>
</tr>
<tr>
<td>Option 2.5 (on page 29)</td>
<td>Assign role Query Engine privileges.</td>
</tr>
<tr>
<td>Option 2.6 (on page 30)</td>
<td>Assign role TADB privileges.</td>
</tr>
<tr>
<td>Option 2.7 (on page 31)</td>
<td>Assign role Tracker UI privileges.</td>
</tr>
<tr>
<td>Option 2.8 (on page 34)</td>
<td>Assign role RCO UI privileges.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (on page 20)</td>
<td>General.</td>
</tr>
<tr>
<td>2 (on page 20)</td>
<td>Alarms.</td>
</tr>
<tr>
<td>3 (on page 21)</td>
<td>Runtime.</td>
</tr>
<tr>
<td>4 (on page 24)</td>
<td>Change approval.</td>
</tr>
<tr>
<td>5 (on page 24)</td>
<td>Event manager.</td>
</tr>
</tbody>
</table>
1. General

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

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic configuration</td>
<td>Enable Dynamic Configuration from functions in the Workbench.</td>
</tr>
<tr>
<td>Process Control</td>
<td>Use the CPC (CIMPLICITY Program Control) utility to start and stop CIMPLICITY processes.</td>
</tr>
<tr>
<td>Start Project</td>
<td>Start a project.</td>
</tr>
<tr>
<td>Stop Project</td>
<td>Stop a project.</td>
</tr>
</tbody>
</table>

2. Alarms

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

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete alarms</td>
<td>Delete alarms from the Alarm Viewer.</td>
</tr>
<tr>
<td>Modify alarm setups</td>
<td>Modify alarm setups in Alarm Viewer.</td>
</tr>
</tbody>
</table>
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

**Right-click menu**

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Viewer OCX</td>
<td>A Popup menu displays. Processes that can be opened through the Popup menu include:</td>
<td></td>
</tr>
<tr>
<td>Checked</td>
<td>• Add a project.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remove a project.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Open the Point Control Panel.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Open a quick trend.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Point Target must also be checked for Point Control Panel and quick trend.</td>
<td></td>
</tr>
<tr>
<td>Clear</td>
<td>No Popup menu displays.</td>
<td></td>
</tr>
<tr>
<td>CimView</td>
<td>A Popup menu displays. Processes that can be opened through the Popup menu include:</td>
<td></td>
</tr>
<tr>
<td>Checked</td>
<td>• Open a Point View window.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Open the Point Control Panel.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Open a quick trend.</td>
<td></td>
</tr>
</tbody>
</table>
### Security | 3 - Role Configuration | 22

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>Point Target must also be checked for Point Control Panel and quick trend.</td>
<td></td>
</tr>
<tr>
<td>Clear</td>
<td>No Popup menu displays.</td>
<td></td>
</tr>
<tr>
<td><strong>Point Control Panel</strong></td>
<td>A Popup menu displays. Processes that can be opened through the Popup menu include:</td>
<td></td>
</tr>
<tr>
<td>Checked</td>
<td>Open an additional Point Control Panel that displays selected points.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open a quick trend.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Point Target must also be checked for Point Control Panel and quick trend.</td>
<td></td>
</tr>
<tr>
<td>Clear</td>
<td>No Popup menu displays.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>System Sentry displays Popup options the same as other CimView screens.</td>
<td></td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

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 **Quick Trends** 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.

<table>
<thead>
<tr>
<th>Point target Checked</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>CimView</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="CimView screenshot" /></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Point Control Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Point Control Panel screenshot" /></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify</td>
<td>Electronically verify a setpoint action for points and/or alarms that require electronic signatures for both the setpoint performer and a verifier.</td>
</tr>
</tbody>
</table>

5. Event Manager

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Event</td>
<td>Trigger Event Manager events from the Basic Control Engine user interface.</td>
</tr>
<tr>
<td>Script Control</td>
<td>Stop, pause, or resume scripts in the Event Manager from the Basic Control Engine user interface.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set point</td>
<td>Perform setpoints from CimView screens that contain Setpoint actions.</td>
</tr>
<tr>
<td>Set-point Audit Trail</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Default</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point by Address</td>
<td>Use point by address points in CimEdit expressions.</td>
</tr>
<tr>
<td>Disable / modify alarms</td>
<td>Disable or modify a point’s alarms in the Point Control Panel.</td>
</tr>
<tr>
<td>Modify Attributes</td>
<td>Change the MANUAL_MODE point quality attribute. Change the QUALITY.DISABLE_WRITE point attribute. Write to a user defined field attribute if <strong>Restrict write by role</strong> is checked in the Field Attribute dialog box.</td>
</tr>
</tbody>
</table>
8. OPC UA

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPC UA server admin</td>
<td>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.</td>
</tr>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Resource Security</td>
<td>Checked</td>
<td>Only see areas whose Resource ID is assigned to the user</td>
</tr>
<tr>
<td>Configuration</td>
<td>Checked</td>
<td>Configure a schedule for any areas that can be seen</td>
</tr>
<tr>
<td></td>
<td>Unchecked</td>
<td>See all areas.</td>
</tr>
</tbody>
</table>
### 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 CIMPILICITY 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.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Publish</td>
<td>Add/publish a WYSIWYG, ASCII or Control Character Token (CCT) form to the list of available Broadcast forms.</td>
</tr>
<tr>
<td>Save As Defaults</td>
<td>Save WYSIWYG form object configurations as defaults for objects that are placed on a form after the defaults are saved.</td>
</tr>
<tr>
<td>Compile</td>
<td>Compile a Control Character Token file, ASCII form or WYSIWYG form.</td>
</tr>
<tr>
<td>Test</td>
<td>Test an ASCII or WYSIWYG form with data to make sure it has the correct layout and configuration.</td>
</tr>
<tr>
<td>Broadcast device group</td>
<td>Configure a Broadcast device group</td>
</tr>
<tr>
<td>Archive job</td>
<td>Archive a job from the history queue.</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancel a job.</td>
</tr>
<tr>
<td>Configure generic fields</td>
<td>Configure job fields in the Broadcast Queue Manager.</td>
</tr>
<tr>
<td>Configure job priority</td>
<td>Specify priority among the following job types.</td>
</tr>
<tr>
<td></td>
<td>• Ad Hoc broadcast</td>
</tr>
<tr>
<td></td>
<td>• Redirect</td>
</tr>
<tr>
<td></td>
<td>• Resend</td>
</tr>
<tr>
<td></td>
<td>• Normal broadcast</td>
</tr>
<tr>
<td></td>
<td>• Test broadcast</td>
</tr>
<tr>
<td>Delete job</td>
<td>Delete jobs in the Broadcast Queue Manager.</td>
</tr>
<tr>
<td>Job Queue limits</td>
<td>Set queue limits in the Broadcast Queue Manager.</td>
</tr>
<tr>
<td>Pause device</td>
<td>Pause a device in the Broadcast Queue Manager</td>
</tr>
<tr>
<td>Pause job</td>
<td>Pause selected active jobs that are in the Broadcast Queue Manager printing queue.</td>
</tr>
<tr>
<td>Redirect job</td>
<td>Redirect selected jobs in the Broadcast Queue Manager</td>
</tr>
<tr>
<td>Requeue job</td>
<td>Re-queue selected archived jobs in the Broadcast Queue Manager</td>
</tr>
<tr>
<td>Resend job</td>
<td>Resend selected history jobs in the Broadcast Queue Manager</td>
</tr>
<tr>
<td>Reset devices</td>
<td>Reset devices, after they have been paused, so the Broadcast Queue Manager will send them forms.</td>
</tr>
<tr>
<td>Reset sequence number</td>
<td>Reset the device group sequence number in the Broadcast Queue Manager.</td>
</tr>
<tr>
<td>Resume device</td>
<td>Resume a device after it has been paused in the Broadcast Queue Manager.</td>
</tr>
<tr>
<td>Resume job</td>
<td>Resume printing of jobs that have been paused in the Broadcast Queue Manager.</td>
</tr>
<tr>
<td>Send adhoc broadcast</td>
<td>Send an adhoc broadcast through the Broadcast Queue Manager.</td>
</tr>
</tbody>
</table>

**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.

### 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.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Create or modify expressions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Create or modify Tracker item types, groups and/or attributes in the TrackerCfg UI</td>
</tr>
</tbody>
</table>
### Privilege Configuration

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Runtime</td>
<td>Create or modify attributes in the PRT UI or through a CimView screen.</td>
</tr>
</tbody>
</table>

**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.
1. #unique_27_Connect_42_AddItem (on page 33)
2. #unique_27_Connect_42_DeleteItem (on page 33)
3. #unique_27_Connect_42_ModifyItem (on page 33)
4. #unique_27_Connect_42_FetchItem (on page 33)
5. #unique_27_Connect_42_FindItem (on page 33)
6. #unique_27_Connect_42_MoveItem (on page 33)
7. #unique_27_Connect_42_AdvanceItem (on page 33)
8. #unique_27_Connect_42_AddAttribute (on page 33)
9. #unique_27_Connect_42_DeleteAttribute (on page 33)
10. #unique_27_Connect_42_ModifyAttribute (on page 33)
11. #unique_27_Connect_42_SetActiveItem (on page 33)
12. #unique_27_Connect_42_AddFlag (on page 33)
13. #unique_27_Connect_42_ModifyFlag (on page 33)
14. #unique_27_Connect_42_DeleteFlag (on page 34)
15. #unique_27_Connect_42_AutolockRegion (on page 34)
16. #unique_27_Connect_42_SetRegion (on page 34)
17. #unique_27_Connect_42_ClearRegion (on page 34)
18. #unique_27_Connect_42_Query (on page 34)
19. #unique_27_Connect_42_SelectView (on page 34)
20. #unique_27_Connect_42_AddProjects (on page 34)
<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Insert Item</td>
<td>Add or Insert an item to a region.</td>
</tr>
<tr>
<td>Delete Item</td>
<td>Delete an item into a region.</td>
</tr>
<tr>
<td>Modify Item</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>• Add Attribute</td>
</tr>
<tr>
<td></td>
<td>• Delete Attribute</td>
</tr>
<tr>
<td></td>
<td>• Modify Attribute</td>
</tr>
<tr>
<td></td>
<td>• Item Set/Clear Active</td>
</tr>
<tr>
<td>Fetch Item</td>
<td>Fetch an item.</td>
</tr>
<tr>
<td>Find Item</td>
<td>Find an item in the PRT database using the PRT_UI.</td>
</tr>
<tr>
<td>Move/Reorder Item</td>
<td>Move or Reorder an item to another region using the PRT_UI.</td>
</tr>
<tr>
<td>Advance Item</td>
<td>Advance an item to the next region using the PRT_UI.</td>
</tr>
<tr>
<td>Add Attribute</td>
<td>Add a PRT standard or extended attribute.</td>
</tr>
<tr>
<td>Delete Attribute</td>
<td>Delete a PRT standard or extended attribute.</td>
</tr>
<tr>
<td>Modify Attribute</td>
<td>Modify a PRT standard or extended attribute.</td>
</tr>
<tr>
<td>Item Set/Clear Active</td>
<td>Activate or de-activate an item's status in a region, e.g. delayed, external hold, internal hold and normal.</td>
</tr>
<tr>
<td>Add Named Hold Flag</td>
<td>Add named hold flags through Object Model scripting</td>
</tr>
<tr>
<td>Modify Named Hold Flag</td>
<td>Modify named hold flags through Object Model scripting</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Delete Named Hold Flag</td>
<td>Delete named hold flags through Object Model scripting.</td>
</tr>
<tr>
<td>Autolock region</td>
<td>Automatically lock the region so you can perform operations on items within the region whenever you want.</td>
</tr>
<tr>
<td>Region Set active</td>
<td>Activate a region’s status.</td>
</tr>
<tr>
<td>Region Clear active</td>
<td>De-activate a region’s status.</td>
</tr>
<tr>
<td>Query</td>
<td>NA</td>
</tr>
<tr>
<td>Select View</td>
<td>Select a configured view.</td>
</tr>
<tr>
<td>Add Projects</td>
<td>Connect to multiple projects.</td>
</tr>
</tbody>
</table>

**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.

![Role Properties - SYMGR](image)

1. #unique_28_Connect_42_EnableSite (on page 36)
2. #unique_28_Connect_42_SuspendSite (on page 36)
3. #unique_28_Connect_42_ManualControl (on page 36)
4. #unique_28_Connect_42_ExecuteDecision (on page 36)
5. #unique_28_Connect_42_Alarming (on page 36)
6. #unique_28_Connect_42_CancelDecision (on page 36)
7. #unique_28_Connect_42_EnableDecision (on page 36)
8. #unique_28_Connect_42_UpdateTrigger (on page 36)
9. #unique_28_Connect_42_ResetTrigger *(on page 36)*
10. #unique_28_Connect_42_ManualTrigger *(on page 36)*

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable site</td>
<td>Enable or Disable control sites.</td>
</tr>
<tr>
<td>Suspend site</td>
<td>Suspend control sites.</td>
</tr>
<tr>
<td>Manual Control</td>
<td>Perform manual decisions.</td>
</tr>
<tr>
<td>Execute Current Decision</td>
<td>Complete current decisions.</td>
</tr>
<tr>
<td>Alarming/Logging</td>
<td>Set alarming and logging through the RCOUI</td>
</tr>
<tr>
<td>Cancel decision</td>
<td>Cancel RCO decisions.</td>
</tr>
<tr>
<td>Enable decision</td>
<td>Enable or Disable manual control decisions.</td>
</tr>
<tr>
<td>Update trigger</td>
<td>Refresh the status of triggers.</td>
</tr>
<tr>
<td>Reset trigger</td>
<td>Reset triggers manually.</td>
</tr>
<tr>
<td>Manual trigger</td>
<td>Manually trip a trigger.</td>
</tr>
</tbody>
</table>
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 (on page 37)* 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.

---

**Proficy Authentication**

When you enable Proficy Authentication (*on page * ) for a CIMPLICITY project and log in to applications using the Proficy Authentication user, that user will automatically be added to the list of users in CIMPLICITY Workbench for security reasons. You can double-click the user to view the configured properties. However, you cannot edit the properties of that user.

---

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

You can determine how long the application must wait before a connection timeout occurs when a connection to an LDAP server is not established. You can use the ADV_LDAP_CONNECT_TIMEOUT global parameter (on page  ) to set the timeout.

Do the following to select and configure the groups that CIMPLICITY will use for authentication.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <em>(on page 40)</em></td>
<td>Open the Windows Authentication window.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <em>(on page 41)</em></td>
<td>List Windows groups in a selected domain.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <em>(on page 44)</em></td>
<td>Select groups that will be authenticated for CIMPLICITY.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <em>(on page 44)</em></td>
<td>Map a role for each group.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td>Prioritize groups.</td>
</tr>
<tr>
<td>(on page 46)</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Enable automatic log ins.</td>
</tr>
<tr>
<td>(on page 47)</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Save or Cancel the Windows Authentication Configuration.</td>
</tr>
<tr>
<td>(on page 54)</td>
<td></td>
</tr>
</tbody>
</table>

**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.
### Security | 4 - User Configuration

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click Edit&gt;Properties on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the Properties button on the Workbench toolbar.</td>
</tr>
<tr>
<td>C</td>
<td>In the Workbench left-pane either double-click <strong>Domain</strong>, or right-click <strong>Domain</strong> and select Properties on the popup menu.</td>
</tr>
<tr>
<td>D</td>
<td>In the Workbench left-pane either double-click <strong>Domain</strong>, or right-click <strong>Domain</strong> and select Properties on the popup menu.</td>
</tr>
<tr>
<td>E</td>
<td>Press Alt+Enter on the keyboard.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Item</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Domain</td>
<td>Select a domain from the drop-down list.</td>
</tr>
<tr>
<td>B</td>
<td>Load Groups</td>
<td>Click <strong>Load Groups</strong>. Domain groups are listed in the <strong>Available Groups</strong> box.</td>
</tr>
<tr>
<td>C</td>
<td>Available Groups</td>
<td>(Optional) Enter a string in the field to list only groups that contain the string in some part of the name.</td>
</tr>
</tbody>
</table>

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.

![Windows Authentication error message](image)

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.

<table>
<thead>
<tr>
<th>Login</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>The domain's available groups are listed.</td>
</tr>
<tr>
<td>Login</td>
<td>Result</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Invalid</td>
<td>a. An error message reports that the login is invalid.</td>
</tr>
<tr>
<td></td>
<td>b. A blank Login window opens.</td>
</tr>
</tbody>
</table>

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:
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, Allow Auto Login, and Advanced runtime settings).

1. Open the Windows Authentication dialog box.
2. Select **Enable Windows Authentication**.
The following options become available: **Allow Configuration Auto Login, Allow Auto Login**, and **Advanced runtime settings**.

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:

<table>
<thead>
<tr>
<th>Allow Auto Login</th>
<th>Allow Configuration Auto Login</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checked</td>
<td>Clear</td>
<td>If the Windows user is a member of a selected group, CIMPLICITY will:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Look for the user in the Selected Groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Automatically log in the user to CIMPLICITY based on the first group in which the user is found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Users have to:</td>
</tr>
<tr>
<td>Allow Auto Login</td>
<td>Allow Configuration Auto Login</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Checked</td>
<td>Checked</td>
<td>Users can potentially be automatically logged into:  ◦ CIMPLICITY configuration. ◦ CIMPLICITY runtime. ◦ Proficy Change Management projects.</td>
</tr>
<tr>
<td>Clear</td>
<td>Checked</td>
<td>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.</td>
</tr>
<tr>
<td>Allow Auto Login</td>
<td>Allow Configuration Auto Login</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

- 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 Authentication group in which the user is found.

Users are:
- Automatically logged into CIMPLICITY to do configuration even if CIMPLICITY Configuration Security (on page ) is enabled.

A failure message may display for a user who does not have Workbench privileges; a Con-
<table>
<thead>
<tr>
<th>Allow Auto Login</th>
<th>Allow Configuration Auto Login</th>
<th>Description</th>
</tr>
</thead>
</table>

Allow Configuration Auto 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 Workbench starts up if Log-
<table>
<thead>
<tr>
<th>Allow Auto Login</th>
<th>Allow Configuration Auto Login</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>gon at Workbench startup is checked.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If Prompt for user name and password at logon is not checked.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Based on whether or not a username/password that is entered for CIMPLICITY/PCM is valid or invalid.</td>
</tr>
</tbody>
</table>

**Important:**
Close and reopen the Workbench after Allow Configuration Auto Login is checked.

4. If you want to specify custom domain and credentials, select **Advanced runtime settings**. You can use this option in the following scenarios:
If your CIMPLICITY services are running on a different server without domain privileges, and you want to specify another user that can access the domain.

If your CIMPLICITY services are running on a different server, and your LDAP connection is on a different server.

The other configuration options below **Advanced runtime settings** are enabled.

5. Enter the following configurations:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user of the domain that you selected.</td>
</tr>
<tr>
<td>Port</td>
<td>The Port of the selected domain. By default, CIMPLICITY uses the SASL framework for authentication. You can also use the TLS connection for communication security when connecting to LDAP servers. The default port for a TLS connection is 636. However, if you have a different port configured, you can use that. To use the TLS connection, you must configure the <strong>WINAUTH_LDAP_SECURITY_MODE</strong> global parameter (on page 53), and set the value as TLS.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the domain user.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. *(on page 56)*
2. Configure user general (security) properties. *(on page 59)*
3. Configure user resource availability. *(on page 63)*
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:

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

**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

You can begin user configuration by:

<table>
<thead>
<tr>
<th>Option 1.1 (on page 56)</th>
<th>Create a new user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 1.2 (on page 58)</td>
<td>Open the Properties dialog box for an existing user.</td>
</tr>
</tbody>
</table>

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 Role (on page 14) 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.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click File&gt;New on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the New Object button on the Workbench toolbar.</td>
</tr>
<tr>
<td>C</td>
<td>In the Workbench left pane, either double-click Users, or right-click Users and select New on the Popup menu.</td>
</tr>
</tbody>
</table>
| 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 if the User ID is approved.

### New Windows Authenticated User

1. **Enable (on page 47) and configure (on page 38) 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 (on page 58) 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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click Edit&gt;Properties on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the Properties button on the Workbench toolbar.</td>
</tr>
<tr>
<td>C</td>
<td>In the Workbench left pane:</td>
</tr>
</tbody>
</table>
### 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.
Security | 4 - User Configuration | 60

1. #unique_13_Connect_42_i6PasswordExpire (on page )
2. #unique_13_Connect_42_i5Enabled (on page )
3. #unique_13_Connect_42_i4Username (on page )
4. #unique_13_Connect_42_i3PasswordConfirm (on page )
5. #unique_13_Connect_42_i2Authentication (on page )
6. #unique_13_Connect_42_i4Username (on page )

Role

1. Select to the right of the input field to display the Select A Role window and use it to select the role.

2. Optional: Select 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:

<table>
<thead>
<tr>
<th>Selection</th>
<th>CIMPLICITY allows access</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>With no password.</td>
</tr>
<tr>
<td>CIMPLICITY</td>
<td>When the user enters the name and password that are in the Users dialog box.</td>
</tr>
<tr>
<td>Selection</td>
<td>CIMPLICITY allows access</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>The user’s role and other specifications are also defined.</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>Available when both:</td>
</tr>
<tr>
<td></td>
<td>• The user is a member of a selected Windows Authentication group.</td>
</tr>
<tr>
<td></td>
<td>• Enable Windows Authentication is checked in the Windows Authentication window.</td>
</tr>
<tr>
<td></td>
<td>The user’s assigned role and name may be different from the role assigned to the group.</td>
</tr>
<tr>
<td>Windows Domain with Group Mapping</td>
<td>Available when both:</td>
</tr>
<tr>
<td></td>
<td>• The user is a member of a selected Windows Authentication group.</td>
</tr>
<tr>
<td></td>
<td>• Enable Windows Authentication is checked in the Windows Authentication window.</td>
</tr>
<tr>
<td></td>
<td>CIMPLICITY assigns the user a role for the first selected group in which the user is found.</td>
</tr>
</tbody>
</table>

**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 (on page 37) 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:

<table>
<thead>
<tr>
<th>Selection</th>
<th>CIMPLICITY allows access when the user enters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No password.</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>The user's authorized Windows password.</td>
</tr>
<tr>
<td>Windows Domain with Group Mapping</td>
<td>The user's authorized Windows password.</td>
</tr>
</tbody>
</table>

**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.

Duplicate a User

1. Right click on a user that you want to duplicate.
2. Select Duplicate. The Copy User screen appears.
3. In the To text box, enter the name of the new user to which you want to copy the properties of the existing user.
4. Select OK.

Result: The new user appears in the users list and the user properties are copied from the existing user.

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 (on page 58) the User’s **User Properties** dialog box.
c. Re-enable (on 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open a Node ID's Client Properties dialog box.</td>
</tr>
<tr>
<td>(on page</td>
<td>68)</td>
</tr>
<tr>
<td>Step 2</td>
<td>Specify automatic access capability based on User Identification.</td>
</tr>
<tr>
<td>(on page</td>
<td>71)</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) Enter a unique client Authorization Code.</td>
</tr>
<tr>
<td>(on page</td>
<td>72)</td>
</tr>
<tr>
<td>Step 4</td>
<td>Close the Client Properties dialog box.</td>
</tr>
<tr>
<td>(on page</td>
<td>73)</td>
</tr>
</tbody>
</table>
Step 1. Open a 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.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click File&gt;New on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the New Object button on the Workbench toolbar.</td>
</tr>
<tr>
<td>C</td>
<td>In the Workbench left pane either double-click <strong>Client</strong>, or right-click <strong>Client</strong> and select New on the Popup menu.</td>
</tr>
</tbody>
</table>
| 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.

![New Client Dialog Box](image)

4. Click **OK**.

The Client Properties dialog box opens.

![Client Properties Dialog Box](image)

**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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Click Edit&gt;Properties on the Workbench menu bar.</td>
</tr>
<tr>
<td>B</td>
<td>Click the Properties button on the Workbench toolbar.</td>
</tr>
<tr>
<td>C</td>
<td>In the Workbench left pane:</td>
</tr>
<tr>
<td></td>
<td>a. Right-click <strong>Client</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Select Properties on the Popup menu.</td>
</tr>
<tr>
<td>D</td>
<td>In the Workbench right pane, either double-click a client, or right-click a client and select Properties on the popup menu.</td>
</tr>
<tr>
<td>E</td>
<td>Press Alt+Enter on the keyboard.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>In the Default User ID Field</th>
<th>Trusted Check Box</th>
<th>Client Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter a User ID from the list of users available for the project.</td>
<td>Cleared</td>
<td>Users from the Client computer with the selected User ID are automatically logged in.</td>
</tr>
<tr>
<td>2</td>
<td>Leave User ID blank.</td>
<td>Selected</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>Enter a User ID from the list of users available for the project.</td>
<td>Selected</td>
<td>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.</td>
</tr>
</tbody>
</table>
Option | In the Default User ID Field | Trusted Check Box | Client Access
---|---|---|---
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.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Logon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>With administrative privileges</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>With administrative privileges</td>
</tr>
<tr>
<td>Windows Server 2003 R2</td>
<td>As actual administrator</td>
</tr>
<tr>
<td>Vista</td>
<td>As actual administrator</td>
</tr>
</tbody>
</table>

1. Make sure a Proficy CIMPLICITY project is running.
2. Run the CIMPLICITY Genauthcode application on the client to find its unique Authorization Code.
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

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”.

<table>
<thead>
<tr>
<th>Logical name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSM_PTM_APPQ</td>
<td>Threshold limit at which the burst handling code will be initiated. The default is <strong>25</strong>.</td>
</tr>
<tr>
<td>BSM_PTM_AQ_OF_DELAY</td>
<td>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 <code>BSM_PTM_AW_OF_DELAY</code> value to zero causes <code>BSM_PTM_APPQ</code> 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 <strong>50</strong>.</td>
</tr>
<tr>
<td>BSM_PTM_DCQ</td>
<td><code>BSM_PTM_DCQ</code> sets the number of messages from a devcom that will be queued for processing in Point Manager to 200 (default).</td>
</tr>
<tr>
<td>Logical name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>page 77)</td>
<td></td>
</tr>
</tbody>
</table>

**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 (on page 77)**

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 Manager 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
   Notepad opens displaying the

```
[ Logical Names List
* value xxx will be replaced by router at:
* sys$node = local_node_name
* IPCRTRCFG = BSH_ROOT: data\RTR + sys$node+
*--------------------------------------------------------
* logical name | table type | table id | mode
*--------------------------------------------------------
*  SYS$NODE|S|default|10|xxx

* set IPC$LL to ' for multi-node (only)
* IPC$LL|S|default|2|N
* IPC$NODE|P|default|20|MASTER
* IPC$RTR|S|default|10|999
* IPC$LL|P|default|2|N
* IPC$NODE|P|default|20|MASTER
* IPC$RTR|P|default|10|999
*--------------------------------------------------------
* Standard Logical names
```
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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remove CIMPLICITY.</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Remove CIMPLICITY applications.</td>
</tr>
<tr>
<td>3</td>
<td>(Optional) Remove CIMPLICITY Historian</td>
</tr>
<tr>
<td>4</td>
<td>(Optional) Remove Microsoft SQL Server Express 2005</td>
</tr>
<tr>
<td>5</td>
<td>Restart the computer.</td>
</tr>
</tbody>
</table>

**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
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.
<table>
<thead>
<tr>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.17MB</td>
<td>Historian Client only is installed.</td>
</tr>
<tr>
<td>247.0MB</td>
<td>Historian with Historian Client is installed.</td>
</tr>
</tbody>
</table>

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

- Login passwords *(on page 84)*
- Role privilege options *(on page 84)*
- Setpoint security *(on page 84)*
- Setpoint password *(on page 85)*
- Security audit trail *(on page 85)*

### 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 (on page 86)
- Setpoint downloads (on page 86)
- Dynamic configuration changes (on page 87)
- Project login/logout (on page 91)

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:
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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;type&gt;</td>
<td>Entity type being changed.</td>
</tr>
<tr>
<td>&lt;name&gt;</td>
<td>Entity name being changed.</td>
</tr>
<tr>
<td>&lt;user_id&gt;</td>
<td>CIMPLICITY login user name of the user making the dynamic configuration change.</td>
</tr>
<tr>
<td>&lt;OS_user&gt;@&lt;computer_name&gt;</td>
<td>Computer login user name of the user making the dynamic configuration change.</td>
</tr>
</tbody>
</table>

**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:
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1  
(on page 88) | Make sure your role has alarm configuration privileges. |
| Step 2  
(on page 89) | Open the Alarm Definition - $DYN_CFG dialog box. |
| Step 3  
(on page 90) | 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.

![Role Properties - SYSMGR dialog box]

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.

![Alarm Definition - $DYN_CFG dialog box]

- Description: Dynamic config change
- Alarm class: $SYS
- Alarm type: $DYN_CFG
- Help file: 
- Severity: 100
- Alarm message: %s %s %s %s%
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