



Reference Guide

Everbridge Control Center

5.74

This document and the computer software described in it are copyrighted with all rights reserved. Under copyright laws, neither the document nor the software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Everbridge. Failure to comply with this condition may result in prosecution.

The software is the property of Everbridge, protected under copyright law and is licensed strictly in accordance with the conditions specified in the applicable Software License. Sale, lease, hire rental or reassignment to, or by, a third party without the prior and written permission of Everbridge is expressly prohibited.

The Everbridge logo, Control Center and the Control Center logo are trademarks of Everbridge. All other brands, company names, product names, trademarks or service marks referenced in this material are the property of their respective owners.

Everbridge's trademarks may not be used in connection with any product or service that is not the property of Everbridge, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Everbridge.

Everbridge does not warrant that the software will function properly in every hardware/software environment. Although Everbridge has tested the software and reviewed the documentation, Everbridge makes no warranty, representation or condition, either express or implied, statutory or otherwise, with respect to the software or documentation, their performance, satisfactory quality, or fitness for a particular purpose. The software and documentation is licensed 'as is', and you, the licensee, by making use thereof, are assuming the entire risk as to their quality and performance.

In no event will Everbridge be liable for direct, indirect, special, incidental, or consequential damages (including but not limited to economic loss, such as loss of profits, loss of use of profits, loss of business or business interruption, loss of revenue, loss of goodwill or loss of anticipated savings) arising out of the use or inability to use the software or documentation, even if advised of the possibility of such damages. In particular, and without prejudice to the generality of the foregoing, Everbridge has no liability for any programs or data stored or used with Everbridge software, including the costs of recovering such programs or data.

Everbridge's policy is one of constant development and improvement. We reserve the right to alter, modify, correct and upgrade our software programs and publications without notice and without incurring liability.

Copyright: © 2025 Everbridge. All Worldwide Rights Reserved

Contents	
About Control Center.....	5
Control Center Service Architecture.....	5
Licensing Control Center	11
Control Center Windows Client.....	13
Configuring the User Interface.....	22
Permissions & Security.....	43
Control Center System Configuration Window.....	66
Control Center Objects.....	83
Sending Emails From Control Center.....	119
Dynamic Permissions.....	120
Managing Alarms.....	128
Response Plans	281
Graphical User Interfaces	315
Dashboards.....	331
Reports	378
Locations.....	401
Mapping	402
Devices & Extensions	491
Video.....	519
Federated Control Center	542
Import / Export.....	590
Disaster Recovery	602
Failover Clustering	609
Internationalization	611
Servers and Services.....	618
Sensor Service.....	627
Secondary Authorization	631
Threat Level.....	650
Tile Layouts	660

Video Export.....672

Video Surveillance Control Board.....686

Video Wall697

Performance Monitoring and Diagnostics704

Auditing in Control Center707

Client Default Theme726

Configurable Branding731

Object Style Templates.....735

Keyboard Shortcuts for Windows Client737

Event Flood Prevention/Rate Limiting742

Administrator Interface.....746

Known Issues766

About Control Center

Control Center sits at the heart of some of the largest, most complex and groundbreaking security integration projects in the world. It is the ultimate PSIM software-based integration and management platform. It connects and manages disparate building and security technologies such as video surveillance, life critical systems, radar, analytics, HVAC, PIDS, GPS tracking and GIS mapping. Through aggregating intelligence from these systems, it allows organizations to react faster and more precisely to incidents. Control Center provides operators with real-time Situational Awareness through a Common Operating Picture (COP) and following an alert, alarm, or event presents step-by-step process guidance, ensuring complete compliance to security policies.

The recent release of Control Center facilitates the deployment of a greater number of larger solutions, resulting in:

- Faster solution deployment
- More robust solutions
- Significant increase in number of handled alarms

Control Center allows the user to build solutions that implement business workflows around alarms and include a specific entity representing a type of alarm. This makes it easier to define the rules and actions related to a specific alarm, reducing the deployment and maintenance time while increasing the performance of the solution.

Control Center Service Architecture

Control Center uses a scalable Service Oriented Architecture (SOA) platform based on the Microsoft .NET Framework. A Control Center solution will therefore comprise several different services, each performing a specific function, configured to provide a complete PSIM solution.

This approach also provides maximum scope for introducing additional services to meet new requirements.

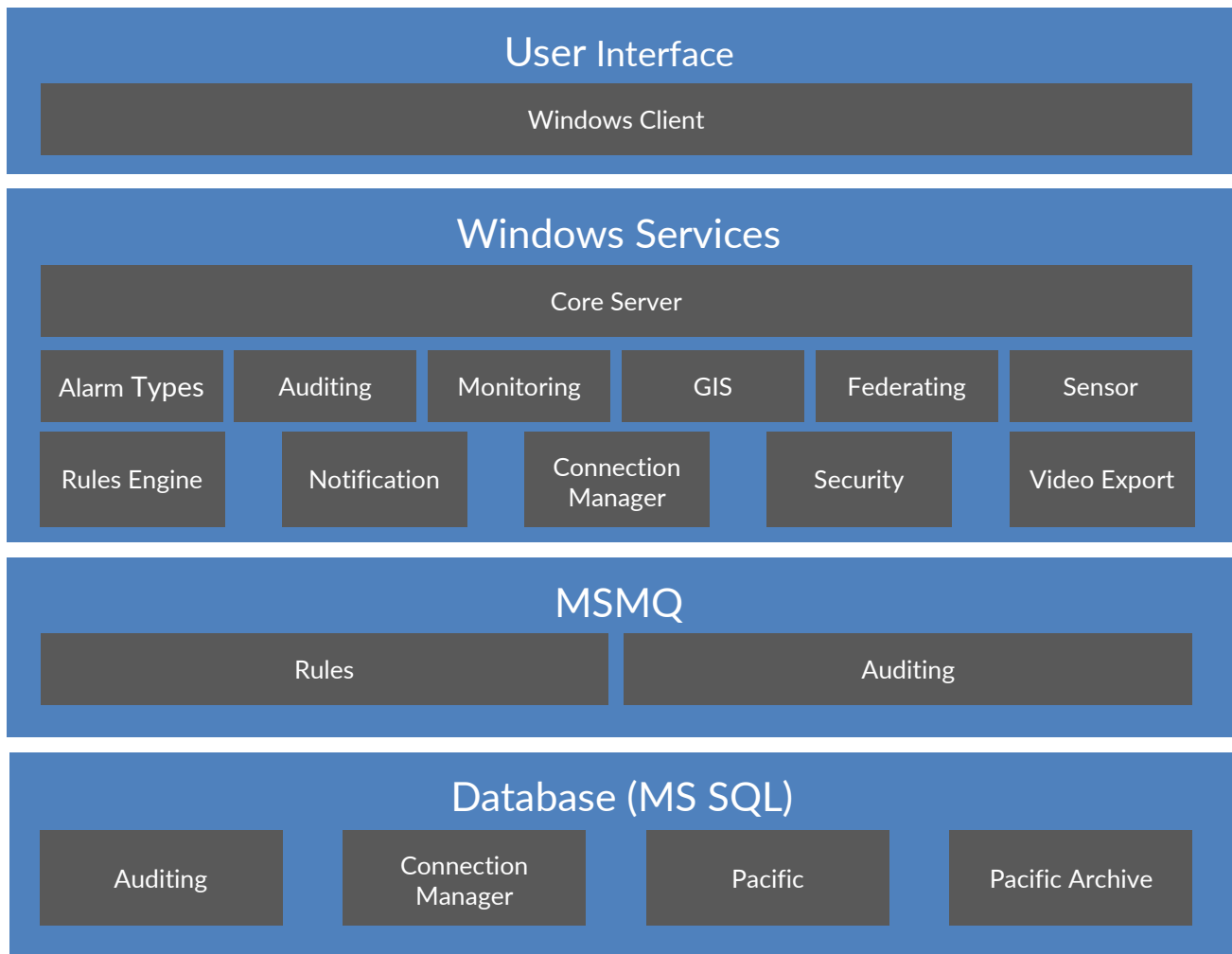
The Control Center installer provides the option to select the components you would like to install. Not all the services are required depending on which aspects of Control Center are to be used. For example, if video export is not required then the video export service does not need to be installed.

Control Center uses Microsoft SQL Server to hold data, therefore the key prerequisite for Control Center is an instance of Microsoft SQL Server. The installer will prompt you for SQL connection details for the database server where the Control Center databases are stored or will be stored. Where a database does not currently exist, for example, on a clean install, the installer will create the database as necessary. You can also specify

custom database names during installation. For more information, see *Control Center Installation Guide*.

Control Center uses a service-oriented architecture to provide scalability and resilience. To facilitate the configuration and maintenance of the different services in a solution, corresponding objects are available within Control Center to represent each service.

- Server Objects - Represent the physical machines running the instance of a service
- Service Objects - Represent the overarching service which is the culmination of all servers



Control Center comprises of the following components.

Service	Description
---------	-------------

Control Center Alarm Types Service	Provides alarm information to the client. Handles CRUD (create/read/update/delete) operations of alarm types in system configuration.
Control Center Audit Server	Logs all audit events in the cnlauding database.
Control Center Connection Manager Service	Provide communications between sub-systems and Control Center.
Control Center Federated Service	Provides the ability to federate independent Control Center solutions. This service is responsible for all communication between the disparate instances of Control Center server.
Control Center GIS Service	Stores and processes GIS information for Control Center.
Control Center Monitoring Service	Provides state information about the different services.
Control Center Notification Service	Provides notification events to Windows Clients; for example, device state changes.
Control Center Open API Service	The interface used by the Mobile App.
Control Center Rules Engine Service	Processes each event logged by devices to determine if any triggers should be activated or an alarm is to be created/updated.
Control Center Security Service	Handles Control Center security.
Control Center Sensor Service	Captures high volume events from sensors and evaluates readings against thresholds.
Control Center Server	Performs all core operations which are not managed by a dedicated service.
Control Center Video Export Server	Performs all video export transactions for all scheduled video export jobs.

Communications Architecture

Control Center Services use three different technologies for service communication depending on the requirement.

WCF

Most Control Center communication is done through WCF:

<https://docs.microsoft.com/en-us/dotnet/framework/wcf/whats-wcf>

Control Center hosts 40+ WCF services across our windows services. These are configured to use NetTcpBinding binding. By default, it generates a runtime communication stack with Windows Security for message security and authentication, TCP for message delivery, and binary message encoding.

<https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/file-schema/wcf/nettcpbinding>

The security configuration settings can be found in the bindings.config file of Control Center Windows services.

SignalR

Microsoft SignalR is used for publish/subscribe notifications:-

<https://dotnet.microsoft.com/en-us/apps/aspnet/signalr>

A SignalR hub is hosted by the Notification Windows service in Control Center to send push style notifications to the client and services for example an alarm or device state update. Signal runs over HTTP or HTTPS if TLS is configured with a certificate.

https://en.wikipedia.org/wiki/Transport_Layer_Security

MSMQ

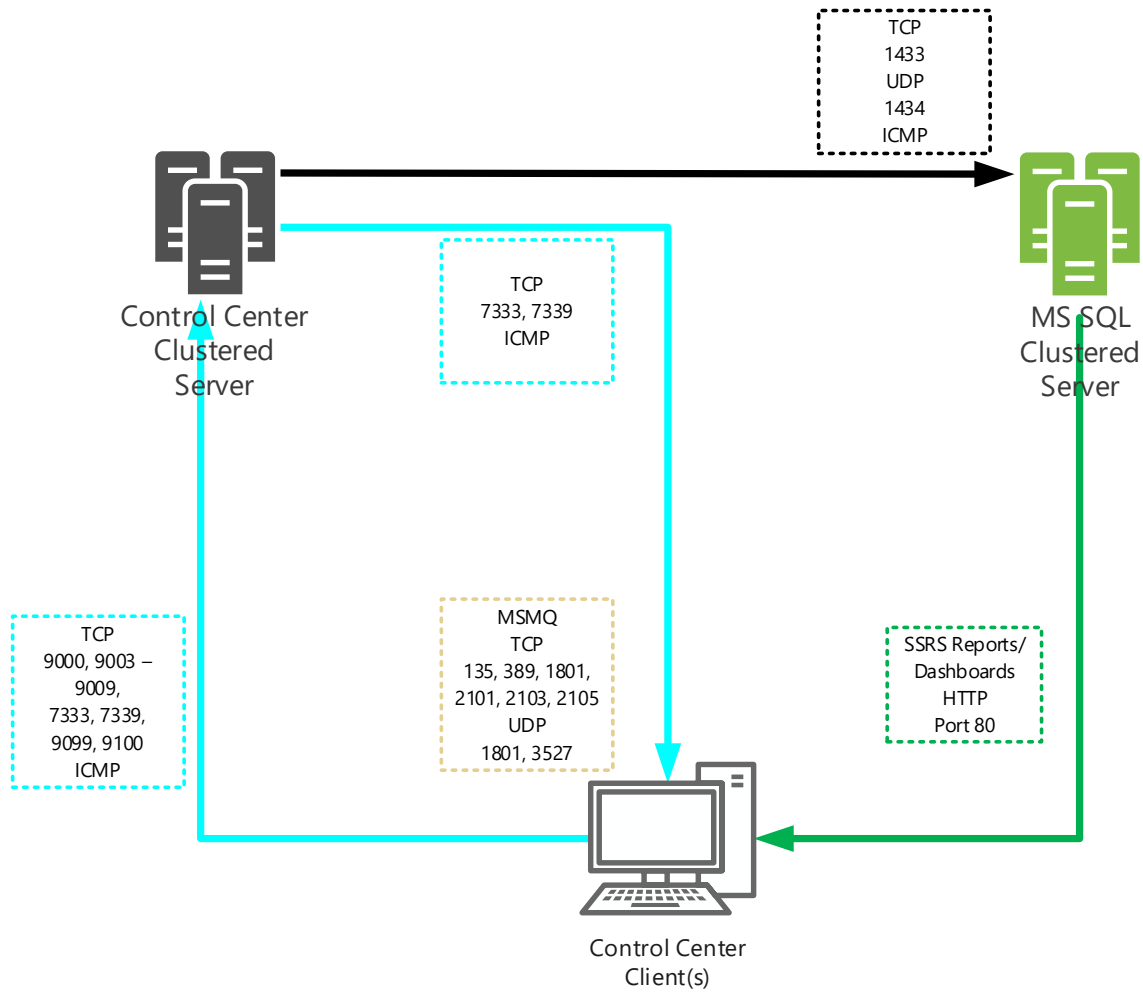
Microsoft message queuing is used by the Rules Engine and Audit Service for guaranteed delivery purposes:- [https://docs.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms711472\(v=vs.85\)](https://docs.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms711472(v=vs.85))

Encryption services provides a secured channel for sending private, 40-bit or 128-bit encrypted messages throughout your enterprise. When private messages are sent, Message Queuing ensures that the body of the messages are kept encrypted from the moment they leave the source queue manager to the moment they reach their destination queue manager. An encrypted message can be decrypted only by the destination queue manager or a connector application.

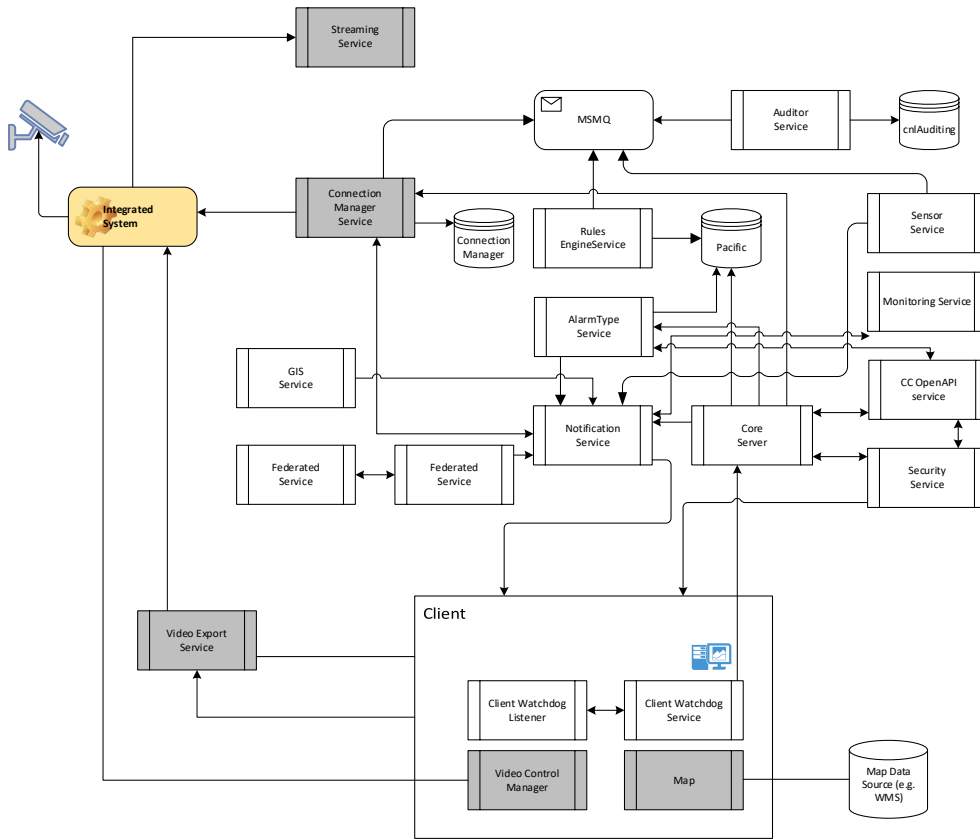
[https://docs.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms700225\(v=vs.85\)](https://docs.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms700225(v=vs.85))

[https://docs.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms705295\(v=vs.85\)](https://docs.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms705295(v=vs.85))

Control Center consists of a number of components that exchange data. This section describes the communications requirements for each component.



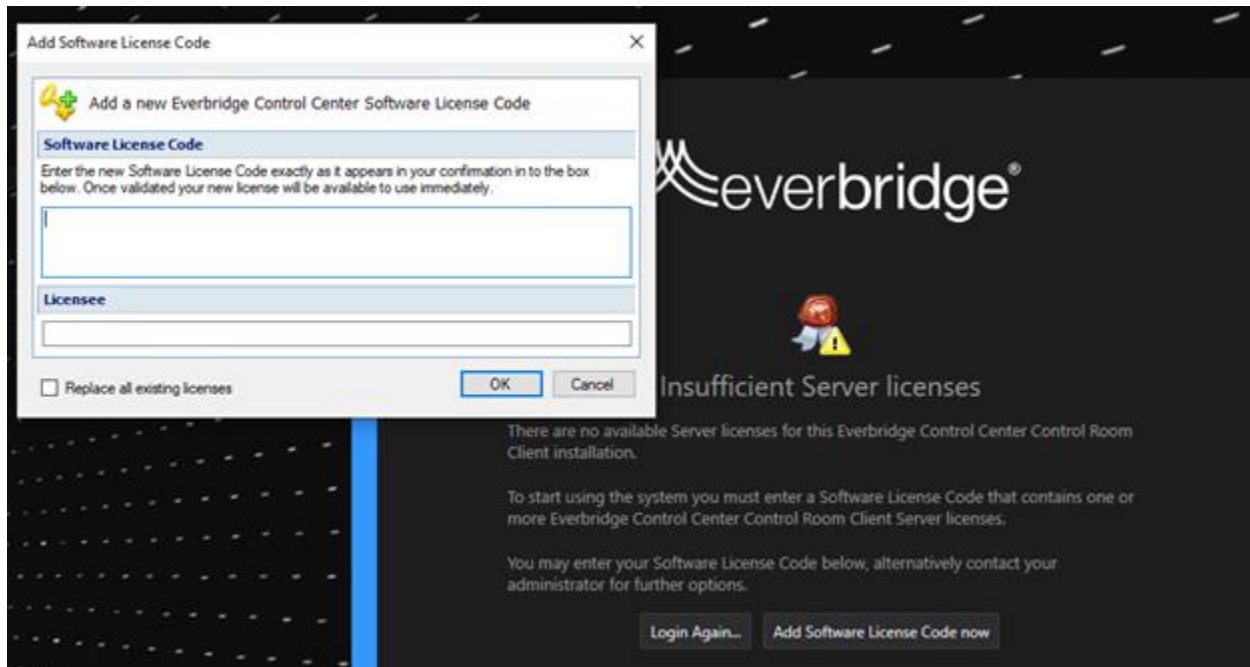
The following diagram illustrates Control Center components and services that communicate directly with non-Control Center components.



For a detailed description of Control Center port usage, see the Installation Guide.

Licensing Control Center

Control Center is licensed using the license code that was entered when logging into the Control Center Client for the first time. Each key specifies the number of server and client licenses, the device modules available, and the number of device license points. If you try to log into a server which has no licenses installed, you are prompted to enter a license code. Enter your license code and Licensee information to continue.



To access the License Manager dialog, in **System Configuration > Toolbar**, click **License Manager**. The **License Manager** dialog appears, which has the following tabs:

- **License Capabilities** – Displays license information such as the Control Center features/capabilities that each of the individual licenses include, a utilization bar to indicate the level of usage of each module, used number of licenses, available licenses, and the total number of licenses available. For example, unless there are enough Control Room Client licenses available in the License Manager, you may not be able to enable the Multiple Logons feature.
- **License Keys** – Displays the quantities of licenses issued, the License Identifier information, the Control Center modules you have access to, and an option to remove the existing licenses available. Control Center supports multiple license codes that unlock additional features. For information about the individual license codes, click License Code.

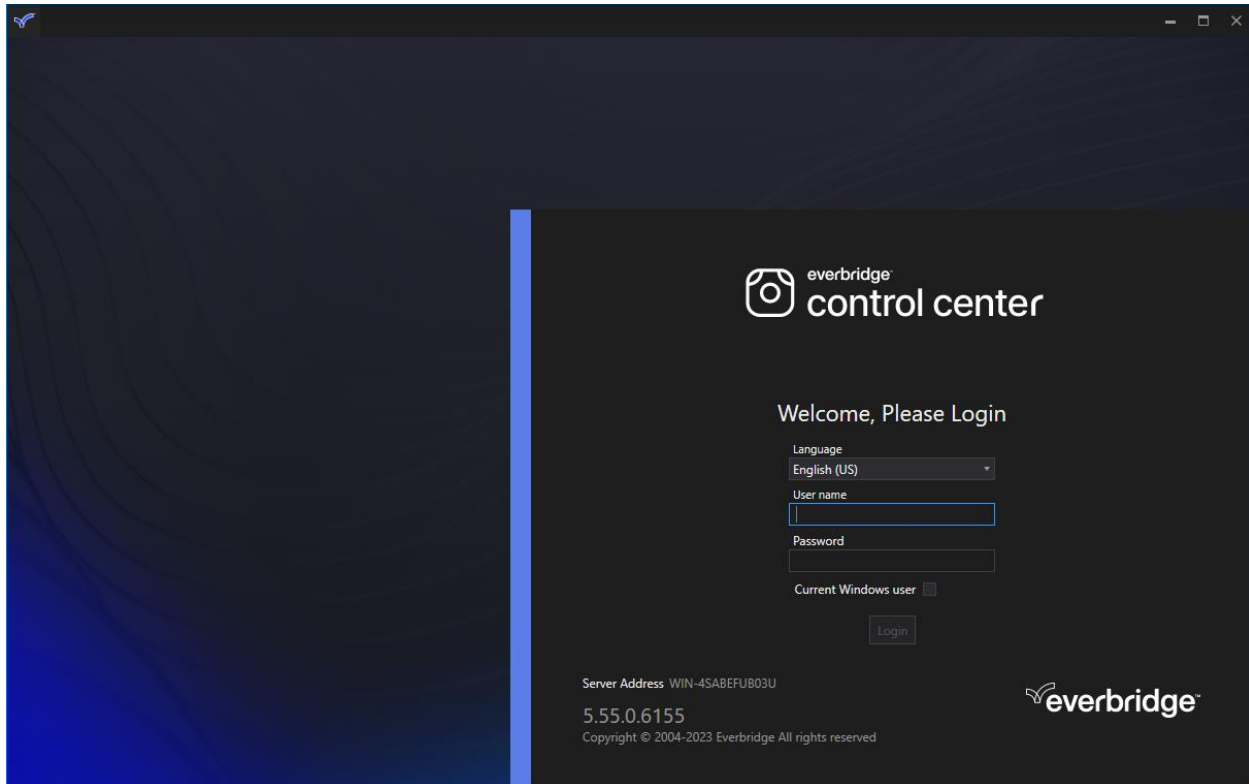
To remove and replace the existing license:

1. In the **License Manager** dialog, click the **License Code** tab > **Remove this code** button. The existing license code is removed and the **Licensed Capabilities** tab appears with no data.
2. Click **Add Software License Code** on the toolbar. The **Add Software License Code** dialog appears.
3. Enter the new License Code, the Licensee Name, and then click **OK**.
4. Select **Replace all existing licenses** to add new software codes without removing the existing license code. This option is useful if you want to add a license with more capabilities and modules in Control Center.

Even though subsequent licenses increment the available components, they do not replace or revoke components made available by previously installed license codes.

Control Center Windows Client

The Windows Client dialog requires a username and password. When logging in for the first time, you must enter the server address, which will be stored for subsequent logins.



The client application is automated to recognize when a server is updated, and to download and update the client software directly.

To log in to Control Center, you must enter a valid username and password when loading the Control Center Windows Client application.

Upon a successful sign-in with the default password, you can change it with a password of your choice in **System Configuration > Users > User**

Logging into Control Center Using Command Line Options

The following command line options are available when running the Control Center Control Room Client.

- `/user:< USERNAME>` - The login username.
- `/pass:< PASSWORD>` - The login password.
- `/server:< SERVER>` - The server to connect to.
- `/port:< SERVERPORT>` - The custom port to which the server should connect.

- `/backupservers` - Backup servers to connect to if the main server is not available.
- `/hideserverdetails` - Obscures the server details from the user when the login box appears.
- `/hidewindowsauth` - Removes the ability for the user to choose login as current user.
- `/currentwindowsuser` - Attempts to login to Control Center using the currently logged in Windows user.

To use these command line options, you must always select **Run as Administrator** and add the appropriate command line option to the Windows Shortcut for the Control Center Client application. For example:

```
"C:\Program Files  
(x86)\Everbridge\ControlCenter\ControlCenter Client\ccrc.exe/user:root  
pass:123456 /server:democccsc.everbridge.com /port:1234" /hideserverdetails
```

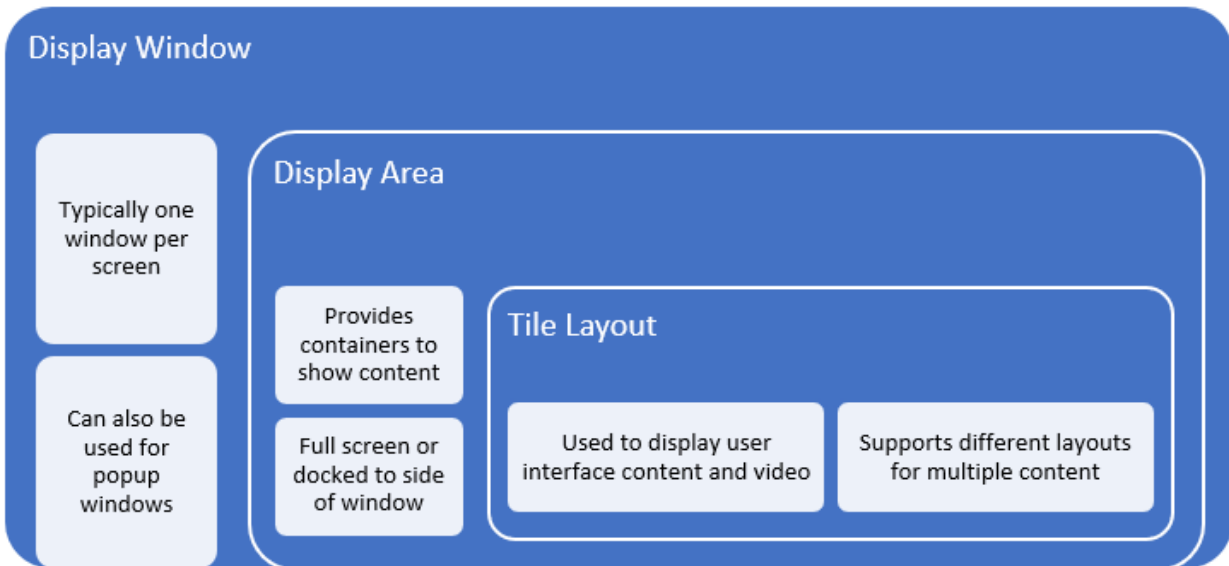
Or

```
"C:\Program Files (x86)\Everbridge\ControlCenter\ControlCenter  
Client\ccrc.exe" /currentwindowsuser/server:democcc.everbridge.com
```

Multiple command line options can be added to the shortcut as shown above.

Control Center User Interface Structure

The Control Center user interface constitutes various components that provide complete flexibility over where content should be shown within the Client.

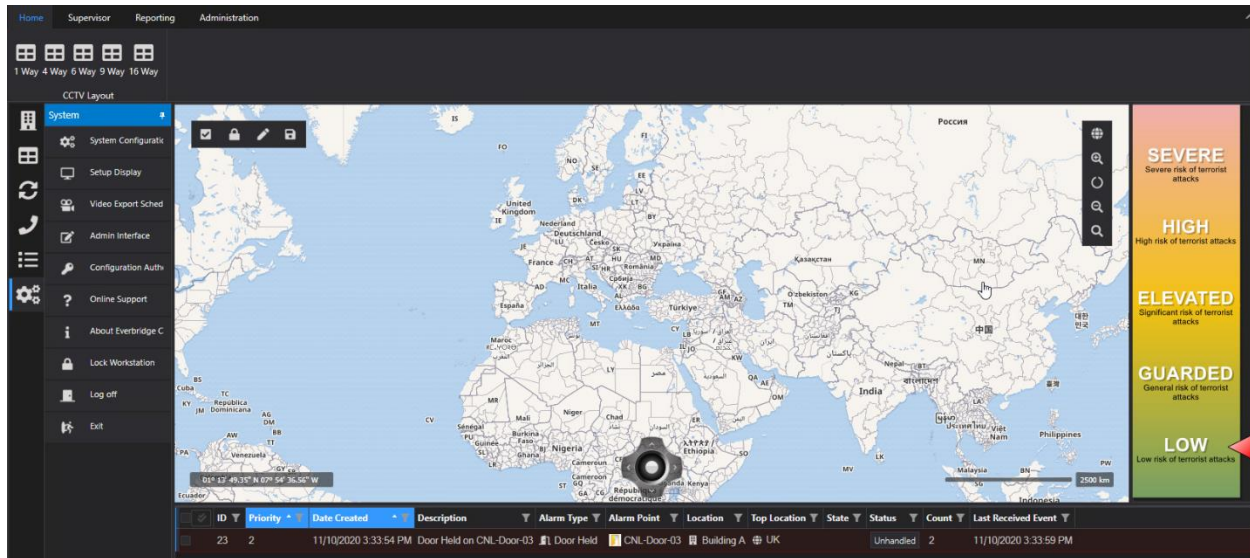


When installing and logging into Control Center for the first time, a default user interface will be shown consisting of a single display window, which can be renamed, and a default display area set to fill the display window. For more information, see [Default User Interface](#).

The solutions engineer must create the necessary display windows and area to satisfy the user interface requirements for the solution. This can include any number of display windows and display areas based on the number of screens available and the content shown. The display configuration can also be cloned from one client to another for easy replication of the setup.

Default User Interface

By default, Control Center comes packaged with system user interface components and displays them when the Client connects to the server. This includes a default display window with the Main Menu docked to the top of the window, the System Explorer docked to the left of the window, and a Status Bar in the lower part of the screen as shown in the screenshot below. The default window also includes the System Main display area which can be used to show content such as maps to the end user.



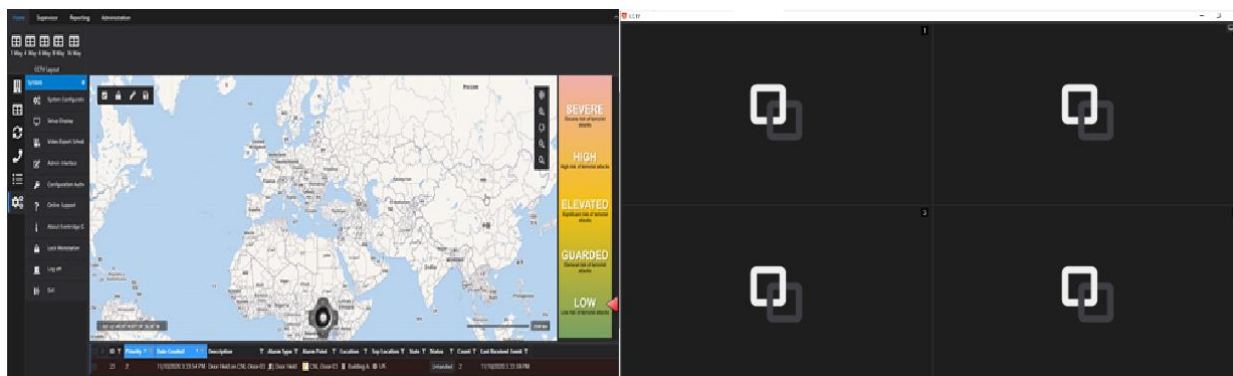
The default user interface comprises the following options:

- **System Menu** – The menu for accessing all the system features in Control Center. For example, to access System Configuration and Admin Interface.
- **Map toolbar** – Displays the options available to modify map settings/display.
- **Map Display** - By default, a new installation of Control Center shows maps for the selected locations. This is implemented in the **System Explorer** user interface. **System Alarm Stack** can be configured to display from the alarms generated.
- **Status Bar** – Shows Health Check connected to the Administrator Interface, Device Licenses that are currently being consumed by the system, the current user, client, and server names.
- **System Explorer** – Displays the details of locations and assets within each location in a hierarchical view. It also includes fast search capabilities and can be configured by accessing the System Configuration window > System Objects > System Explorer GUI.
- **System Main** – Main display area to display maps, tile layouts, dashboards, and so on for the end user.

You must first configure the user interface to include display windows and display areas to show the required user interface.

The alarm stack and alarm control display areas are docked to the sides of their respective windows. The System Main and Video Workspace display areas are set to fill their respective windows. The Video Workspace display area in the following example contains a blank 2x2 tile layout, which demonstrates how a tile layout can be used to segment a single display area into different tiles.

The following is an example of a typical two-screen configuration:



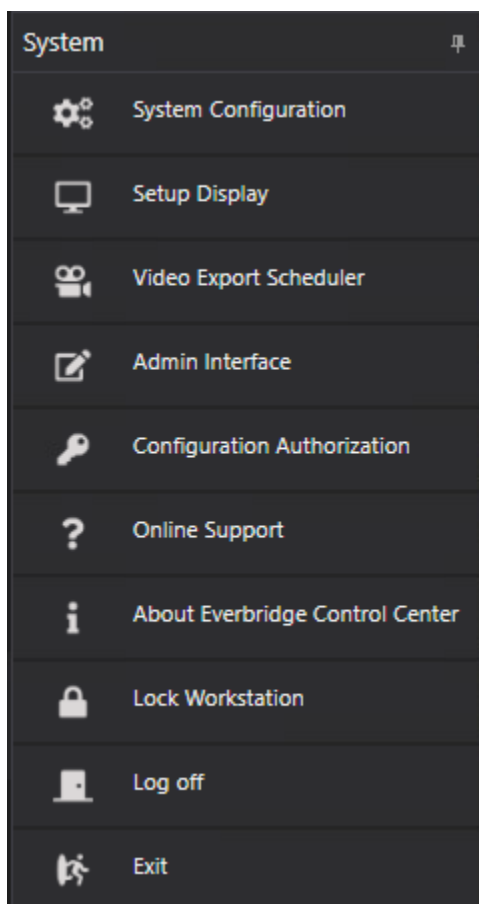
System Menu

System Menu can be accessed by selecting **System**.



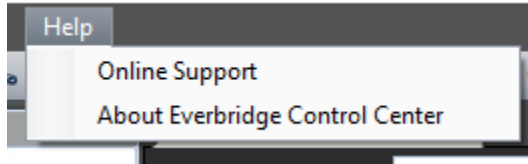
Option	Description
System Configuration	Opens the System configuration window

Setup Display	Open the setup display window for creating new window and display area.
Video Export Scheduler	Opens the Video Export Scheduler window.
Admin Interface	Opens the Admin Interface window
Online Support	Takes you to the URL Address it is defined with
About Control Center	A summary about Control Center
Lock Workstation	Locks the workstation. The user need to authenticate before logging into the client.
Log off	Logging off as the current user
Exit	Exit Control Center



A URL address can be set by the administrator for online support in the Enterprise Settings as follows:

1. Go to **System Configuration**.
2. Click on **Global Settings** tab on the top ribbon.
3. Select **Enterprise settings** from the options in the left pane.
4. Enter a URL address for the support URL option available in the right window. If this field is left blank, then the Online support option will not be shown in the System Menu or in the help menu of System Configuration.

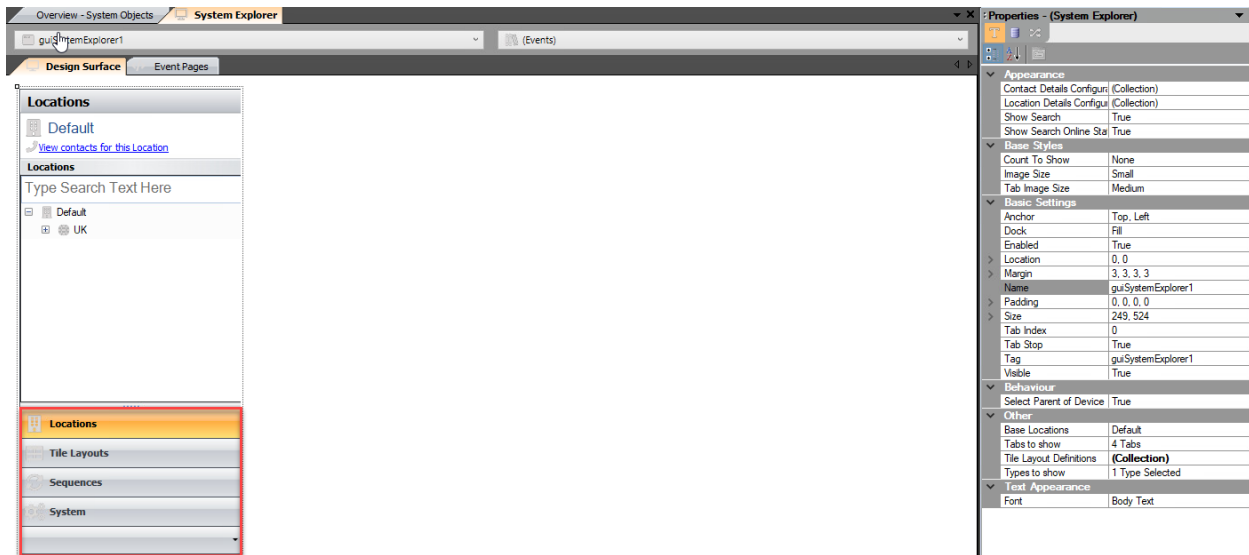


5. Click **Apply** to save the settings.

Configuring How System Tree Displays

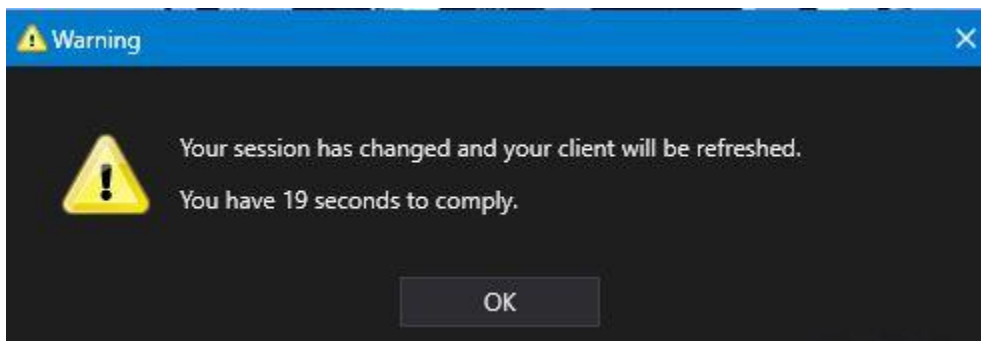
The left pane on the main display screen is the System explorer or System Tree. You can configure how your system explorer is displayed.

1. Go to **System Configuration > My Organization > System Objects**.
2. From **Overview - System Objects** tab, navigate to **Graphical User Interface** and double-click **System Explorer**. The System Explorer GUI opens in design view so you can edit it.
3. From **Design Surface** tab, select one of the tab controls to display the properties pane. You can amend these properties, depending on your requirements. For example, you can change the size of the icons by selecting a size from the **Tab Image Size** drop-down list.



Reconnected to the Server

When the network connection is restored, the lost connection to the server will automatically be established using the user credentials entered previously and the client session (if not expired) will be restored if SSO is in use, without the need to login again. A session changed event will be triggered to notify the user for any missed notifications during the outage.

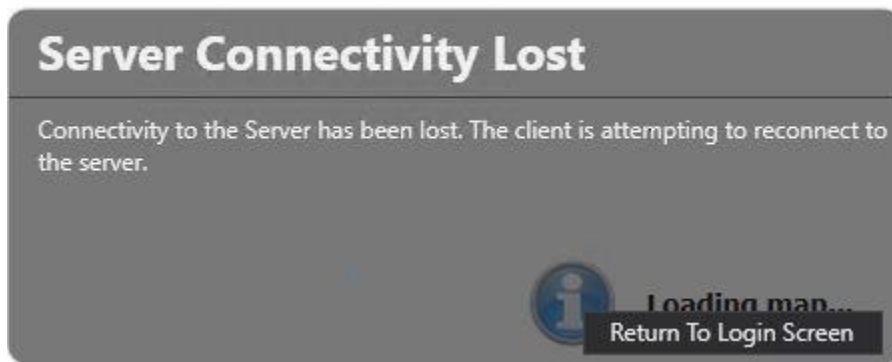


If the client has been disconnected longer the session duration itself, then the user will be taken back to the login screen.

Disconnected from the Server

A server in a Control Center setup can be connected to several clients deployed at various sites in a federated system. The client may have a video wall which receives the video feed from many devices installed at the site. There are instances when the client loses connection with the server due to network issues but may be required to continue relaying the video on the videowall and keep trying to connect to the server in the background until it is successful.

This feature is made available to facilitate the client to remain alive and allow the user to view the video wall. However, the user is restricted from performing any actions on the client until it gains back connection to the server. An error message window pops up as shown below when the connection is lost, but the video wall will continue to receive the video feed from the devices at the site. This does not obscure the video in the background and the error message window can be moved to the corner of the screen to keep the video display clear.



In this scenario, the user can choose to click on the **Return To Login Screen** button, to go back to the login screen.

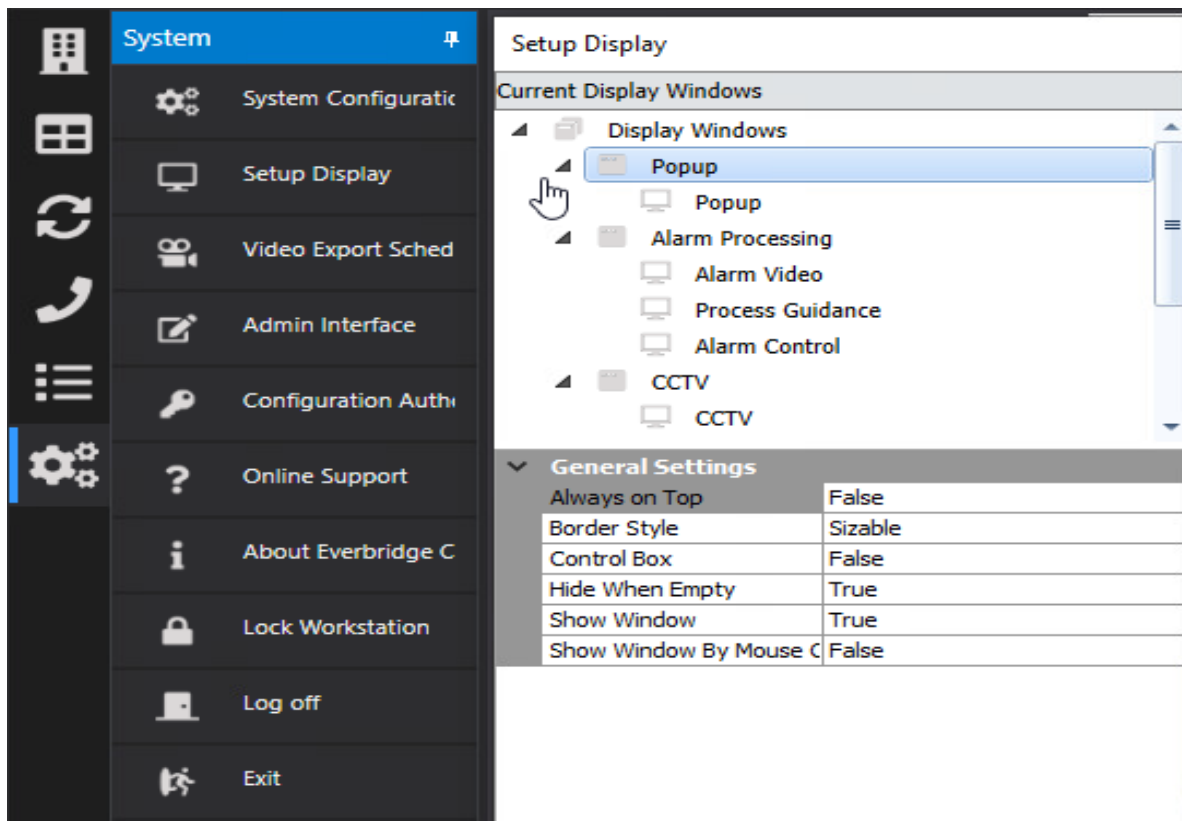
Configuring the User Interface

Setup Display

You must configure the system before it can display a video feed or Graphical User Interface (GUI) on the Control Center client. This requires adding display windows and display areas in the **Setup Display** dialog.

- **Display Window** – Serves as a blank canvas where you can place one or more display areas. The Display Window enables individual customization of the workspace.
- **Display Area** – Available within the Display Window, you can set the Display Area to fill the window or docked to an edge.

You can configure display for Control Center client using the **Setup Display** dialog, by going to **System > Setup Display**.



The display configuration is held on a per-client basis and must be setup for each client that is connected to the same server.

The **Setup Display** dialog enables you to add, rename, and remove several display windows and display areas.

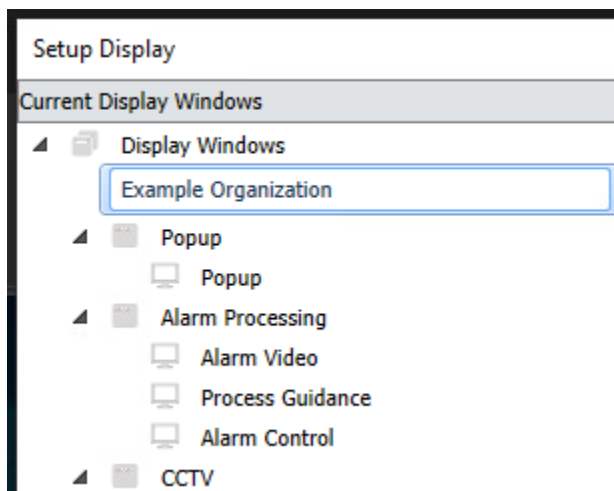
You can also copy the display configuration from one client to another using the **Clone From** button in the **Setup Display** dialog. This is helpful if you want to run several clients with identical screen configuration settings.

Renaming Default Display Settings

You can change the label of a display window in the **Setup Display** dialog. By default, the main window is displayed as **[enter customer name here]**.

To rename a display window:

1. Click the display window that you want to change to enter the edit mode.
2. Specify a new name, for example, **Main**.



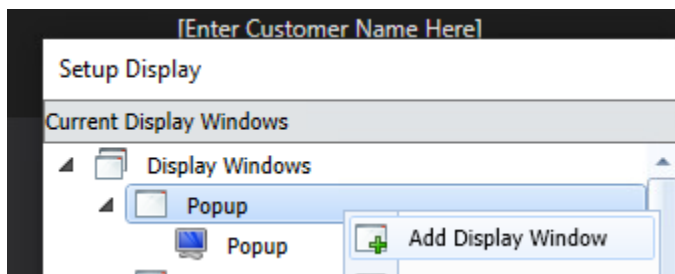
3. Click **Save**.

Adding a Display Window

You can add additional display windows from the context menu.

To add a display window:

1. Right-click the **Display Windows** node to show the context menu.
2. Click **Add Display Window**.



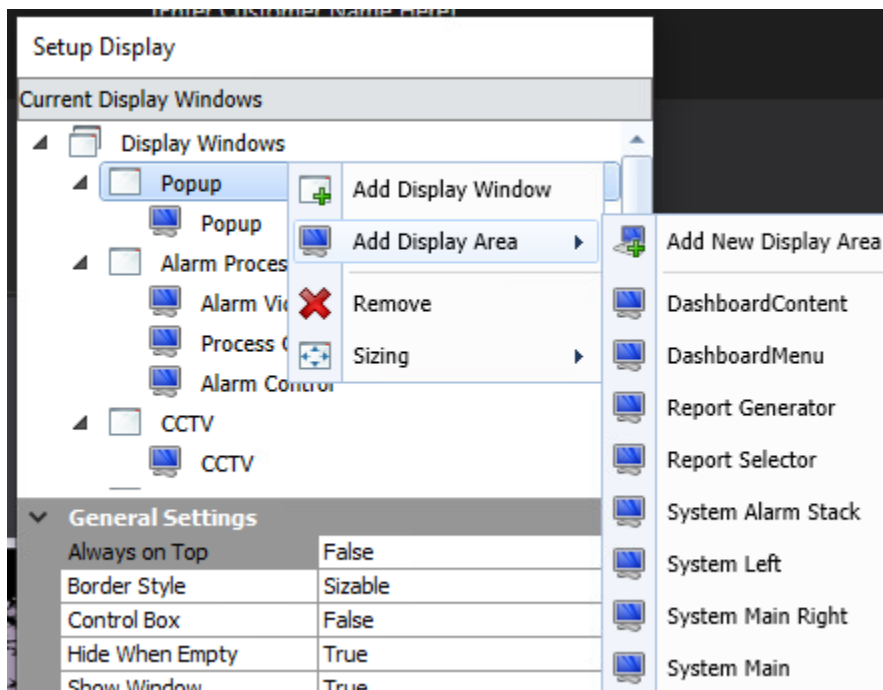
3. Specify the window name as **Right**.
4. Click **Save**.

Adding a Display Area

You can also add display areas to a display window using the context menu.

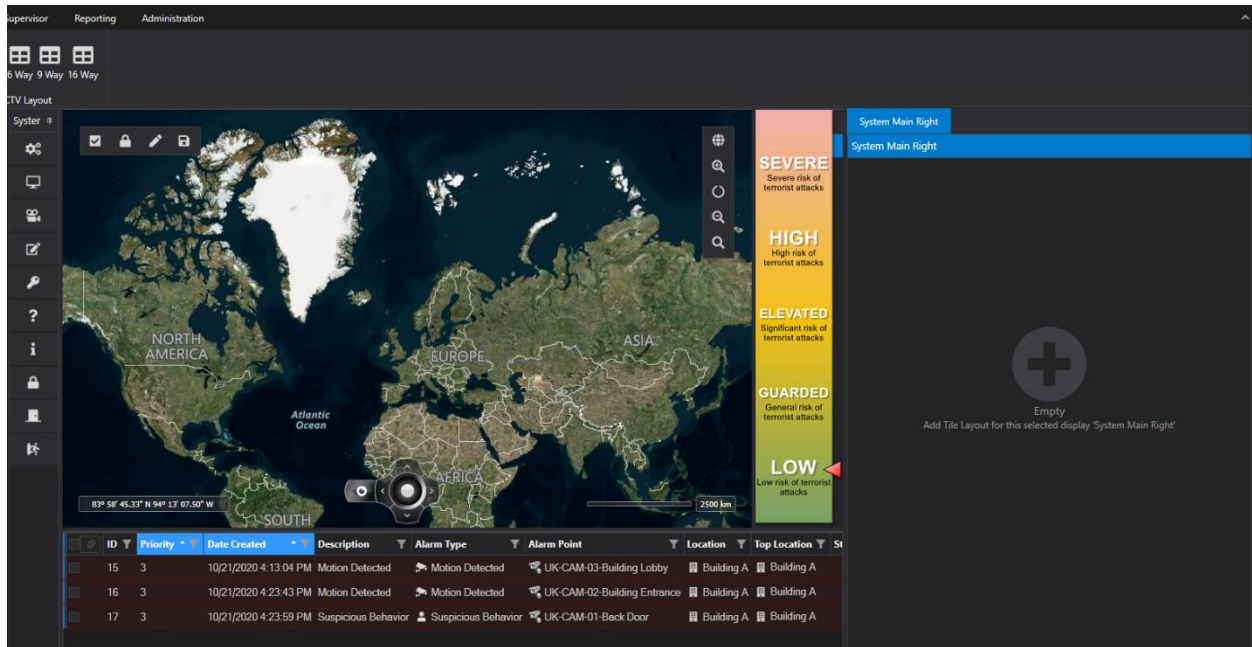
To add a display area:

1. Right-click the new display window called **Right**.
2. Click **Add Display Area > System Right**. **System Right** appears in your **Setup Display** dialog.



The configuration of the display area is stored in the Client. Display windows only exist within the configuration, whereas display areas are created as objects within the Control Center solution and can therefore be referenced through the system. For example, to show a camera into a display area.

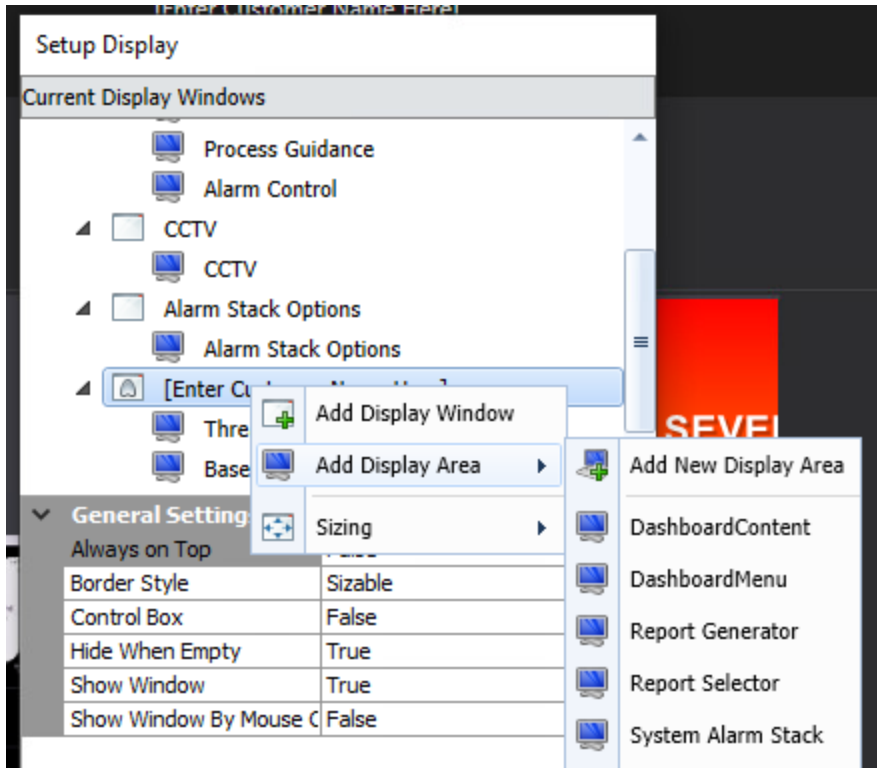
3. Click **Save**. The right display window is now configured.



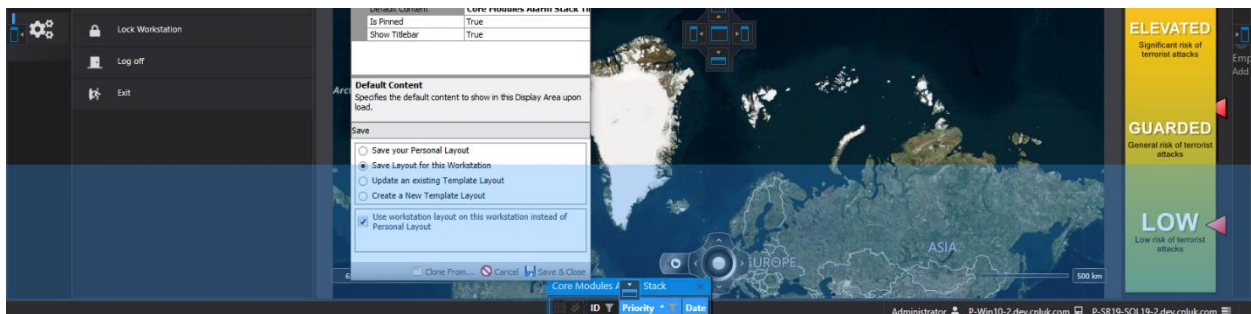
Adding the System Alarm Stack

To add the System Alarm Stack to the Main display window:

1. Right-click the **Main Display** window.
2. Click **Add Display Area** and select **System Alarm Stack**.



- From **Properties**, set **Container Type** to **Docked**. This enables you to drag and drop the display area using the title bar to another part of the display window.
- While **Setup Display** is still open, click the title bar and drag the display area to another part of the **Display** window.



- Ensure that all the windows are configured the way you want to display your display windows, click **Save**.

The size and position of the windows is retained in the client record when saving. Therefore, the display windows returns to the last saved size and position upon logging into Control Center, if they are subsequently moved.

To close the dialog box without committing changes to the database, click **Cancel**.

Theming Customized Graphical User Interface Controls

Theming can be applied to customized Graphical User Interfaces. Theming applies to a sub-set of the controls:

- Alarm Activity Grid
- Button
- Checkboxes
- Comments
- Date/Time
- Drop-down lists
- Form panels
- Labels
- Link Labels
- Listboxes
- Manual Alarm Types Comb Boxes
- Number
- Panel
- Paragraph Text
- Resolution Types Combo Box
- Single Line Text
- Section breaks
- Table layout panels
- Titles. **Note:** If a Title control is themed, then then the **Background Image Mode** property becomes redundant.

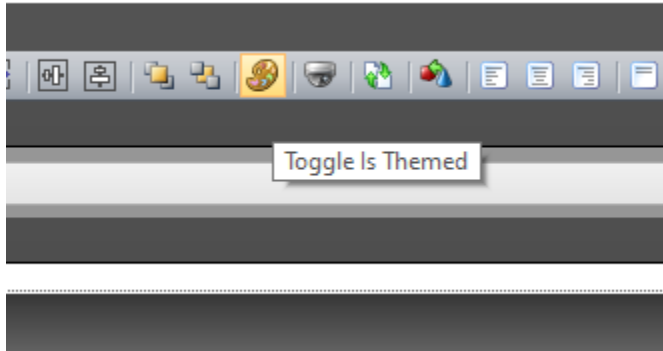
Theming is enabled by default.

To disable theming:

1. From **System Configuration**, navigate to the GUI control that you want to untheme. To do this, you can either:
 - If it's an existing GUI, double-click the GUI whose control you want to theme to open the GUI editor.
 - If it's a new GUI, create the new GUI, drag the control you want to the **Design Surface** tab.
2. Select the GUI control. If theming is available for the control, the **Is Themed** property displays in the **Property** page.
3. Set the **Is Themed** property to **False**.

4. Reload the form, for example, by logging off and on again. The theme you have configured in the Modern Client Theme is no longer reflected in your GUI control. See [About Modern Client Default Theme](#) for more information.

The **Is Themed** property can be updated for all the controls within the current GUI at the same time by selecting the **Toggle Is Themed** button on the toolbar. The **Toggle Is Themed** button is only available in the GUI editor.



Configuring Control Box Icons

You can also enable and disable the Control Box icons: Minimize, Maximize, and Close to show or hide on the Setup Display window.

The Close icon appears only on the Main Display window and Minimize and Maximize icons are supported only on other Display windows.

The Close icon that appears on the Main Display window follows the security policy that prevents exiting the Control Room Client. If a user without authority attempts to close the window using the Control Box icon or the Task Bar Close, then the security policy requests that a user with appropriate permission confirm the action by entering a username and password.

If the user ends the Control Room Client Process using the Task Manager, then Control Center will be unable to intercept it. Therefore, ensure that a Group Policy preventing user access to Task Manager is implemented.

Saving Display Layout Configuration

A layout records the size and arrangement of windows in the application. Changes made to the layout by end-users at runtime are not automatically saved. After the user has logged out, the user changes are lost. Upon logging back in, if the user wishes to see the same set of applications open, windows properly positioned, URL's, files or directories opened as needed, he will have to iterate the same set of steps to recreate the setup. Control Center now provides a solution that allows the user to save the layout manually when the application closes and restore it when the application is restarted.

For instance, if a workstation needs to load a video wall and play video from the cameras it is configured to each time it is logged in, regardless of the user, then the administrator can configure the video wall settings and save it for the workstation. So, every time a user login, the video wall pops up and starts to receive the video feed.

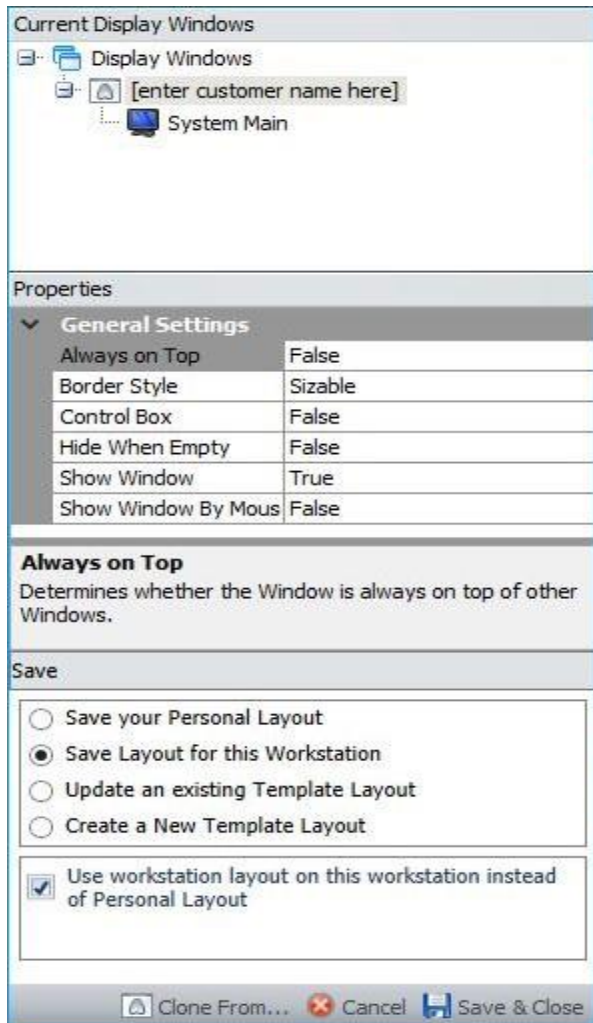
The Setup Display dialog has been updated to support saving layouts against a user, client or saved as a template for future use. Several layouts can be saved, and a desired layout can be restored when needed.

When the display setup is saved for a user, the software will load the user's layout regardless of client workstation. By default, user layout always takes precedence unless chosen otherwise. Saving of templates has been updated to allow users to specify the template name.

The Setup Display window will now show four save options and an optional check box to allow the software to load the client layout regardless of user. The four options are listed as below:

- Save your personal Layout - saves the layout for the user
- Save Layout for this Workstation - Saves the layout for the Client or workstation
- Update an existing template layout - Changes made can be saved to the current template being used
- Create a New Template Layout - Creates a new template

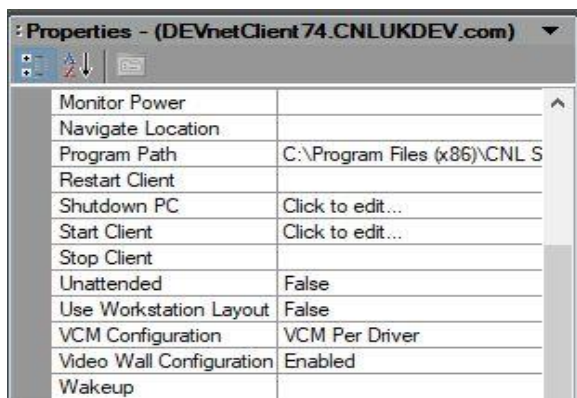
The optional check box shown below, when ticked will ensure that the Client layout is always loaded regardless of the user.



When the user has logged in, and wishes to choose another layout, it can be achieved by clicking on **Clone From** at the bottom of the Setup Display window. All saved layouts and templates are displayed. The user can choose from the list displayed and the layout will be applied straight away

You can also create a new template for the client or edit the existing one for any changes and save it for future use.

A hot key can also be defined to save a layout against a client or a user. When the **Use Client Layout** property for the windows client object is set to true, then the layout is saved against the client. It will be saved against the user if set to false. A message will be displayed to confirm against whom the layout was saved.



A new type permission **Layout Configuration** is also introduced to restrict users from saving or updating the layouts. The Administrator can grant/deny access to a user or groups for saving the layout and templates for the user or for a workstation.

Grouped by:		Permission Type			
Type	Allow	Can Read	Allow	Can Write	
GIS Layer Manager	Allow		Allow		
Global Settings	Allow		Allow		
Icon Manager	Allow		Allow		
Import	Allow		Allow		
Layout Configuration	Allow		Allow		
License Manager	Allow		Allow		

Positioning of Display Areas

Control Center provides an enhanced user capability to dock/undock and pin/unpin the display areas to correspond to the user needs.

You can now position floating display areas anywhere in the application. Docked display areas always remain connected to the window and occupy a unique position in the window frame. It can also be combined with other docked display areas in the same position into a tabbed collection.

Configuring the Display Area

Four properties allow users to dock or pin a display area to enhance user experience, as listed in the table below.

Property	Description	Value	Function
----------	-------------	-------	----------

Allow User Docking	Allows the display areas whose container type property is not full screen to be docked	True/False	Allows the user to Dock/Undock the Display area Note: For the Display area to be able to move to a different location and be docked 'Allow Float' Property must also be True.
Allow User Float	Allows the display area to float about and be placed anywhere in the application	True/False	Allows the user to drag the display area and place it anywhere in the application or dock it at a desired location.
Allow User Pinning	Allows pinning/minimizing of the display areas	True/False	Allows pinning of the display area so that they continue displaying in its place or minimized when unpinned. Setting this property to True will allow the user to pin/unpin the display area.
Is Pinned	Determines the Initial state of the display area when logged in	True/False	By default, it is set to True. The display area will be displayed in its position when the application loads up. This can be changed anytime during runtime to false to minimize the display area.

Properties	
Display Area Appearance	
Allow Drop	False
Allow Tile Menu	False
Allow User Docking	True
Allow User Float	True
Allow User Pinning	True
Border	False
Hide When Empty	False
Tile Aspect Ratio	Fill
Tile Layout Aspect Ratio	Fill
Tile Menu Mode	All
Workstation/Personal Configuration	
Container Type	Docked
Default Content	System Alarm Stack
Is Pinned	True
Show Titlebar	True

Only Administrators or users with Administrative rights or users with Type permission **Layout Configuration** set to Allow will be able to modify the above-mentioned properties. However, the administrator can set the properties for the end user to be able to dock or pin a display area.

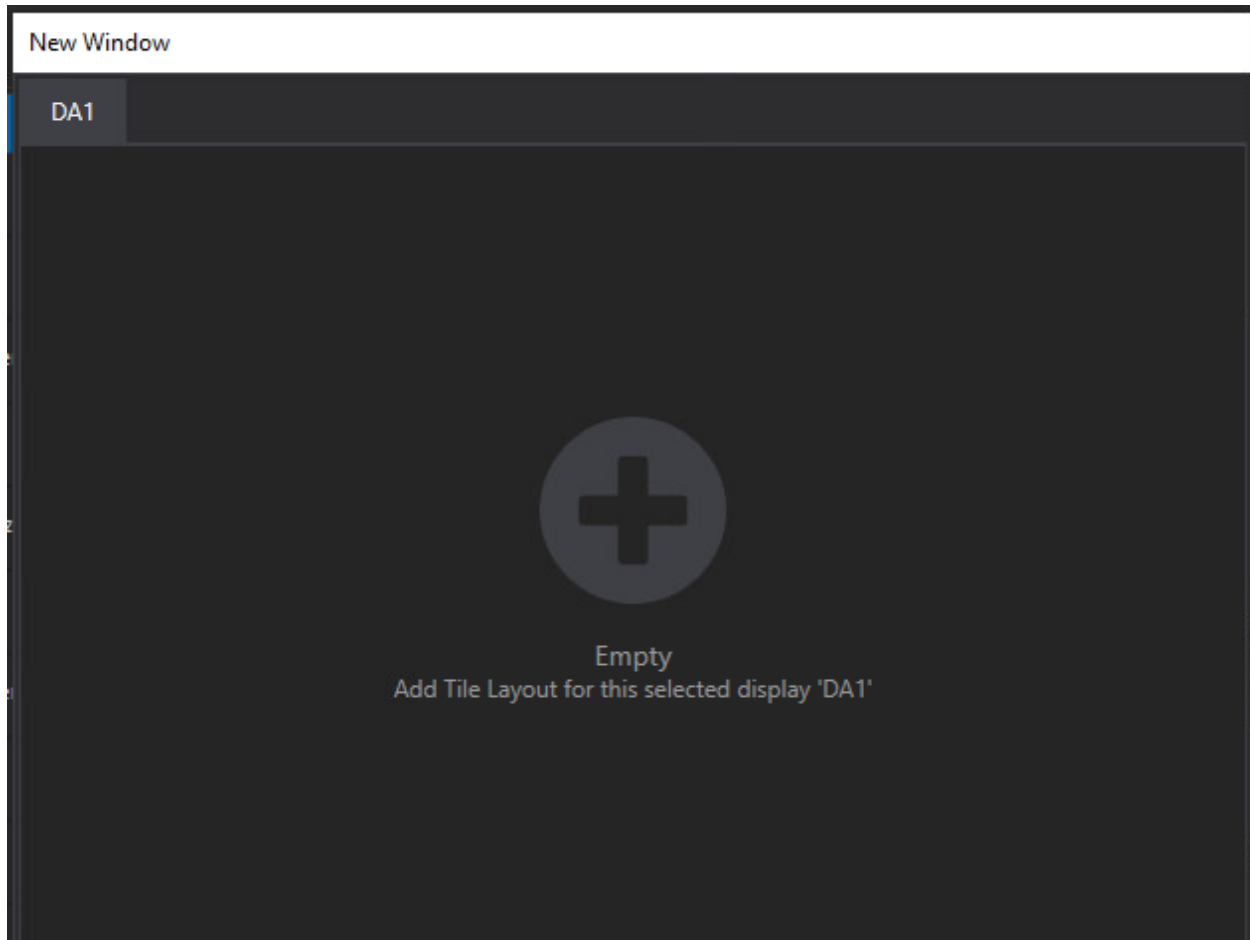
Grouped by: Permission Type				
Type	Allow	Can Read	Allow	Can Write
GIS Layer Manager	Allow		Allow	
Global Settings	Allow		Allow	
Icon Manager	Allow		Allow	
Import	Allow		Allow	
Layout Configuration	Allow		Allow	
License Manager	Allow		Allow	

Points to be Noted Before Upgrading to Version 5.9

When you are upgrading to version 5.9, there are a couple of behavioral changes you may notice and some work around to make it look like your display from the previous versions:

1. Display area tab is shown even when there is only one display area in the window. If you have a display area with container type set to **Fullscreen**, the window will still show a tab at the top left corner. This can't be hidden at the moment even when there is only one display area to show. The users with administrator rights

can however set the display area to 'docked' which will hide the tab from the display.



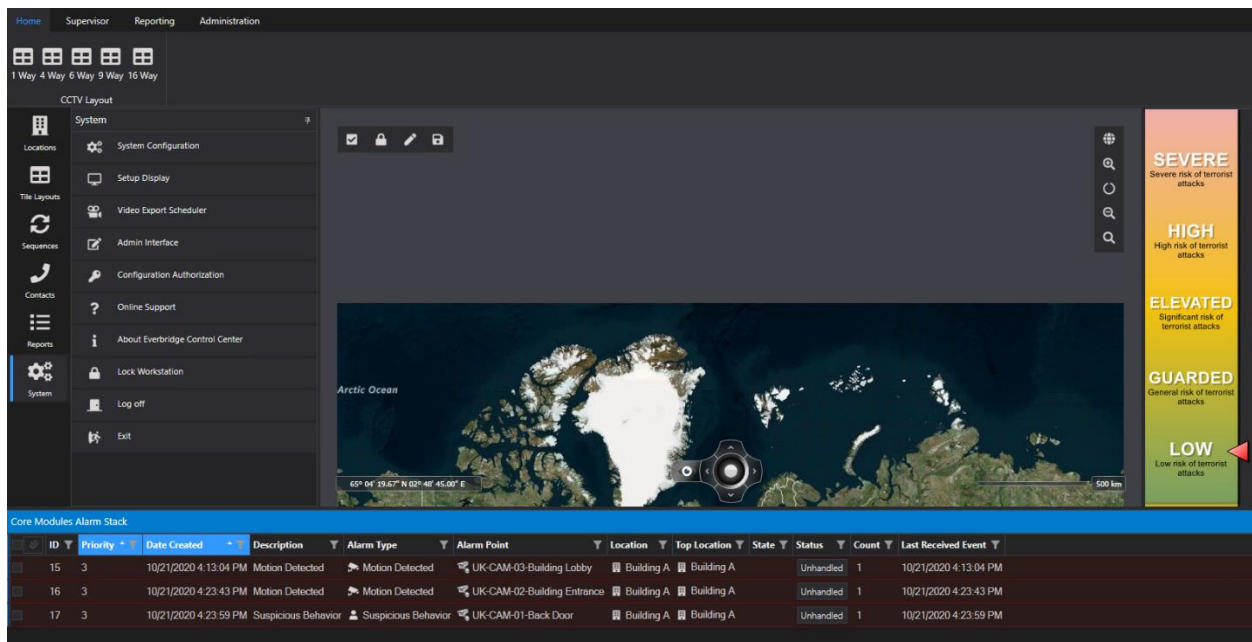
2. By default, the docking and pinning properties for all display areas (**Fullscreen** or **Docked**) are set to false. Hence, they cannot be dragged out of its place or docked elsewhere unless the administrator changes the property to **True** in the **Setup Display** window. But the **Fullscreen** display area stays in its place regardless of the property set on it. However, the System Main is seen to behave slightly differently. Although it is of **Fullscreen** container type it can still be dragged out of its place. To avoid the end users doing this, the administrators can do one of the two workarounds mentioned below:
 - Set the **Allow User Docking** and **Allow User Float** properties to **False**
 - Set the **Show Titlebar** property to **False**

Pinning and Unpinning the Display Area

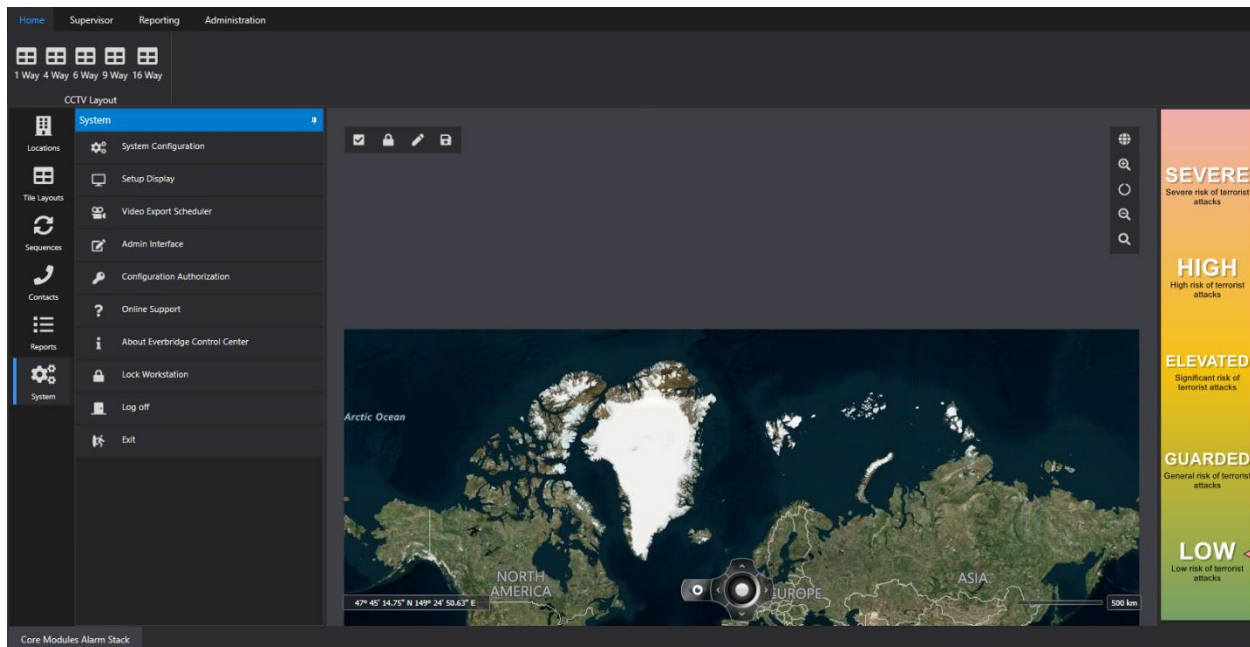
A display area can be minimized if the user is allowed pinning. The administrator can set the **Allow User Pinning** property in the **Setup Display** window to true for the user to be able to minimize the display area.

If for instance the **System Alarm Stack** display area is created and docked below the **System Main** window, and is allowed pinning, you will be able to minimize the Alarm Stack, either by clicking on the pin at the top right corner of the window or by setting the **Is Pinned** property in the **Setup Display** window to false. However, in minimized state, when a new alarm gets populated in the stack, the title bar of the alarm stack starts to blink to alert the user. The user can choose to hover over the title bar to temporarily expand the window and view the alarms and then click anywhere on the application to collapse it. If the window needs to be restored to its original state, the user needs to click on the title bar of the window.

System Alarm Stack Pinned



System Alarm Stack Minimized



Notes:

- When the System Main is set to container type **FullScreen** and unpinned, upon hovering on the tab, the content isn't visible. The user will have to click on it and pin it to see the contents again.
- When you log in with the upgraded Control Center Version 5.9 you will not be able to drag the System Explorer or dock it. However, if the system explorer window is unpinned and pinned back to its place you will be allowed to drag it out of its position and either float it or dock it into another position.
- When the alarm stack with multiple views is minimized/unpinned, the user is not able to pin it back to its position. Upon hovering the alarm stack temporarily opens but does not allow to be pinned. The suggested workaround would be to click on the highlighted bar at the bottom of the minimized view as shown in the picture below which brings the alarm stack back to life and then pin it.

Floating a Display Area

A floating display area is not connected to any window, hence, can be moved anywhere in the application and will always appear in the foreground, in other words, it cannot be hidden behind the window. To make the floating window active you need to click on its title bar

To be able to secure the floating display area and not accidentally loose it, the **Show Titlebar** property in the **Setup Display** becomes insignificant and bear no changes regardless of the value set to the property. This is because the title bar is always used to move the display area around.

To float a display area, do the following:

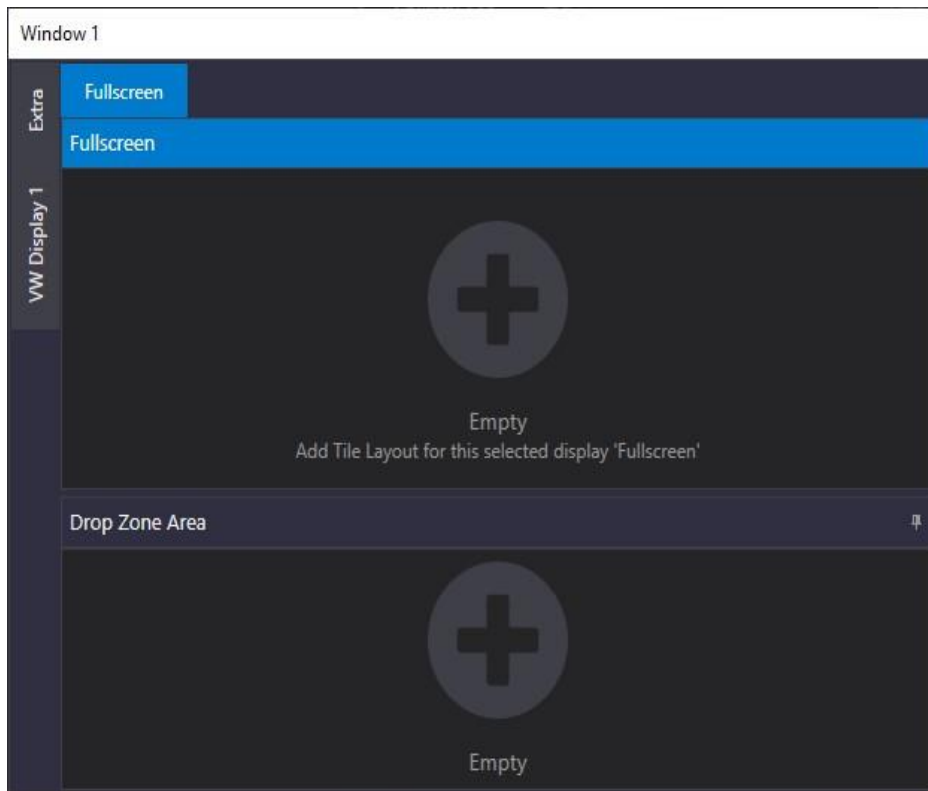
1. Go to **System > Setup Display** window.
2. Click on the display area you want to change the properties for.
3. Click on the **Allow User Docking** property and set it to **True**.
4. Click on the **Allow User Float** and set it to **True**.
5. Save the layout.
6. On the main screen, drag the display area from its position and either dock it in another position on the window or allow it to float.

Notes:

- Only docked display areas can be floated.
- You cannot save your System Explorer layout if the System Explorer is floated. You must dock the System Explorer and then save your layout.

Docking a Display Area

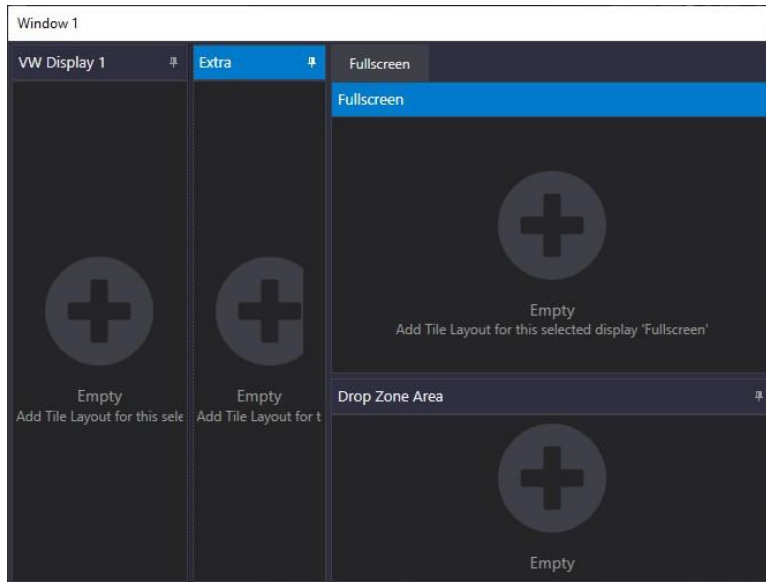
A docked display area occupies a unique dock position within the window. Two or more docked display areas can be tabbed if they are unpinned into the same dock position within the window. As a result of this, you can only see one window at a time. A collection of tabs can be seen at the top of the dock frame. The tab selected/hovered in the collection determines which display area is active and visible.



If the display area is docked, you can move the display area to a new docking position or undock the display area by dragging it out of the window and allowing it to float.

To dock a floating Display area, do the following:

1. Grab the **Title** bar of the floating display area and drag it over the window in which you wish to dock.
2. Choose the dock position and release the mouse.
3. Unpin the display area if you want it to be a part of the tabbed collection.



If the display area has never been docked before, it will be set in a new non-tabbed location in the window. If it had been docked before and was in a tabbed collection, it still assumes a new dock location and will not return to the previously docked position. The user can manually move the display area to a tabbed collection or retrieve it from the layout which has the previously saved setting.

When you are docking a display area by dragging it, you can control its destination position. As you drag the display area out of its docked position it can either be left to float or can be docked in any of the four positions [left, Right, Top, and Bottom] in the window frame. The positions are shown when you have grabbed the display area from its position and holding it.

When you choose the dock position and move the display area to it, a transparent window will appear to show the new positioning of the display area. This outline shows where the display area will be docked if you release the mouse button at that point.

Few points to note when you drag a display area:

1. If you drag a display area over an empty dock, it will be docked in the position and occupies the entire frame. However, if you drag it to a dock that already has a display area, then they are compelled to share the frame and hence will appear side by side.
2. If two or more display areas are docked in the same dock position and are pinned, it appears as a tabbed collection and only the display area selected is visible consuming the entire frame.
3. If you drag a display area to a position outside the window, the display area will remain floated.

4. If the display area is allowed docking and has been denied floating, it is not possible to move the display area to a new location. Hence for the display areas to be moved to a different dock location, Allow Floating property must also be enabled.
5. If you want to re-dock a display area to the previously docked position, you will have to manually set it up or retrieve a saved layout that has display areas docked in the desired locations.

Undocking a Display Area

You can drag a docked display area by grabbing on its title bar and dragging out of its docked position. This action enables you to move the display area to a different dock position or undock it to let it float. Dragging a docked display area to a new position works exactly like dragging a floating window to a new dock position.

Tabbing a Display area

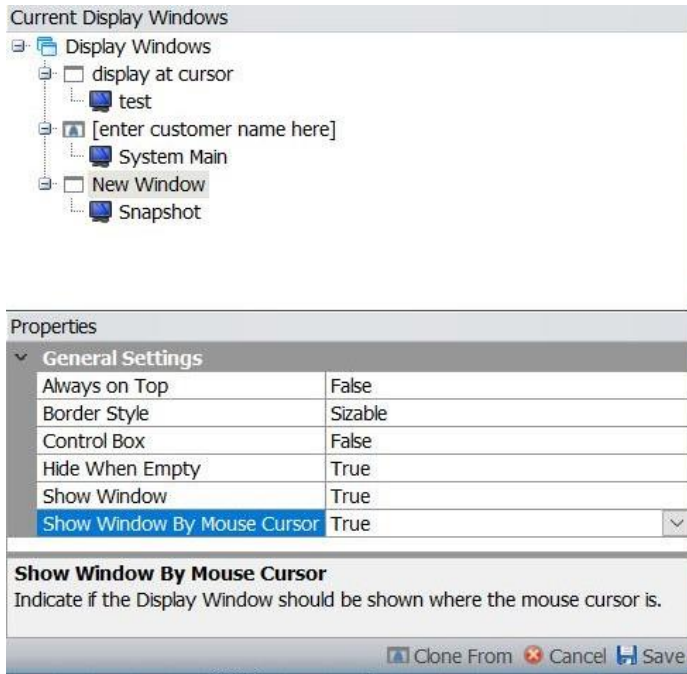
You can create a tabbed collection of all docked and full screen display areas. All full screen display areas are automatically tabbed. Display areas in the same dock location appear side by side unless they are pinned. Only the ones that are pinned will appear as tabbed and the ones that aren't will appear in the frame all the time until the pinned display area is selected. At this point of time the unpinned display area goes in the background and will remain there until clicked outside of the current dock position.

Floating Display areas cannot be tabbed. It requires to be docked to a position where there are at least one display area and pinned to the location.

Display the Window at the Mouse Cursor Location

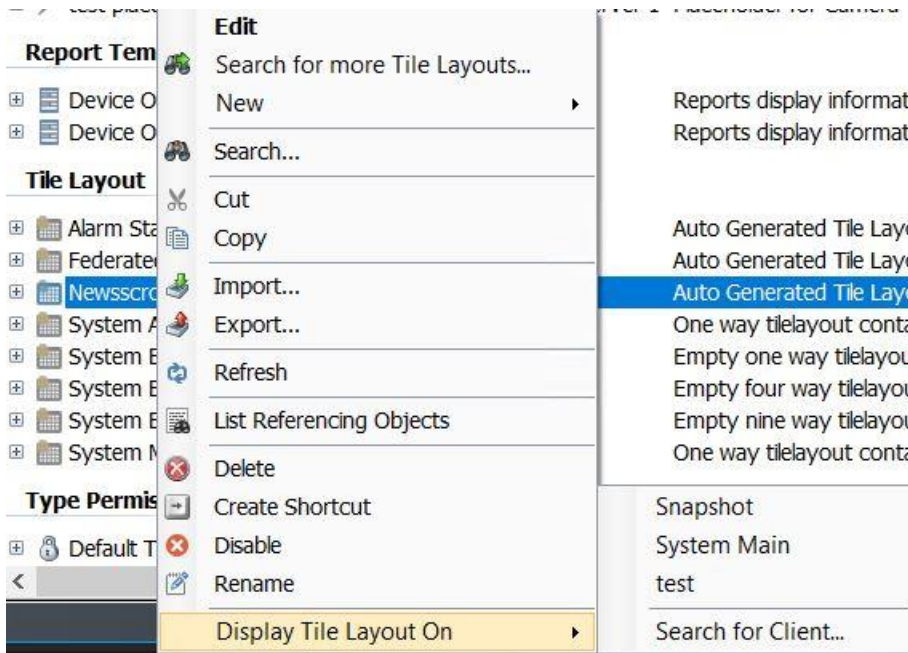
This feature enhances the user experience by providing the user the ability to display a window at a desired location. This helps to expand the definition to include the user's context in the application. This feature necessitates better accessibility and flexibility to the user.

A property in the Setup Display dialog allows you to specify if the display window needs to be shown at the cursor location or not.



For example, if the user has configured a GUI to be displayed in a tile layout, then:

1. Go to **System Configuration > System Objects** and select the **Tilelayout** object to display.
2. Right click on the **Tilelayout** object and select the display area.
3. The display window is shown at the mouse pointer location.



4. Double click on a Camera on the map to start the video feed.

The user can extend this functionality by drafting a response plan to start a video feed from a camera. You can configure the display window to popup and start the video feed at the location where the mouse cursor is located by double clicking on the asset. The video feed on the window will continue until another camera is selected to display or the tilelayout is closed.

Configuring System Explorer to Display Different Objects

You can configure what type of object types should be shown on the System Explorer by configuring the Types to show property.

To configure System Explorer to display different objects:

1. From **System Objects**, double-click the **System Explorer** GUI to open it.
2. With **Locations** selected, click **Types to Show** in the **Properties** pane. The **Object Types** dialog appears.
3. From the **Object Types** dialog, click select **None**. Any existing object type that was displayed previously will disappear from the System Explorer.
4. Select the required objects by selecting the check box against the object type. For example, devices, placeholders for displaying camera objects.
5. Save and close the **System Explorer** GUI.

Configuring Object Types in System Explorer GUI

The Add Types to show method can be used within a response plan for the System Explorer GUI as an alternative to configuring the Types to Show property. For instance, you can limit viewing of specific devices types by specific users by scripting it in a response plan via the System GUI control.

Following is an example of how to configure the Add Types to Show method via in a response plan scripting to view specific device types in System Explorer.

To use the Add Types to Show method:

1. From **System Objects**, double-click the **System Explorer** GUI to open it.
2. With **Locations** selected, click **Types to Show** in the **Properties** pane. The **Object Types** dialog appears.
3. From the **Object Types** dialog, click select **None**. Any existing object type that was displayed previously will disappear from the **System Explorer**.
4. From the **Events** drop-down, select the **System Explorer Load** event. The event page is displayed.
5. Edit the System Explorer Load response plan to include the following information:
 - a. Drag and drop a **User in Group** shape on to the VRP Editor.
 - b. Drag a **Script** shape on to the true route in the editor.

- c. Edit the **Script** shape to include the following script:

```
My.SystemVariables.[System Explorer].guiSystemExplorer1.AddTypesToShow("CNL.IPSecurityCenter.Driver.Training Driver.ITrainingCamera")
```

```
My.SystemVariables.[System Explorer].guiSystemExplorer1.[Refresh Tree]()
```

Where, `Driver.TrainingDriver.ITrainingCamera` is the camera that you want to display.

- d. Drag and drop an **End** route to complete the response plan.
6. Save the **System Explorer Load** response plan.
 7. Viewing the System Explorer should now display the device type based on the user group.

Permissions & Security

A granular security permission structure sits at the core of Control Center, which is primarily defined in the following areas:

- Security Policies, which define behavior, for instance, the right to access the **System Configuration** interface.
- Object Type Permissions, which define the ability for users to read and write specific types of objects, Folder.
- Object permissions which defines read, write, and execute access to folders and objects.

Adding Users and Groups

Before a user can start using Control Center, at least one User Group must exist, and the user must have an account that is a member of the user group. By default, Users with the administrator role can create and remove a list of users and groups providing administrator users with greater control over managing security permissions for those users.

Typically, you create a user account and make that account a member of an existing user group.

To configure users and groups:

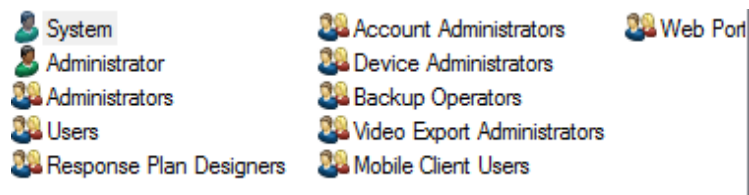
1. Create a new user group called **Supervisors**.
2. Configure the **Supervisors** group to have full control.
3. Create a new user account and make that user account a member of the group **Supervisor**.

To remove users and groups, simply right-click on the user or user group and click **Delete**.

You can create users and groups via the Admin Interface as well.

Default User Groups in Security Settings

By default, the following user groups are available in **Security Settings** on a fresh installation of Control Center.



Security Policies for Client and User

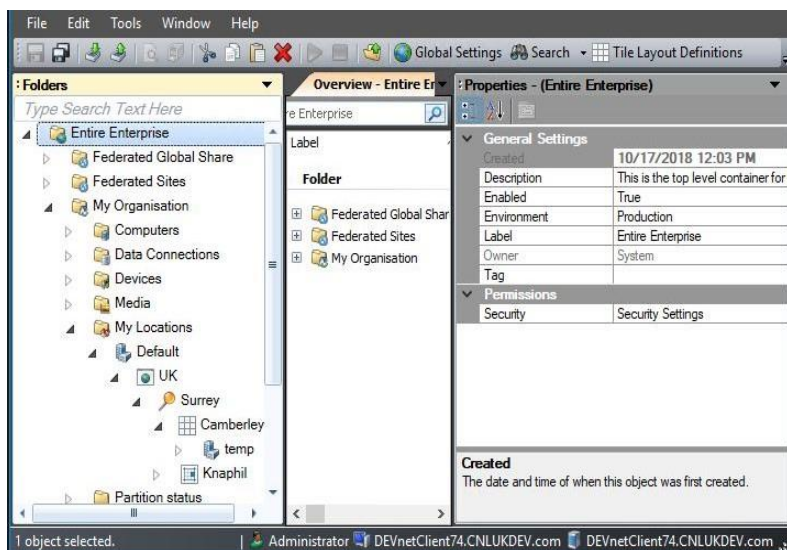
Use security policies to define password policies and login information for Control Center clients and users. For example, you can choose to restrict or allow multiple logons, or enable and disable complex passwords, define the minimum password length and so on.

There are two types of security policies: Client and User. See [User Policies](#) for more information about configuring user security policies.

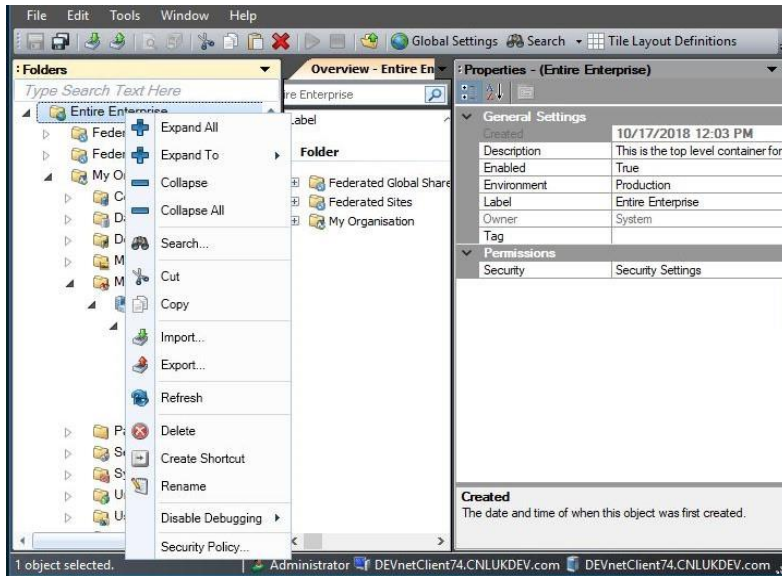
Configuring Client Security Policies

To configure security policy for the client:

1. Click **System > Configuration**. The **System Configuration** dialog opens.



2. Right-click on the **Entire Enterprise** folder and select **Security Policy**. **Security Policy** window opens up.



3. Select **Client Policies**. The available security policies are displayed on the right.
4. Double-click **Allow multiple logons** to define whether multiple clients can connect to a single server. The **Allow Multiple logons Properties** dialog opens.

To enable multiple logons:

1. Select **Define policy**.
2. Set the value of **Allow multiple logons** to **True**, and then click **OK**.

Ensure that there are sufficient Control Room Client licenses available in the License Manager to enable this feature.

To prevent multiple logons:

1. Select **Define policy**.
2. Set the value of **Allow multiple logons** to **False**, and then click **OK**.
3. Click **Save**.

User Policies

Each of the user policies have a unique purpose in Control Center:

- Video-specific
 - PTZ Lease
 - Video Export Administrator
 - Video Export Deferrers
 - Video Export User
 - VideoWall Leasing Priority
- Permissions related

- Access to System Configuration
- Access to Admin Interface
- Access to Response Plan Designer
- Access to Setup Display Window
- Can manage users and groups
- Config Authorization x2
- Allow Interactive log on to Mobile Client
- Allow Interactive log on to Web Portal
- Allow Interactive log on to Windows Client
- Access to the Map Note editor
- Add Clients
- Security related
 - Password Settings
 - Account Expiration Notification
 - Mobile Client Credentials
- Auditing-specific
 - Message for users Logging on
 - Auto Log off
 - Can exit Control Room Client
 - Can Lock Application
 - Can logoff from application
 - Can manage Auditing and Activation Logs.
- Alarms-specific
 - Allow Alarm Handling Takeover
 - Allow Bulk Resolution of Alarms

Defining Password Policies

To define the password policy for the Control Center user:

1. In the **System Configuration** window, right-click on the **Entire Control Center Enterprise** folder and select **Security Policy**.
2. Click **User Policies**. The available policies are displayed on the right.

Policy	Security Setting
Access to Admin Interface	Administrator, Administrators
Access to Response Plan Designer	Administrator, Administrators, Response Plan Designers
Access to Setup Display window	Administrator, Administrators
Access to System Configuration	Administrator, Administrators
Access to the Map Note Editor	Administrator, Administrators, Users
Account Expiration Notification	Disabled
Add Clients	Administrator, Administrators, Account Administrators
Allow Alarm Handling Takeover	No Security Principals Defined
Allow Bulk Resolution of Alarms	Administrator, Administrators
Allow interactive log on to Mobile Client	Administrator, Administrators, Mobile Client Users
Allow interactive log on to Web Portal	Administrator, Administrators, Web Portal Users
Allow interactive log on to Windows Cli...	Administrator, Administrators, Users
Auto log off	Disabled
Can exit Control Room Client	Administrator, Administrators, Users
Can Lock Application	Administrator, Administrators, Users
Can Log off from Application	Administrator, Administrators, Users
Can manage Auditing and Activation Logs	Administrator, Administrators
Can manage users and groups	Administrator, Administrators, Account Administrators
Configuration Authorisation Required	Users
Configuration Authorisers	Administrator, Administrators
Message for users logging on	Disabled
Mobile Client Credentials	Enabled
Password Settings	Disabled
PTZ Lease	Administrator, Administrators, Device Administrators
Video Export Administrator	Administrator, Administrators, Video Export Administrators
Video Export Deferrers	Administrator, Administrators, Video Export Administrators
Video Export User	Administrator, Administrators, Video Export Administrators
VideoWall Leasing Priority	Administrator, Administrators, Device Administrators

3. Double-click **Password Settings**. The **Password Settings Properties** dialog opens.
4. Select **Define policy** and specify the following settings:
 - a. Enable **Complexity** check to **True**.
 - b. Enable **Password Policy** to **True**.
 - c. A value for **Maximum Password Age**.
 - d. A value for **Minimum Password Age**.
 - e. A value greater than **1** for the **Minimum Password Length**.
 - f. A value greater than **2** for previous passwords to be stored in the logs.
5. Click **OK**.

Changing Password

To change the password:

1. Go to the **System Configuration > My Organization > Users** folder.
2. Right-click **Administrators** and select **Reset Password**.
3. In the **Reset Password** dialog box, enter the new password.
4. Select **User must change password at next logon**, if you want the password to be changed at the next logon.
5. Click **OK**.

Lock Application and Logging off Security Policies

Two new security policies have been introduced to prevent unauthorized users from locking and logging off the Control Center application. The following new security policies enable you to:



- **Can Lock Application** – Determine which users and groups can lock the workstation using the normal process.
- **Can Log off from Application** – Determine which users and groups can log from the application.

If you attempt to lock or log off from Control Center without the security policies enabled, then you are prompted to confirm the action by entering a username and password of a user with appropriate permissions.

For backwards compatibility, the security policies are enabled by default when you add new User groups to ensure all existing customers and users can continue to work in the same ways prior to the upgrade.

Allow Interactive Log on Settings

Use the **Allow Interactive log** on settings to manage permissions for users as part of the login process. For example, you can define which users can log in to the Windows Client, Mobile Client, and Web Portal.

	Allow interactive log on to Mobile Client	Administrator, Administrators, Mobile Client Users
	Allow interactive log on to Web Portal	Administrator, Administrators, Web Portal Users
	Allow interactive log on to Windows Client	Administrator, Administrators, Users

- **Allow interactive log on to Mobile** – Add log on permissions for mobile users.
- **Allow interactive log on to Web Portal** – Add log on permissions for Web Portal users.
- **Allow interactive log on to Windows Client** – Add log on permissions for Windows Client users.

If you have upgraded Control Center and wish to use the Mobile Client and Web Portal, ensure that you have manually added the Mobile and Web Portal user groups to the folder structure using the **Security settings option**.

Control Center Security Settings

Security settings determine which users have Read, Write, or Execute permissions at the folder level. Security settings can be configured for an object type at a folder level or locations level.

Objects do not normally have permissions of their own, they inherit it from their parent folder. The following permissions are available in the system:

- Read – View permissions to objects

- Write – Edit and update permissions
- Execute – Run executable methods

Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
General Settings(200)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Permissions(202)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Properties(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
General Settings(200)	<input type="checkbox"/>	<input type="checkbox"/>
Permissions(202)	<input type="checkbox"/>	<input type="checkbox"/>
Properties(2)	<input type="checkbox"/>	<input type="checkbox"/>
Execute	<input type="checkbox"/>	<input type="checkbox"/>
General Settings(200)	<input type="checkbox"/>	<input type="checkbox"/>
Permissions(202)	<input type="checkbox"/>	<input type="checkbox"/>
Properties(2)	<input type="checkbox"/>	<input type="checkbox"/>

By default, permissions are allocated in the following order:

- All users except the Admin Users are allocated with read permissions at the folder and location level.
- All Administrator users are allocated with Read and Write permissions.
- All Administrators users are allocated with all permissions.

Permissions on exported objects shall not be retained.

Inherited Settings

You can apply inherited permissions across folders and locations if required by simply selecting the **Allow inheritable permissions from parent** to propagate to this object option. For example, if you had specific permissions applied to a user or user group, and then you select the inheritable permissions check box, the permissions will change and therefore the permissions at the top parent folder hierarchy will apply.

To reset permissions for child objects, select the Reset permissions on all child objects and set propagation of permissions option. In other words, if you want to remove inherited permissions from the parent folders to child items (doors, devices), then select the reset permissions option.

Object Type Permissions

Object Types' permissions flow in the following order depending on how they are set:

Read	Write	Execute	Permissions
Allow	Allow	Allow	View, edit and run an object type.
Allow	Allow	Deny	View and edit an object type but cannot run any of the methods on the object type.

Allow	Deny	Deny	View the object type, but cannot edit, or run any of the methods on the Alert State.
Allow	Deny	Allow	Can view and run methods on an object type.
Deny	Deny	Deny	Cannot see the object type in System Configuration and hence cannot run methods or edit.
Deny	Deny	Deny	Cannot see the object type that is raised against an object when plotted on a map. A user can see the selected object type in System Explorer and Map whose read permissions are denied.
Deny	Allow	Allow	Cannot see the object type and hence cannot run methods or perform the edit operation.

Allowing\Denying Users With Read-Access Permissions to View a Folder

In this example, the folder location has been used to describe permissions. At least two clients are configured to the same server (one as an administrator and the other as a user).

To deny read-access permissions to a location:

1. On the first client, create a new user account.
2. On the second client, log in to Control Center using the new user account.
3. Create a location called **UK** and create a scene.
4. On the first client, in **System Configuration** with the location selected, click **Properties > Security Settings**. Then, clear the **Allow inheritable permissions** from parent to propagate to this object selection.
5. From the **Security Settings** dialog, click **Add**. The **Search Objects** dialog appears.
6. Click **Find Now**, then select the new user and click **OK**.
7. Click **Deny** in the **Read** section.
8. Verify the first client to verify that the location **UK** has now disappeared.

Any child folder under UK should also have now disappeared. For example, the scene UK will not be available to view. You will see the following error message:



Error you don't have read permissions to view the scene

For example, if a location had a door or device, then they will be hidden as well. In the above example, the R2 user will disappear from the list of users & groups.

Notes:

- Make sure to restart the client to see the changes take effect.
- To provide read-access permissions, simply select the user group and click **Allow** under the **Read Type** category

Setting Permission to View/Hide Device Events

The permissions to view/hide the Alarm and Event history from the device context menu on the map can be set in the Enterprise Properties window as explained below:

1. Go to **System Configuration**.
2. Select **Entire Enterprise** from the folders in the left pane.
3. Select **Security** from the **Properties** window on the right. A dropdown window displays the list of users and related permissions for the selected user.
4. Uncheck the **Allow inheritable permissions from parent to propagate to this object** to set permissions for a particular device or location. In this case, the permissions will be localized and does not inherit permissions from the parent.

If you do wish to keep the parent permissions then you need to leave it selected.

5. Scroll down to **Device Events** options to set the **Allow/Deny** permissions for the user.
6. Click **OK**.

Properties - (Entire Enterprise)

General Settings

Created	10/17/2018 12:03 PM
Description	This is the top level container for
Enabled	True
Environment	Production
Label	Entire Enterprise
Owner	System
Tag	

Permissions

Security Settings

System, Administrator, Administrators, Users, Response Plan Designers, Account Administrators, Device Administrators, Backup Operators, Video Export Administrators, Mobile Client Users, Web Portals

Add... Remove

Permissions for System

Type Category	Allow	Deny
Device Analytics(710)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Configuration(721)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Connection Details(702)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Events(708)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Logoff as Administrator and login as the user whose permission was set in the previous step. If the permission was denied, the user will not be able to see the **View Recent Alarms/Events** option on the right click menu on the map.



Setting Active Directory Group Permissions

To set Active Directory group with read-only permissions

1. Create a new group independently or by using the wizard.
2. Create a user and add the user to the Admin group.
3. Select the created group and verify that the user only has read permissions to the group.
4. Log in as the user and view the property grid for the user. Verify if the active directory group property can still be selected.

Frequently Asked Questions

Can permissions specific to objects be exported?

Imported objects inherit their permissions from their parent objects. If your import contains folders, the hierarchy structure of child folders will be maintained.

Describe the difference between Denying Read Access permissions and not having read access?

They are one & the same.

What happens to child locations when settings at the parent level changes?

It inherits unless you select the second (reset permissions) check box.

Are Security Policies and Permissions related?

Security policies and permissions are completely separated from each other.

What is a typical usage of permissions in a federated solution?

At the parent site, the permissions are set on the site folders under the Federated Sites folder to determine who can see the site in the location tree and who would receive alarms from that site. You can also control other settings such as permissions to unlock doors and so on. For example, the permissions are set at the high-level folder and then inherited downwards.

Typically, in the federated sites folder, the permissions are set on the site folder to determine what roles can see that site using the Security Settings property.

Type Permissions

The Type Permissions enables greater granularity with permissions for limited administrator users. The primary objective of this feature is to allow administrators to restrict the ability of users to perform certain actions and to interact with certain object types within Control Center for specific user groups across a federated solution or in an isolated installation.

A Type Permissions object will typically have permissions configured for multiple security principals. When deciding whether a user has permission or not, the security permissions, which the user is member of are tested against the security permissions

configured for the Security Principals in the Type Permissions object. If a user is part of multiple groups, then depending on the permissions type set, you can determine what set of permissions take precedence. For any given feature or object type, if any of the security principals in the Type permissions object has deny access set against it, then the user will be denied access. If there is no deny set for the feature or object type, then the user will be granted access if any of the security principals have Allow access.

Permissions can be set to Allowed, Denied, or Unspecified. Denied always takes precedence over Allowed. Unspecified results in Denied, if no other permissions are defined.

Configuring Type Permissions

With a fresh installation, a Default Type Permission object is created which can be renamed and edited by the user. A new object can also be created and the user can choose which object will be used on the system at any given time.

1. Create a new **Type Permission** object under **System Objects** in the **System Configuration** window.
2. Double-click and open the **Type Permissions** object. The **Security Principals** window opens up.

The screenshot shows two windows from the Everbridge Control Center. The top window is titled "Security Principals" and contains a list box with "Administrator" and "Users" selected. To the right of the list are "Add" and "Delete" buttons. The bottom window is titled "Permissions" and shows a table of permissions for various features. The table has columns for "Type", "Can Read", and "Can Write". The "Type" column is set to "Allow" for all features. The "Can Read" column is set to "Not specified" for most features, and "Allow" for "License Manager". The "Can Write" column is set to "Not specified" for all features.

Type	Can Read	Can Write
Feature		
Export	Allow	Not specified
Drivers & Extensions	Allow	Not specified
GIS Layer Manager	Allow	Not specified
Global Settings	Allow	Not specified
Import	Allow	Not specified
License Manager	Allow	Allow

3. Click **Add**. The dialog to select one or more user groups appears. Make a selection and click **OK**.

Select these object types:

Users or Groups Object Types...

From the following locations:

All Folders Locations...

Federated:

Local All Sites Specific Site Sites

Label: Contains Find Now

Description: Contains Stop

Select All Select None OK Cancel

Label:	Type	Folder	Last Modified
Device Administrators	Group	Users	10/17/2018 12:03:1
Mobile Client Users	Group	Users	10/17/2018 12:03:1
Response Plan Designers	Group	Users	10/17/2018 12:03:1
System	User	Users	10/17/2018 12:03:1
Users	Group	Users	10/17/2018 12:03:1
Video Export Administrat	Group	Users	10/17/2018 12:03:1
Web Portal Users	Group	Users	10/17/2018 12:03:1

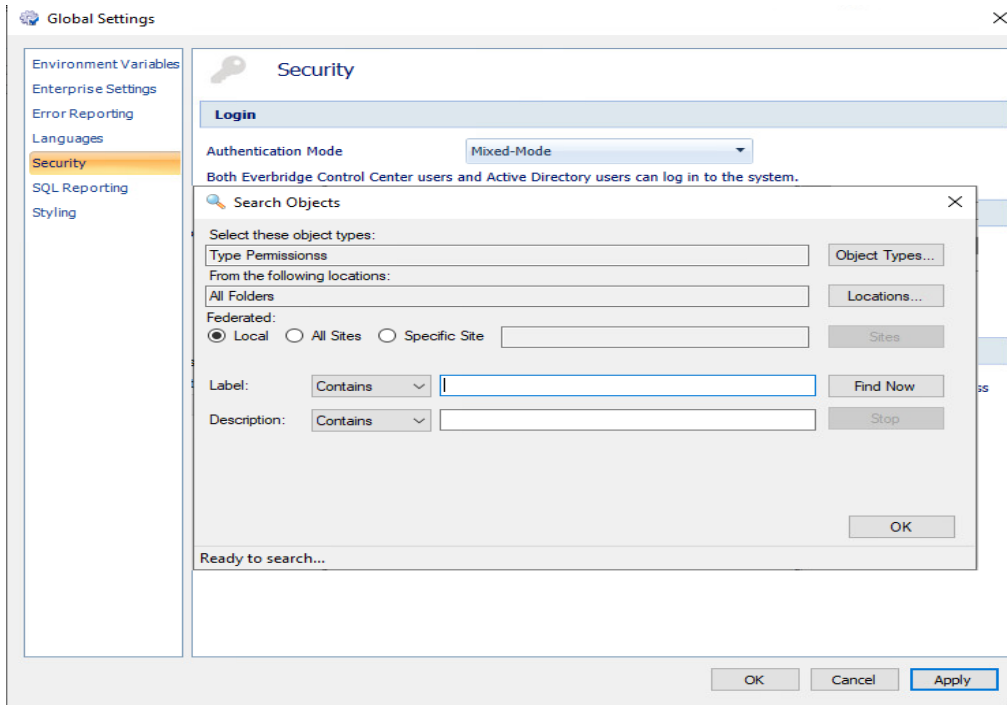
Searched 2 types, 11 objects found , search took 23.3208 milliseconds.

4. Highlight the user you want to set the permissions to and choose the feature and object from the list below to allow or deny read/write access.

Selecting Type Permission Object for the System

Considering that there are more than one Type Permission objects available, you can choose which object to use for the system as shown below:

1. Click on **Global Settings** tab on the main toolbar.
2. Select **Security** from the list on the left pane.
3. Search for the available objects for the system.
4. Select the object whose type permissions you want to use.
5. Click **OK**.



As an administrator you can Allow/Deny Read and Write access to yourself and also set permission for other user groups.

Edit Type Permission

An administrator can grant permissions to various users and user groups based on the environment setup and user requirements. Care must be taken where one user is part of many groups with different Read and Write permissions, as permission denied for a particular user in one group will override Allow permission on other groups, thereby restricting him from doing the necessary actions in that group.

The table below details a scenario explaining this.

User Group	Feature	Read	Write
Usr Grp 1	Global Settings	Not Specified	Not Specified
Usr Grp 2	Global Settings	Allow	Deny
Usr Grp 3	Global Settings	Not Specified	Allow

Assuming the user is part of all 3 groups, he will be granted Read access to Global Settings Feature and denied Write access.

The access to a feature or object for a particular user is affected by different permissions in different groups. For example: If the user has read access to a feature they will be

allowed to see what settings have been configured for that feature. The write access gives them the ability to edit and save changes to the configuration of that feature. If the user has no access to a feature, then they will not be able to view it.

Similarly, for objects, if the user has read access to an object type they will be allowed to see object of that type and the object's property values. If a user has write access to an object type, they will be able to edit and save changes to instances of the object type. If they have no access to an object type, they will not see any instances of that object.

Demonstration of UserType Permission

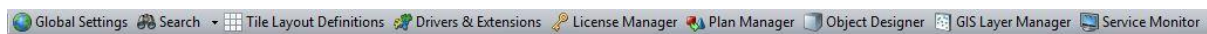
If user A is a member of Administrators and other user groups and is Allowed permission for License Manager feature in Administrator group and denied access in User group, he will have restricted access to License Manager The following screens demonstrates the scenario.

The image shows two screenshots of the Control Center interface. The top-left screenshot shows the 'Administrators' group with 'Users' selected. The top-right screenshot shows the 'Security Principals' section with 'Administrators' and 'Users' listed. The bottom-left screenshot shows the 'Permissions' table for the 'Administrators' group, and the bottom-right screenshot shows the 'Permissions' table for the 'Users' group.

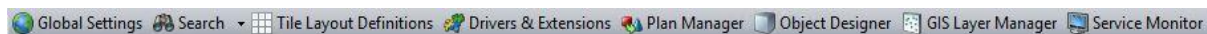
Type	Not specified	Can Read	Not specified
Feature			
Drivers & Extensions	Allow		Allow
Export	Allow		Allow
GIS Layer Manager	Allow		Allow
Global Settings	Allow		Allow
Import	Allow		Allow
License Manager	Deny		Deny

Type	Allow	Can Read	Not specified
Feature			
Drivers & Extensions	Allow		Not specified
Export	Allow		Not specified
GIS Layer Manager	Allow		Not specified
Global Settings	Allow		Not specified
Import	Allow		Not specified
License Manager	Allow		Allow

The toolbar with full Allow access in all groups will typically look as below.



The toolbar with allow access in one group and denied in the other will look as follows.



Active Directory Integration

In addition to using built-in Control Center user/group roles, Control Center provides the ability to connect to a Microsoft Active Directory repository for authentication of users and group members. This allows users to access Control Center using their windows

credentials. Single sign-on is also supported to further reduce the steps required to log into Control Center.

This feature can be used to maintain a Control Center user group on the Windows network to avoid re-entering and maintaining a user base in Control Center itself. Permissions and policies in Control Center can then be applied to active directory users and groups by associating Control Center user groups with active directory user groups.

Control Center does not support making changes to the contents of Active Directory, and other features of Active Directory, such as computer management and policies.

Four modes are available to determine the authentication options for users:

- **Standalone** - Only Control Center users can log into the system.
- **Mixed-Mode** - Both Control Center users and Active Directory users can log into the system.
- **Active Directory Only** - Only Active Directory users can log into the system.
- **Single Sign-On** - Users will be automatically logged into Control Center with the same credentials they use to log into the computer.

Prerequisites for Active Directory Integration

Listed below are the prerequisites for using active directory integration with Control Center:

- The site must be using Active Directory for user authentication.
- The Control Center server and all clients must be installed on computers that are registered with the same Active Directory.
- The Control Center must run as a unique domain user account.
- The server user account must have access to the SQL Server that holds the Pacific database.
- The server user account must have read access to the Active Directory areas that contain all users and groups intended to be used by Control Center.
- The Active Directory user accounts must have **Allow interactive log on security policy** enabled on the computers used for Control Center client terminals.
- Control Center services can run in no-domain mode as well.

Configuring Active Directory

The configuration of Control Center to work with Active Directory is minimal as most of the configuration is transparent to both end-users and engineers. The engineer must specify the authentication mode for the entire solution and then associate Control Center groups with Active Directory groups.

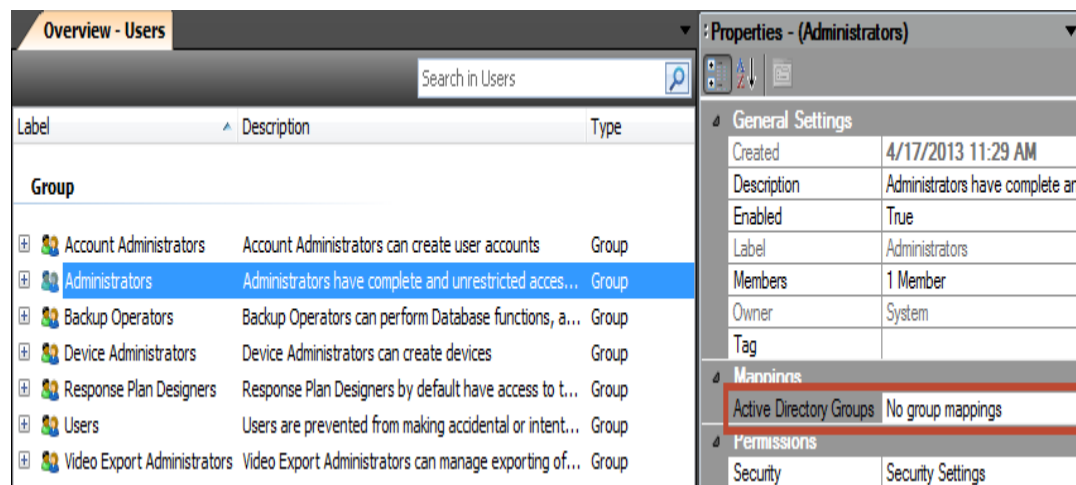
You can create associations between Control Center and Active Directory groups, configure the different authentication modes in Control Center, and log into Control Center using an Active Directory user account.

Associating Control Center Groups With Active Directory Groups

Permissions and policies set against Control Center user groups can be applied to Active Directory groups by associating the two types of objects. Note that no changes will be made to Active Directory. When a user logs in to Control Center, the associations will be checked to determine the level of permissions and policies to be applied to the user.

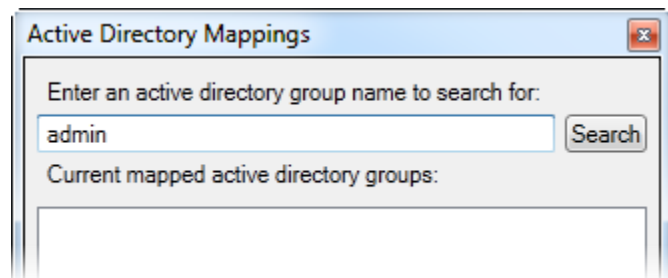
To associate Active Directory Groups to Control Center Groups:

1. Select a group in Control Center and edit the **Active Directory Groups** setting.



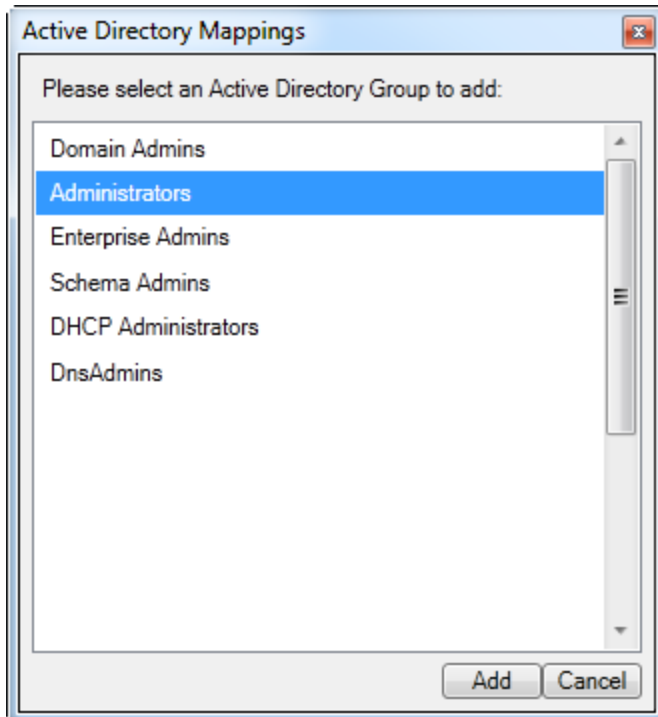
The **Active Directory Mappings** editor appears.

2. Enter all or part of the Active Directory Group to associate and then click **Search**.

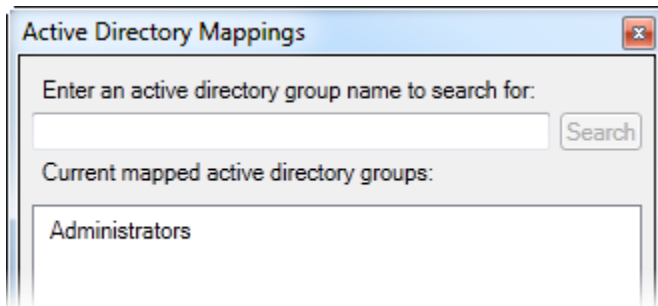


Relevant Active Directory Groups appear, if available.

3. Select a group and then click **Add**.



The selected group will be added to the list of currently mapped Active Directory groups.



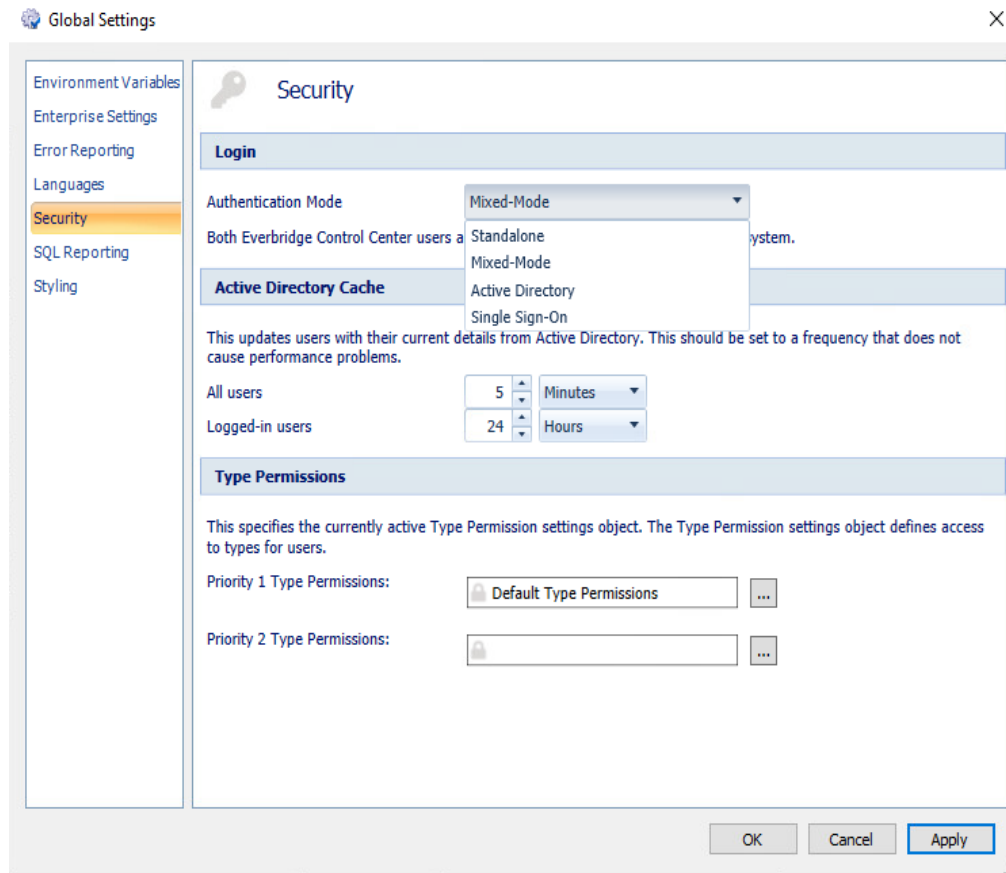
4. Click **Save** to submit the changes and close the dialog.

Any users within Active Directory that are a member of the Administrators group will now be subject to the same permissions and policies based on the Control Center Administrators group.

Changing Authentication Mode

The authentication mode can be specified in the Global Settings dialog within System Configuration.

1. Click **Global Settings** to open the **Global Settings** dialog.
2. Click **Authentication** from the options on the left, and then select the required authentication mode.



Notes:

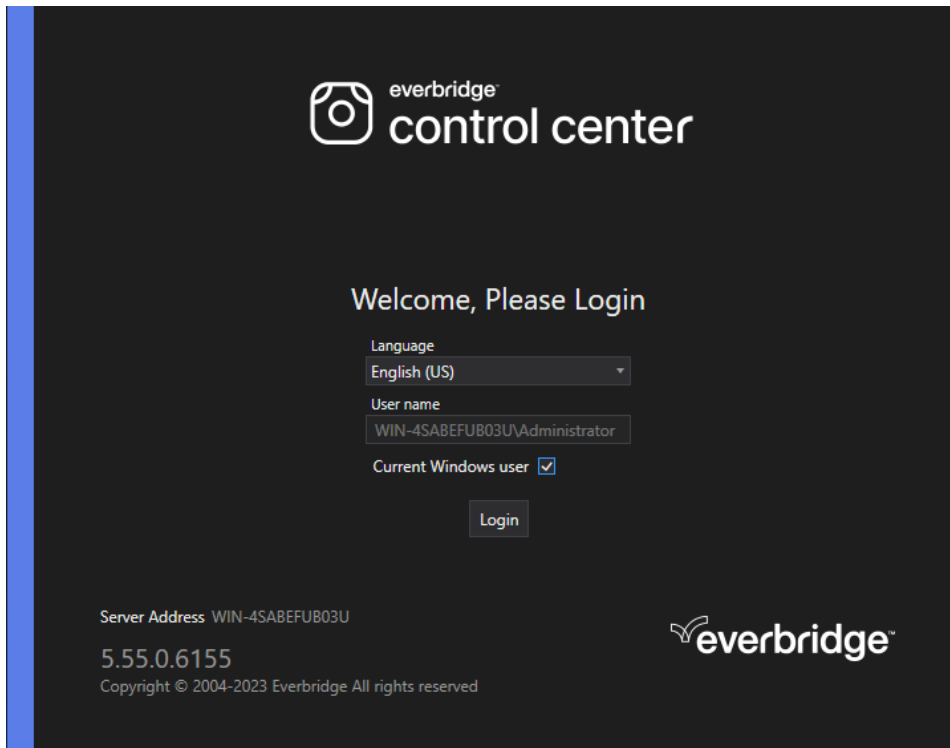
- The Single Sign-On setting only propagates to the clients during login. All clients will therefore need to log into the server following a switch or from Single Sign-On mode to get the updated setting.
- Pressing Shift in Single Sign-on mode makes Control Center behave like Mixed-Mode.

Logging into Control Center Using an Active Directory User

The Control Center **Login** dialog provides the option to specify Control Center user credential, Active Directory Credentials, or simply use the current windows user. The selection made in **Global Settings > AuthenticationMode** determines if the user is permitted to login based on the type of user specified and the mode selected.

If the Active Directory only authentication mode is selected, the **Login** dialog will include an additional option to log in with the Current Windows User. The user can then check this option to log in as the currently logged in user.

An Active Directory user can log into Control Center even when the connection to the Active Directory is lost. However, this is only possible if the AD User has logged into Control Center at least once.



This option will be hidden by default after the first log-in as the user does not need to specify any other setting.

Alternatively, you can also specify the Active Directory credentials different to the currently logged-in user. To enter different credentials:

1. Clear the **Current Windows User** option and then enter the username in the format DOMAIN\USERNAME.
2. Enter the password and then click the **Login** link.

Using Read Only Domain Controller With Control Center

Control Center allows users to authenticate using Windows Domain account credentials. Windows will authenticate the user using a Domain Controller (DC). In a federated solution, with many sites connected to a central location, a common infrastructure issue is that the Domain Controller is deployed centrally, and users cannot authenticate if they are at a site that has been disconnected from the central Domain Controller.

Windows Server 2008 introduced a new type of domain controller, the Read-only Domain Controller (RODC). This provides a domain controller for use at branch offices where a full domain controller cannot be placed. The intent is to allow users in the

branch offices to log-on and perform tasks like file/printer sharing even when there is no network connectivity to hub sites.

Control Center 5.9 introduces support for RODC. If a RODC is available within the user's network and the central DC cannot be reached, Control Center will attempt to use the RODC to authenticate the user and the users AD group memberships when the user logs in.

No specific Control Center configuration is required to support RODC other than the standard configuration for using Active Directory.

WCF Communication Options

WCF represents all direct request/response communication between clients and services with the Control Center product. There are two security deployment options for the WCF communications in Control Center and the required configuration must be set on every server and workstation hosting Control Center software applications. If not configured correctly, clients and services will be unable to communicate with each other and fail to load. The two deployment options are referred to as *Domain Mode*, and *Non-Domain Mode*.

Domain Mode is the recommended and default mode and configures the WCF communication between clients and services to be encrypted using the associated computers domain security credentials. This security protection protects the communication between the server and clients based on the same configuration that the Windows OS system calls use with other Domain services on the network. It also restricts all access to Control Center to Windows machines that are authorized to join the associated Domain.

Temporarily offline Domain Controllers don't prevent clients/services in Domain mode from communicating. However, with the domain controller offline, there can often be follow-on issues with LDAP communication or other Domain services becoming unavailable, preventing Active Directory users being able to login (start new sessions). If a workstation/server is unlucky in its timing, the domain controller becoming unavailable may prevent the client/workstation from renewing its domain lease, and cause issues with it being able to communicate on the domain (not just Control Center but other domain services). Another common issue can be the failure of Domain Controllers to maintain time-syncs with members of the domain. If time-sync issues persist and results in time differences that exceeds 3 minutes between clients and services, then WCF and LDAP connections can start to fail preventing the product from working on those servers/workstations.

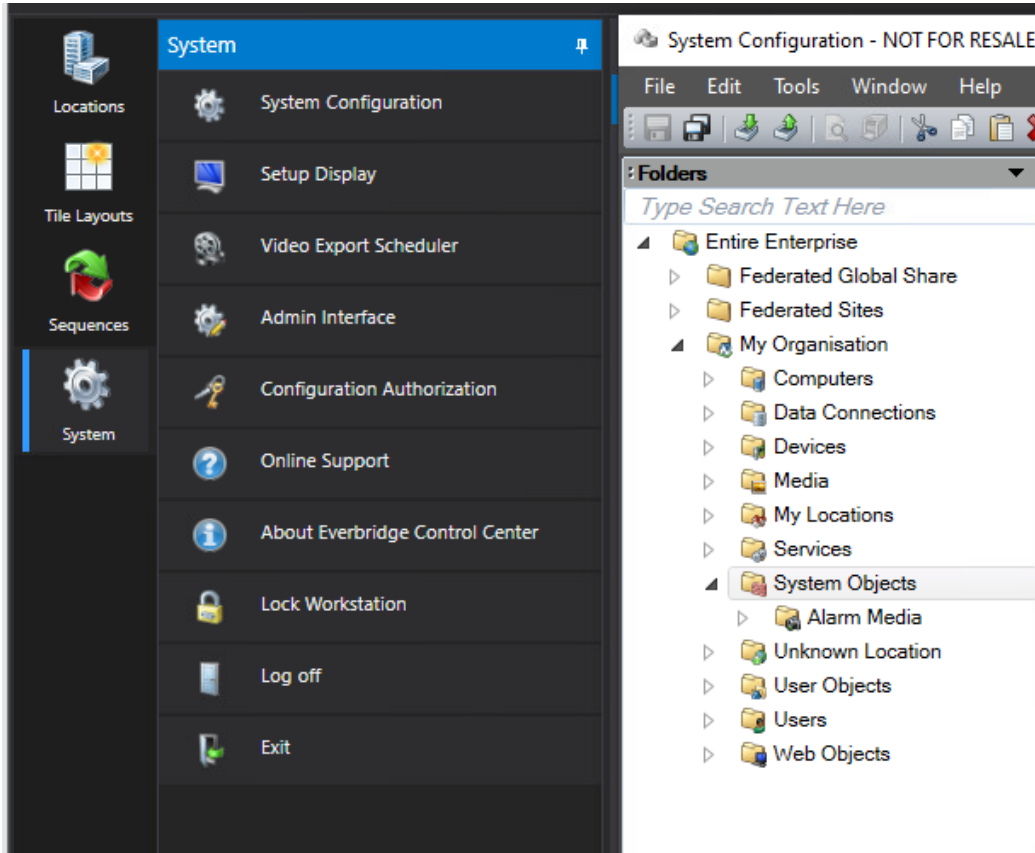
Non-Domain Mode removes transport security from all WCF calls between client and services. This not only removes the encryption of the data transmitted, but also the restrictions on the local/domain for those workstations are a part of. This provides the ability for services to be deployed and shared across multiple networks without complicated Active Directory configuration structures in place, however, comes with the risks. System owners should consider the security of their network infrastructure and susceptibility to man-in-middle attacks on their network traffic (whether direct by a connected active listener, or indirectly by captured logs).

See the Installation Guide for more information about how to configure domain mode .

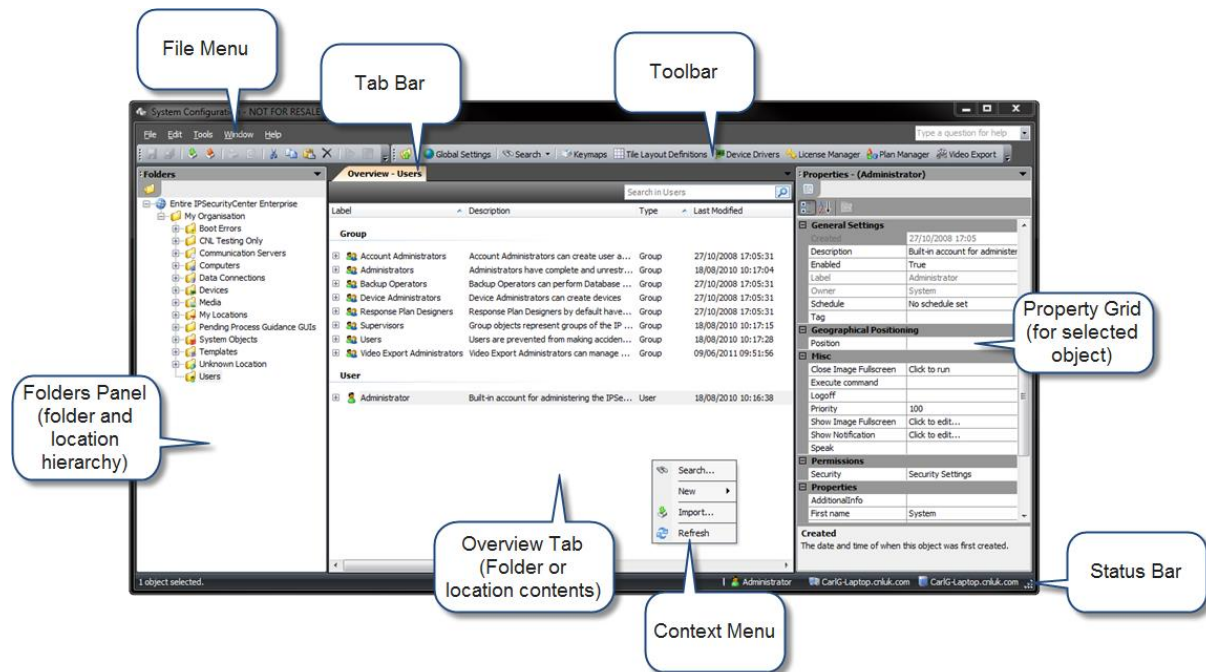
Control Center System Configuration Window

Almost all configuration of Control Center is performed using the System Configuration window, also referred to as System Config.

To open the System Configuration window, click **System > System Configuration** on the main menu.



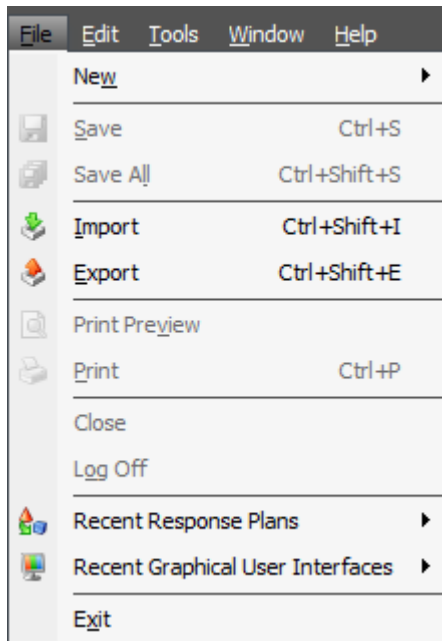
This provides a Windows Explorer style view with a hierarchy of folders on the left, the contents of the folder in the middle, a property grid on the right for the currently selected object and various menus and toolbars.



File Menu

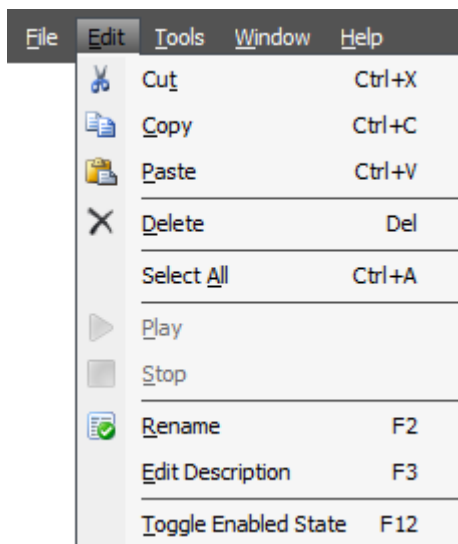
The **File** menu provides a series of useful commands for use against a list of objects in a folder, location, and within the various designers. Most commands also have associated keyboard shortcuts, for example, you can use F2 to edit the label of an object.

Use the **File** menu to access common commands such as save, print, close, and exit. You can also import and export Control Center objects to and from an XML file. In addition, you can view the recent response plans and graphical user interfaces that you viewed recently.



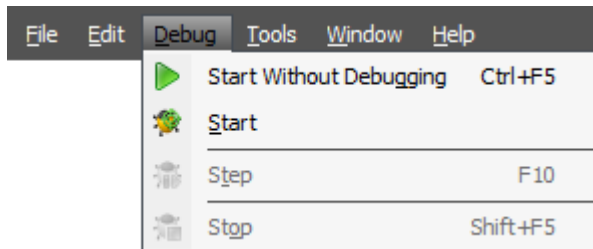
Edit

Use the **Edit** menu to cut, copy, paste, and delete commands which can be used to manipulate Control Center in the folder or location being viewed as well as working with components in the various designers. The play and stop buttons apply to starting and stopping response plans which can be run from System Configuration for testing purposes. You can also rename, and toggle object enabled status using the appropriate commands.



Debug

The **Debug** menu only becomes visible when viewing the **Response Plan** editor. You can debug response plans to determine the logic if any issues arise.



Tools

The **Tools** menu provides the option to refresh the contents of the **Overview** tab and a link to the **User Settings** dialog.



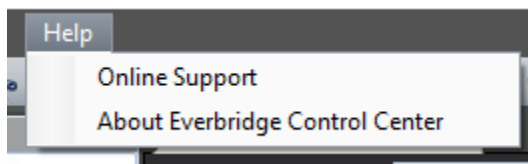
Window

The **Window** menu enables you to close all tabs that are currently open in the System Configuration window except the **Overview** tab. Any unsaved items will prompt you to save before closing.



Help

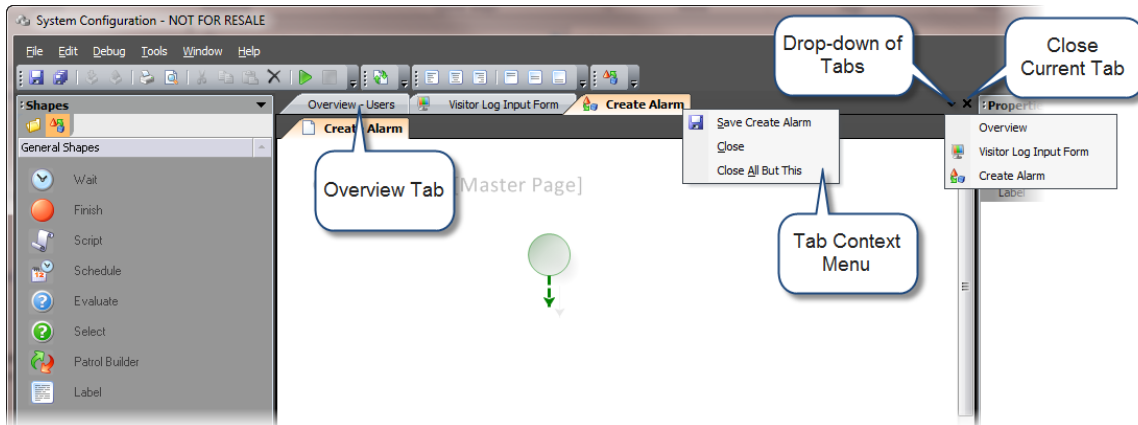
The Help menu provides access to the Control Center website which includes the support information. You can click About Control Center to view the version, copyright, and license information.



Tab bar

The **Tab** bar in the System Configuration window shows which designers are currently open and a context menu on each tab offers save and close options. A small drop-down arrow on the right of the tab bar offers a drop-down of currently open tabs and the

option to close the active tab. The **Overview** tab shows the contents of the currently selected folder and cannot be closed.

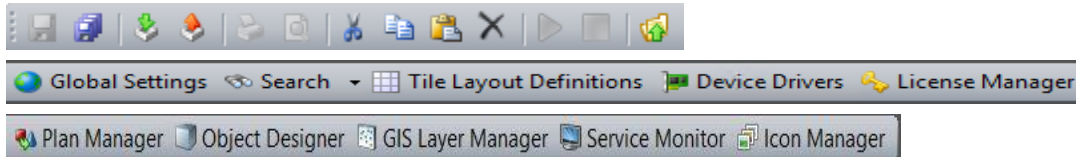


Toolbar

The toolbar in the System Configuration window exposes easy access options to functionality based on the currently selected object(s) or the designer being used.

The toolbar provides common commands such as save, save all, import, export, print and cut/copy/paste. This toolbar also provides options to start and stop response plans which are only available when one or more response plans are selected.

The toolbar also provides access to key components of Control Center. The first button provides the option to navigate to the parent folder.



The following table provides a description of the toolbar items.

Menu Item	Description
Global Settings	Provides core configuration of system features such as GIS, email settings, and so on.
Search	The search button is crucial to finding any object within the solution. This button offers a dropdown of two options to search and return a flat list of results or to search for an object and view the results in a dialog (see Object Designer> Search).

Tile Layout Definitions	Allows for the management of custom tile layout definitions.
Device connectors	Manage all device connectors loaded into the system.
License Manager	View license allocation and usage, apply additional licenses, and replace existing licenses. See Licensing Control Center .
Plan Manager	View and stop and currently running Response Plans.
Object Designer	Manages custom object properties. For more information, see Object Designer .
GIS Layer Manager	Manages GIS layers that are used in scenes.
Service Monitor	Provides a view on the performance of services.
Icon Manager	Provides a standard icon set to choose from and also allows a custom icon set to be created.

Configuring Control Center Icon Set

When using icon sets in Control Center, you can either

- use the icon sets provided in Control Center.
- create your own customized icon set. See [Creating a Customized Icon Set](#).

Control Center is available with more than one icon set. You can configure the icon set you want Control Center to use. By default, when you first install or upgrade, Control Center uses **FontAwesomeLight**. The table below describes the different icon sets.

IconSet	Description
FontAwesomeLight (Default)	Font Awesome provides an icon set with a more modern appearance. You can choose whether to use light or dark.
FontAwesomeDark	
HighDetail	HighDetail provides an icon set with a more detailed appearance.

To configure Control Center to use a different icon set:

1. Go to **System Configuration > Global Settings**.
2. From **Global Settings**, select **Enterprise Settings**.
3. Scroll down to **UI Configuration**.

4. Configure the following:

- **IconSet** - This allows you to configure an icon set for your System Explorer.
- **Secondary IconSet** - This allows you to configure an icon set for System Configuration.

The screenshot shows the 'Enterprise Settings Configuration' dialog box. On the left is a sidebar with navigation options: Environment Variables, Enterprise Settings (selected), Error Reporting, Languages, Security, SQL Reporting, and Styling. The main area is titled 'Enterprise Settings Configuration' and contains a 'Configure Enterprise Settings' section. Below this, there's a dropdown for 'Enterprise Settings' set to 'Local Enterprise Settings'. A table lists various settings:

Name	Value
Server Address	
SMTP Port	0
Use SSL	<input type="checkbox"/>
General	
Support URL	http://support.cnlsoftware.com
Object	
Object Selection Color	#FFFA500
RateLimit	
Rate Limit Default	60
Rate Limit Option	Disabled
Rate Limit Window	60
UI Configuration	
IconSet	FontAwesomeLight
Main Menu GUI	Core Modules Main Menu
Secondary IconSet	FontAwesomeDark
System Explorer GUI	Core Modules System Explorer
Tooltip Template	Default Tooltip Template

At the bottom of the dialog, there are 'OK', 'Cancel', and 'Apply' buttons. A note at the bottom of the settings area reads: 'Highlight color of object when selected in a tile.'

Select the icon set you want from the drop-down list. The icon set does not have to be the same for **IconSet** and **Secondary IconSet**. For example, you can select **FontAwesomeLight** for **IconSet** and **FontAwesomeDark** for **Secondary IconSet**.

Customized Icon Set

Control Center has a default icon set that can be used to represent alarms, system objects, locations and many others to make it more appealing and increasing the user experience and relevance of the object being used. We are now providing the user with

the ability of creating a custom icon set, where the user has the capability to create his own icon set by importing the icons from various resources. Care must be taken to import only those icons sizes and types that are supported by the Control Center. A comprehensive list is as mentioned below:

Icon sizes (in pixel size) supported	File type supported
16x16	Currently we support *.png type only, maximum size 1Mb
24x24	
48x48	
64x64	

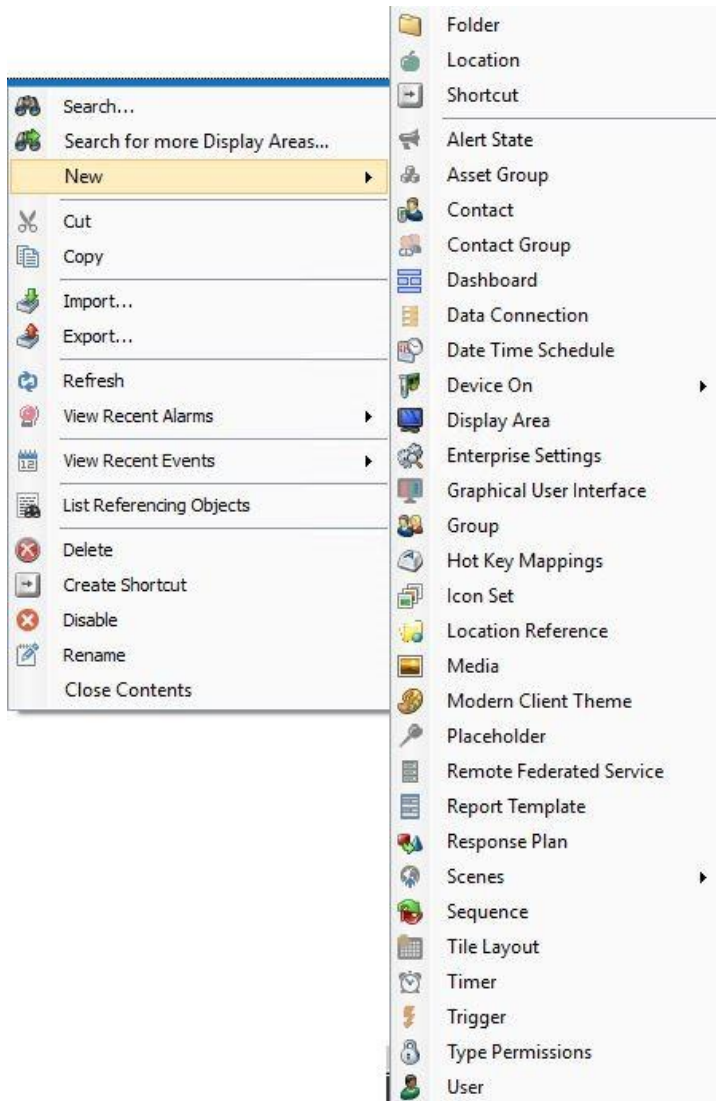
The icons can be used anywhere within the Control Center setup. The user has the choice to select an icon from the default set or the custom set. This makes an excellent addition to the user capability, especially for those who wish to add a little customization to their application. It is perfect to be used on the local client-side instance or to be standardized by the administrator in the NOC and published to all sites to showcase a similar environment with a compelling user experience on all sites in the network. With this in mind, Control Center is now providing an icon set that can be easily crafted to suit unique user needs.

Creating a Custom Icon Set

Creating a custom icon set is an extended functionality provided in the Control Center to the end users. The users can import icons from various online resources or repositories to create their own custom set.

To create an icon set, you need to:

1. Go to **System Configuration > System Objects**.
2. Create an icon set object by right clicking on an empty space in the right window and select **New > Icon Set**. Name it appropriately.
3. Double click on the object to open the **Icon Set** editor window.
4. Add the icons from any reliable resources.
5. Save the icon set.



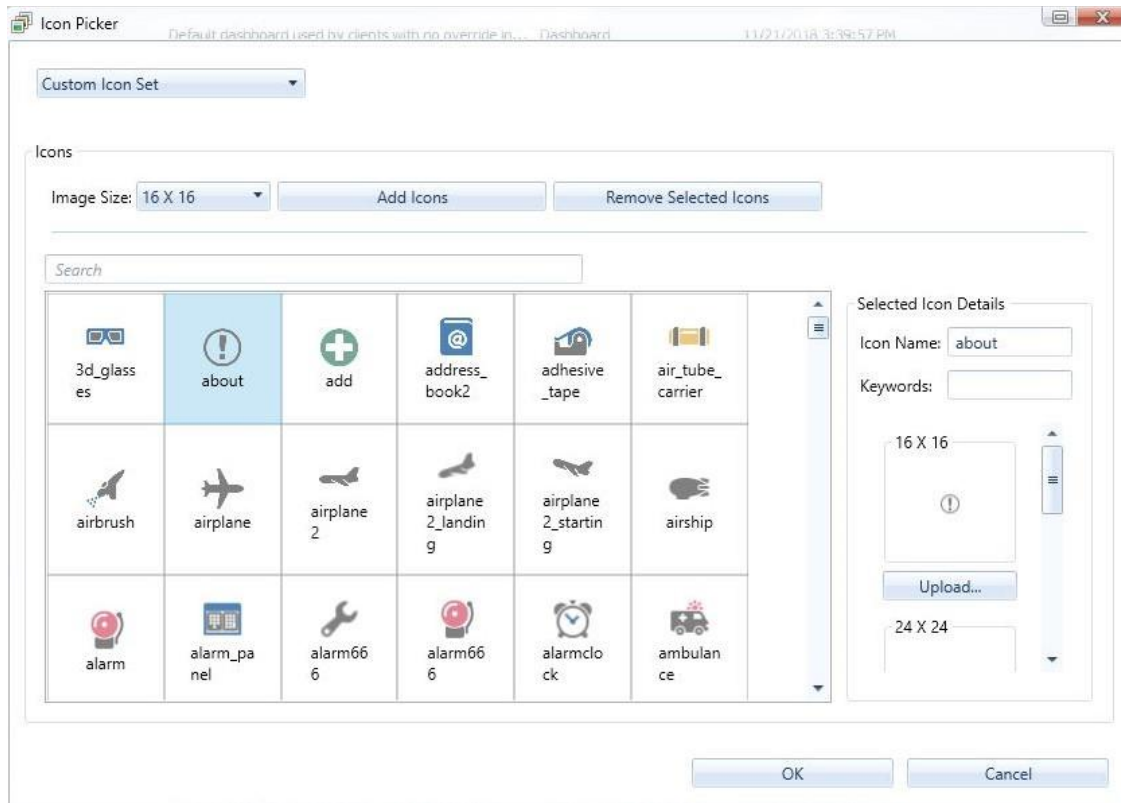
Adding Icons

To add icons:

1. Select the icon size you want to import from the **Image Size** drop down menu and click on the **Add Icons** tab on the top menu.
2. Browse to the location where the icons are stored and select one or more icons to be added.
3. Click **Open** to see the chosen icon/icons added to the custom set.

Icons of a particular size can also be added by clicking on **Upload** button available on the right side of the window. By default, when an icon is selected, all the existing sizes of the icon are displayed on the right. If the icon of a certain size is unavailable it is left blank.

It is possible to add an icon here only if an icon already exists in the set. If the icon of an intended size is present, then it will be added in the box on the right or if unavailable, it will be scaled to fit to the desired size.



Renaming an Icon/Icons

To do this:

1. Select an icon you wish to rename.
2. In the **Selected Icon Details** on the right, click on the **Icon Name** box and give it a desired name.
3. Optionally, you can also specify keyword/keywords separated by a comma based on which it can be searched.
4. Save the icon set.

Deleting an Icon/icons:

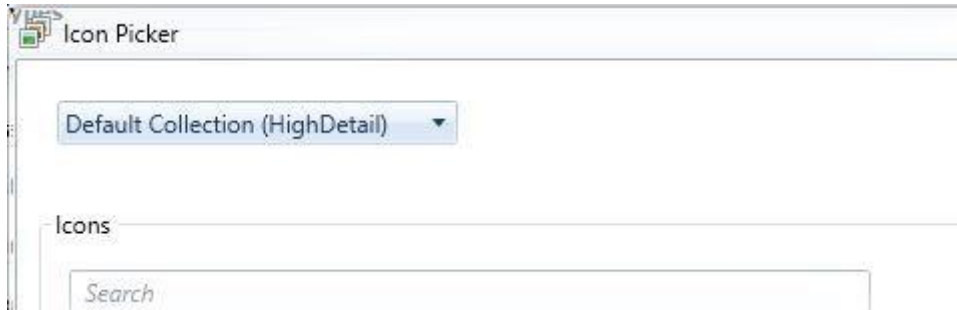
1. Select an icon you wish to remove from the set.
2. Click on **Remove Selected Icons** tab in the top menu.
3. Save the icon set.

If icons in use are deleted from the set, then a X will be displayed in place of it being used. Hence care should be taken before removing it from the list.

Searching for an Icon

Searching for a particular icon is challenging in an elaborate set. So, a search bar is provided to either search by icon name or by keywords, if specified during adding or renaming the icon.

For example, if an alarm icon is named as **ambulance** and the keyword is specified as **emergency**, then searching for emergency would list all icons tagged to the keyword.




Using the Icon Set

The Icon set can essentially be used to represent system objects such as GUI, alarm groups, response plans, alarms, and so on, or can be used to depict a location or a device. Objects can be represented by icons when it is being defined or can be modified later in the property window of the object. A complete set of icons available can be accessed by clicking on the Icon Manager tab in the top menu ribbon of the System Configuration.

Below are a couple of scenarios detailing the use of Icon set.

Scenario 1: Adding icons to new alarm type

An icon can be attached to a new alarm type in the Alarm Type wizard to make it visually appealing and catchy. After entering a name and description to the alarm, you can click on  button to open the Icon picker window. Search and select the desired icon and click **OK**.

Icons can be added to any object in a similar manner.

Scenario 2: Changing the icon of a location

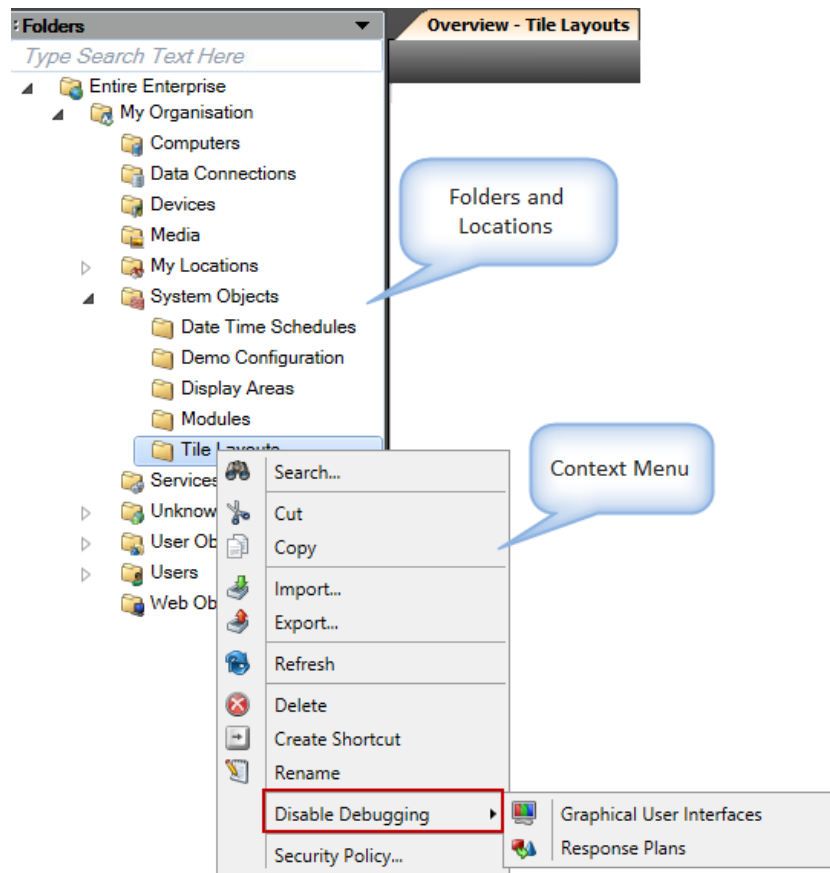
If you wish to change the icon of a location, click on the location you wish to change the location and go to properties window. Select the **Icon** property and click on to open the icon picker. Choose the icon for the location and select **OK** to save.

General Settings	
Created	11/21/2018 3:39 PM
Description	The default location for the system
Enabled	True
Environment	Production
Icon	alarmclock
Label	Default
Owner	System
Tag	

Folders Panel

The folders panel in **System Configuration** shows all the folder and locations in the solution in a tree structure. Selecting a folder will show the contents of that folder in the **Overview** tab. Folders can be expanded and collapsed in this view. Folders can also be rearranged by dragging and dropping a folder onto another to restructure the hierarchy.

This control also provides a context menu with options to search, modify the location, import/export, disable debugging on GUIs and VRPs and setup security policies.



Overview Pane

The **Overview** pane shows all objects in the currently selected folder. Objects are the building blocks of a Control Center solution. An object can be a device, graphical user interface, tile layout, response plan and so on.

Overview - Computers			
Label	Description	Type	Last Modified
Server			
test17server.cnluk.com	Server Computer with the IP hostname of TEST17SE...	Server	6/25/2018 10:50:58 AM
Windows Client			
test17server.cnluk.com	Client Computer with the IP hostname of TEST17SER...	Windows Client	6/29/2018 10:07:38 AM

Selecting Objects

The Objects area displays the following columns for each object.

Property	Description
----------	-------------

Label	The name of the object.
Description	A description of the object or how it is used.
Type	The type of object.
Last Modified	The date on which the object was last changed.
Extra Information	Further information regarding the object, including warnings.

You can also use the following shortcut keys for changing the label and the description of an object:

- Press F2 to change an object's label.
- Press F3 to change an object's description.

Working with Objects

You can make changes to objects by modifying their property settings. The properties are grouped under headings that you can expand and collapse. All objects have the General Settings group of properties. The other properties that are displayed depend on the type of the object.

To modify a property:

1. Click the property you want to change.
2. Select the appropriate value from the drop-down list or click the **Search** button (...) to search for the appropriate value.

You can also double-click the property name to scroll through the values in alphabetical order. This is particularly useful when toggling between a pair of values, such as True and False.

The following properties grouped under **General Settings** are common to all objects.

Property	Description
Description	The description of the object as displayed in the Objects area.
Enabled	Enable or disable the object by setting to True or False.
Hidden	Set the Hidden attribute for the object to True or False.
Label	The label or name of the object as displayed in the Objects area.


Schedule	The Date/Time schedule for the object. Clicking the button opens the Search Objects dialog with the available Date/Time schedules.
Tag	The Tag (Text Property) of the object.
Security	The security and permission settings for the object.

Complex objects have a designer associated with them that enable you to specify the object fully. For example, GUI objects and response plans each have a designer associated with them.


You can access the designer for an object in one of the following ways:








- Double-click the object, or,
- Right-click the object and select **Edit** from the context menu.

Server

 test17server.cnluk.com Server Computer with the IP hostname of TEST17SERVER.CNLUK.COM

Windows Client

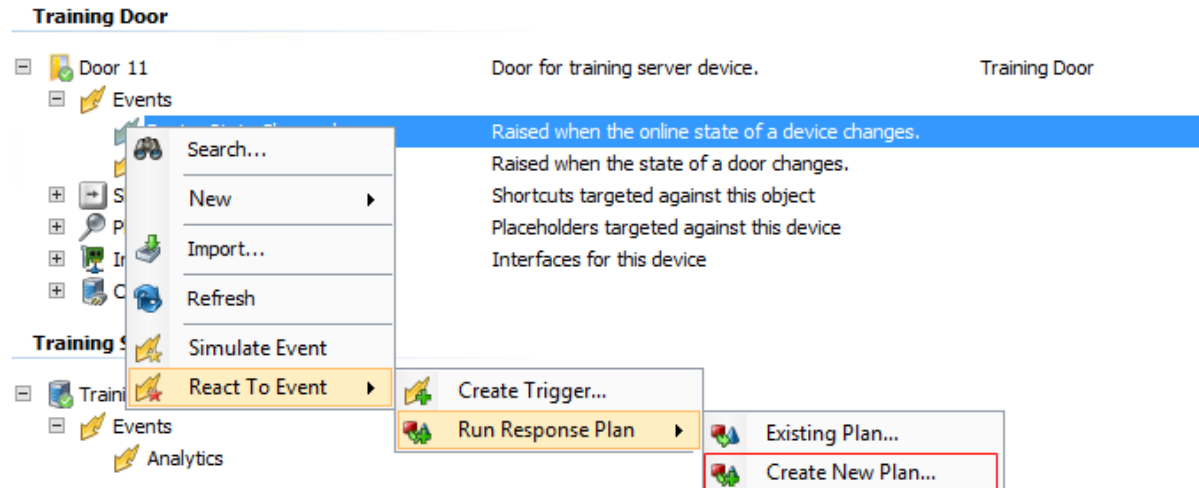
 test17server.cnluk.com Client Computer with the IP hostname of TEST17SERVER.CNLUK.COM

-  Events
 -  Client log off Event raised when this client logs off of from the system
 -  Client log on Event raised when this client logs onto the system
 -  Client Notification Clicked Event raised when a user logged into this client clicks on a notification.
 -  Joystick Button Down Fired when a joystick button is pressed down on a selected device.
 -  Joystick Button Up Fired when a joystick button is released on a selected device.
-  Shortcuts Shortcuts targeted against this object

Each object within the **Overview** tab can also be expanded to view any associated events and shortcuts to that object. To expand an object, click on the small '+' symbol to the left of the icon. Expanding the Event sub item will then show all associated events for the object.

Reacting to Events

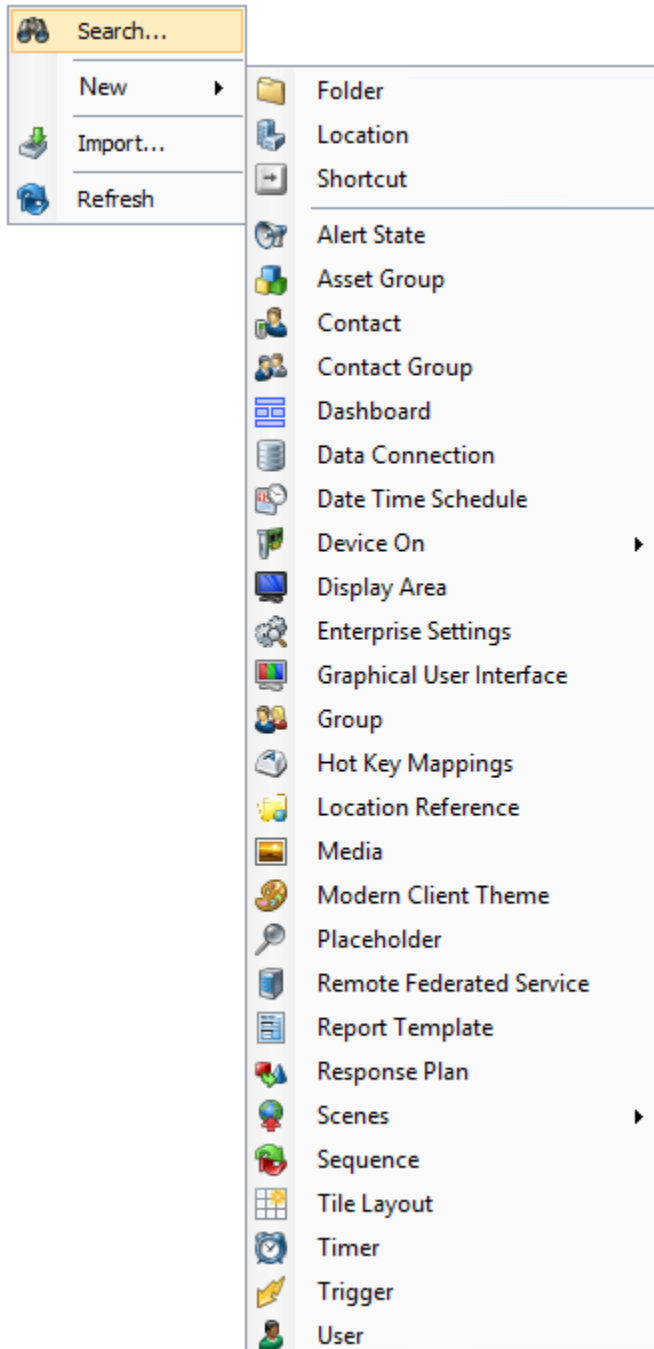
Viewing the available events within the **Overview** tab also provides context menu items for creating objects to react to any event. The screenshot below shows how to react to the **Client Log On** event.



About Context Menu

The context menu in Control Center provides the ability to search, add new objects, import objects from an XML file or refresh the contents of the **Overview** tab.

Using the **New** menu item, you can add any object to the Control Center solution except servers and Windows clients which are added automatically. Note that when selecting **New > Client Device On** or **New > Device On**, a Windows client or server must be selected because both client devices and regular devices require a host.



Property Grid

Selecting an object in the **Overview** tab displays its properties in the **Properties Grid** on the right of the System Configuration screen. The properties include the object definition, how it is set up, what it looks like, and what functions it can perform. The properties available depend on the object, except for the General Settings which are

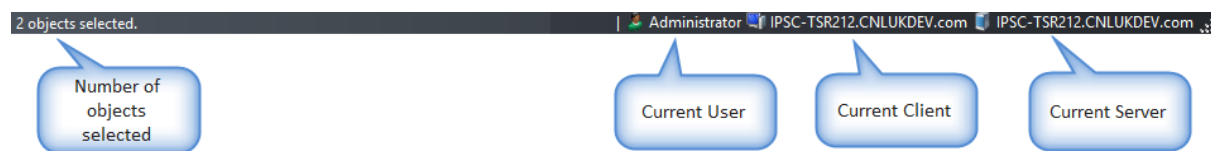
common to all objects. Modify the property settings to see the changes for the selected object.

If you select more than one object of the same type, then any changes you make to the properties affect all the selected objects. If you select more than one object of different types, there are no properties in common and no properties are displayed.

For some objects types, additional fields can be added.

Status Bar

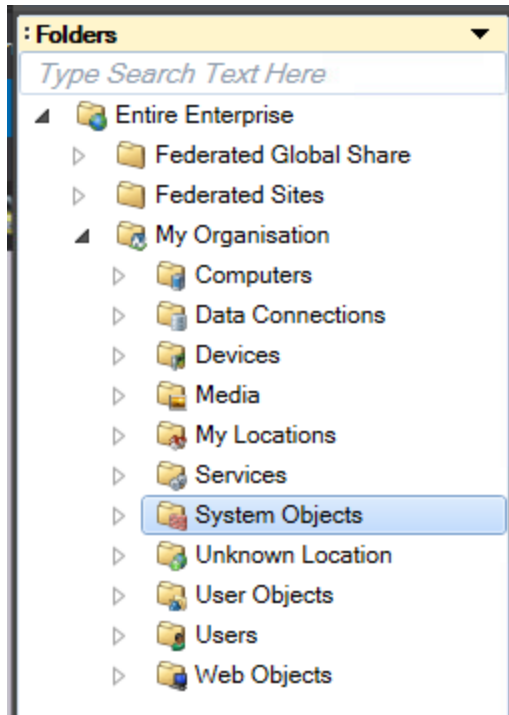
The status bar shows the number of selected objects in the **Overview** tab and shows the current user, client and server.



Control Center Objects

The Control Center installer creates a new database if an existing Pacific database is not found. When the server first starts up, it creates several default objects in case they do not already exist. Some of these are fundamental to being able to use the solution, such as a default user account, and others are more useful in accelerating the building of a solution, such as a series of default folders. The default objects which are created by default are as follows.

The following folder structure is created when the server starts for the first time.



Some folders then include default objects as discussed below. Other folders are blank and should be used for containing newly created objects. The use of folders is essential to keeping an organized solution.

Objects created automatically by the server cannot be deleted and can often be edited on a limited basis.

Understanding Control Center Objects

Control Center is built in a very similar approach to OOP (Object Oriented Programming) where different objects with different properties and attributes are used to build up a solution. All the objects can be created and edited in the System Configuration window. Certain objects include an Editor, such as Report Designer, and are also accessible via the System Configuration window.

A full list of Control Center objects is as follows.

Object Name	Description
Action	Allows you to set the value of one or more properties and/or executing one or more functions on one or more objects of the same type.
Alarm Type	A single system-generated alarm type object provides a central point within the solution to configure All the different types of alarms in the system. Using the Alarm Editor, you can manage

	alarm types, alarm stack views, resolution types, activity types, and service levels.
Alert State	Provides the ability to apply formatting to UI components representing any other object in the system. Commonly used for alerting the user to an alarm activation on a device.
Client	Runs the Control Center Windows Client, which provides the front-end to Users. This is also used to perform most configuration of a Control Center solution.
Client Device	Represents a client-side device such as a PTZ keyboard. Each client device must be associated with a Windows Client.
Connection Manager	A Connection Manager provides the data conduit between Control Center with each of the connected sub-systems. A Connection Manager is automatically created when the Connection Manager service starts and communicates with that type of device as per the protocol defined in the manufacturer API.
Contact	Represents a contact in a Control Center solution. This is like a user with contact fields but without the ability to log in to Control Center.
Contact Group	Represents groups of contacts.
Data Connection	Provides a connection to a third-party database. Once the connection has been established, a SQL Management Studio style designer allows for viewing of the data schema. A series of Response Plans shapes allow for programmatic select, insert, updates and delete of data.
Date Time Schedule	Provides the ability to specify when events may occur based on a repetitive cycle. This is commonly used for defining blocks of time, for example, Office Hours. Evaluation of a Data Time Schedule can then be made to determine alarm creation, for example, only create alarm outside of working hours.
Device On	Includes real-life edge device such as single camera or something more complex such as an access control server. Each device is reliant on a specific device connector to be loaded into the solution. The device will then expose any functionality that is

	available per the manufacturer SDK, wrapped by the Control Center device connector.
Display Area	Provides a container for grouping tile layouts on a client. Display Windows are used to represent a section of the Windows desktop in size from a portion of one physical monitor to span monitors which are used to contain one or more Display Areas. The arrangement of Display Windows and Display Areas is held on the Client object and can be cloned between Clients.
Enterprise Settings	Provides global, federated settings which, for instance allows you to save PTZ active behavior and object selection color information in the Global Settings > Enterprise Settings tab.
Folder	Folder objects are management containers for all types of Objects within Control Center and maybe structured to an unlimited depth and used to manage both Security Permissions and Policies.
Graphical User Interface (GUI)	Allows customization of the Users visual experience by building controls that are subsequently displayed within Tile Layouts. Controls placed within a Graphical User Interface include basic controls such as buttons, labels, textboxes or more complex controls such as search control, Web viewer and so on.
Group	Contains User objects for the purposes of simplifying security management.
Hot Key Mappings	Displays the default set of system hot key mappings within the system that can be globally set across all clients that connect to the server. You can also modify the existing mapping and define additional shortcut keys for other areas in the system.
Location	Represents physical locations within the solution such as a region, city, campus, building, floor, room, and so on. A location is typically associated to a GUI and media to represent the map for that location or can be assigned geographical positioning information to be used with GIS mapping technology. A location then contains assets, such as devices and contacts, and other locations.
Media	Represents a range of files held within the solution, such as JPEG images for maps, PDF files for reports, and so on.

Modern Client Theme	Represents the theme available for the Modern Client. You can either customize the existing theme or create a new set of themes for the Modern Client.
Object Style Template	An Object Style Template allows configuration of different visual styles which can then be applied to some objects displayed on a scene to alter their appearance.
Placeholder	Represents an end-point connected to a complex device such as an access control server. Each placeholder must specify the parent device such as an access control server and a unique identified called Device Data (for example, a door number). This object can then be used throughout the system to represent that end-point, for example, plotting a door on a map and using that placeholder (door) to identify a location and nearest cameras based on an event from the access control server.
Remote Federation Service	Provides a means to communicate alarm information between sites. Depending on the license type, you can unlock the Node and Hub functionality, where a Node site is configured to send alarms and a Hub site to receive alarms from the connected federated Node. Ensure that each federated installation of Control Center has specific licenses for Hub and Node.
Report Template	Provides a form-based designer for building templates based on a Data Connection which can then be used to generate PDF reports.
Response Plan / VRP	<p>A Response Plan (Visual Response Plan or VRP) provides the framework for executing a process-based workflow. It provides the core mechanism for implementing a business logic within a solution. Response Plans can be executed from other objects in a solution such as from a Trigger, Alarm Types, or another Response Plan to automate specific user actions. Typically, response plans are used to automate user actions by raising events from a sub-system, for example to display a camera, handle alarms such as park or resolve alarms, display warning/informative notifications and so on.</p> <p>For more information, see Response Plan Shapes.</p>
Scenes	Allows you to create a new scene geographic or a scene schematic.

Sequence	Allows one or more cameras to be encapsulated in a single object. The sequence contains one or more steps where each step determines the camera, dwell period, and PTZ position. When shown, the sequence will iterate through each step showing the specified camera for the specified dwell period. Sequences can be managed by the end user via the System Explorer control.
Shortcut	Represents any other object in the system to provide a duplicate object of that type with similar features and functionality as the source object.
Tile Layout	Provides a container for GUIs and Devices which can be shown within a Display Area. A Tile Layout adopts a definition which specifies the number of rows, columns, and cells which span any number of rows and columns. Tile Layouts can be managed by the end user via the System Explorer control.
Timer	Provides a source of periodic events that can be reacted to by Triggers.
Trigger	Provides a means of acting upon, or reacting to, an event occurring on an object (or objects) managed by the Control Center Server.
User	Represents an individual who has access to log into the Control Center Server.

Computers

All servers and Windows clients are created in this folder. The server running Control Center will automatically create a Server object for itself upon load. The name of the server will assume the host name of the server machine. If there are insufficient licenses available for the server (this may occur when starting a server on an existing database) then the server will fail to start, and a message will be entered in the Event Viewer.

Equally, when a client first logs into a server, then the server will create a Windows Client object for the client with the same label as the host name of the PC. If there are insufficient client licenses available when the client is added, then the client object will be created as disabled and any user will not be able to log into Control Center using that client until additional licenses have been applied. Alternatively, another client can be disabled, and the new client enabled.

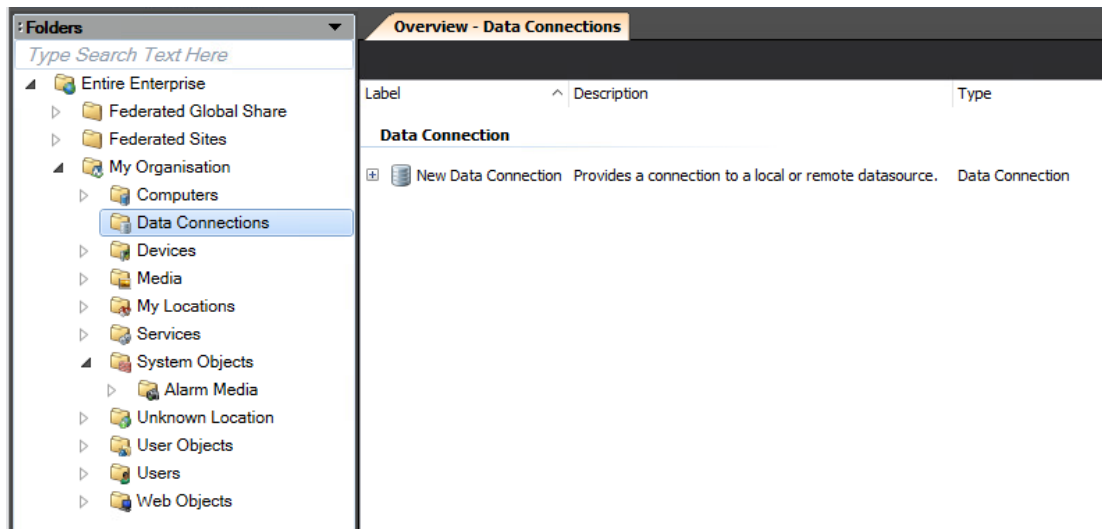
Label	Description	Type	Last Modified	Extra Information
Alarm Types Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Alarm Types Server	10/5/2020 12:46:27 PM	
Audit Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Audit Server	10/5/2020 12:46:26 PM	
Connection Manager Server				
P-SR-19-SQL17-1.dev.cnluk.com [Default]	Connection Manager instance 'Default' running on th...	Connection Manager Server	10/5/2020 12:46:28 PM	
Federated Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Federated Server	10/5/2020 12:46:29 PM	
Geographic Information Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Geographic Information Se...	10/5/2020 12:46:27 PM	
Notification Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Notification Server	10/5/2020 12:46:24 PM	
Rules Engine Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Rules Engine Server	10/5/2020 12:46:27 PM	
Security Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Security Server	10/5/2020 12:46:27 PM	
Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server Computer with the IP hostname of P-SR-19-SQ...	Server	10/5/2020 12:45:58 PM	
Video Export Server				
P-SR-19-SQL17-1.dev.cnluk.com	Server with the IP hostname of P-SR-19-SQL17-1.dev...	Video Export Server	10/5/2020 12:46:27 PM	
Windows Client				
P-Win10-2.dev.cnluk.com	Client Computer with the IP hostname of P-WIN10-2....	Windows Client	10/5/2020 12:50:11 PM	

Additionally, a server object is created for every service that could be deployed on a separate server. However, only the Server objects consume server license points.

Data Connections

The Data Connections folder contains all data connections created to external databases. By default, an Online State Data Connection is created, which is used for logging all device state changes and users for reporting against device health in the Admin Interface.

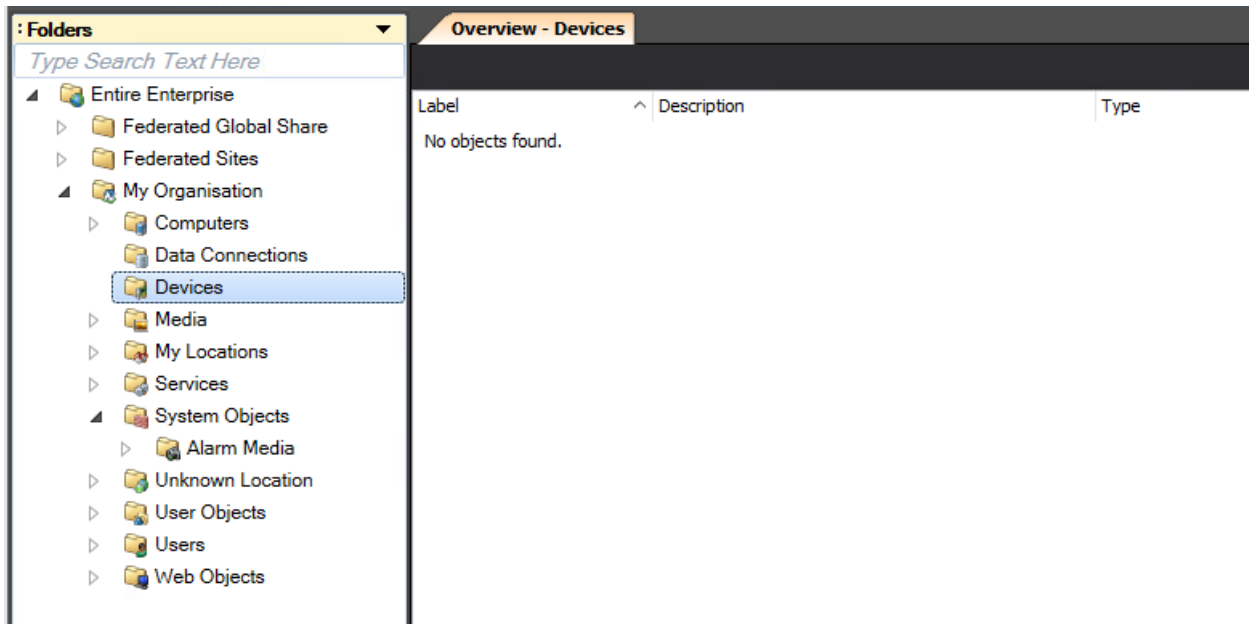
In addition, the Data Connections folder is checked when restoring an existing solution database as any failed data connections will show as enabled.



Devices

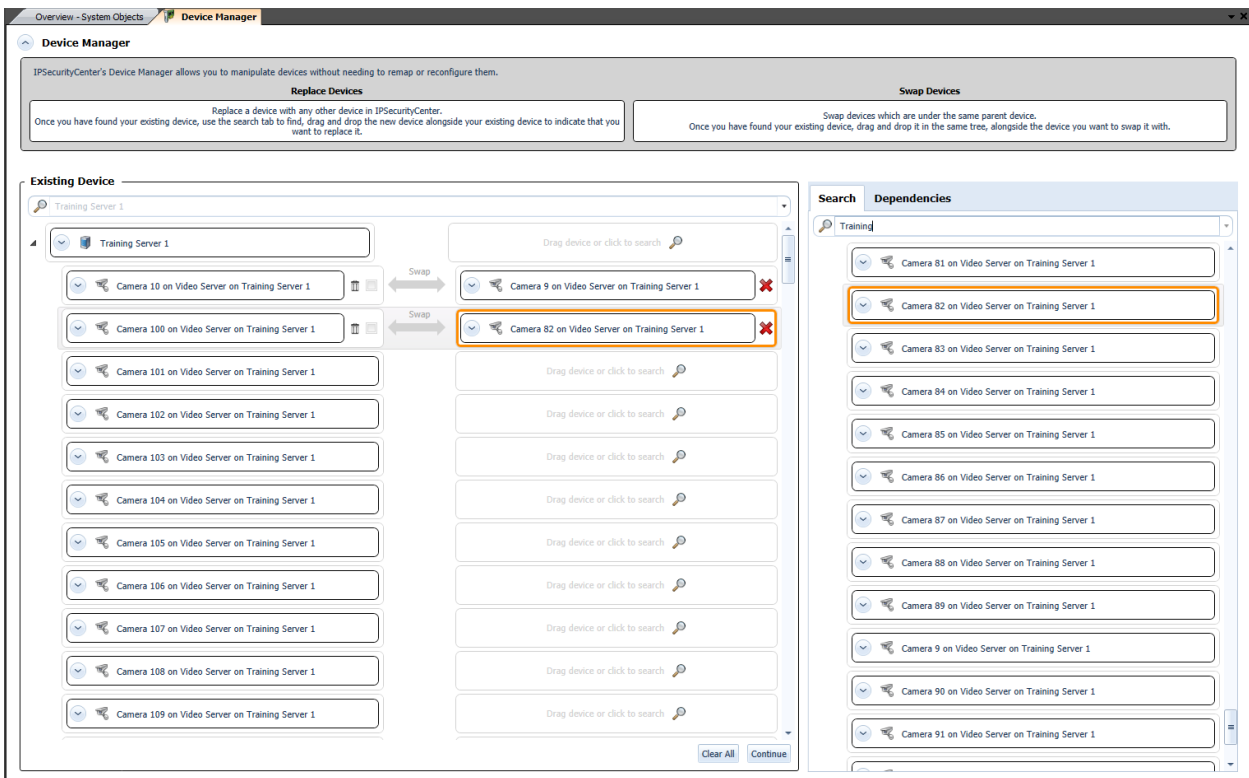
Even though devices are not available by default, all devices that are created in the solution are added into the Devices folder. Typically, extra folders are added in this section to differentiate between different types of devices. Any number of folders with any depth of hierarchy can be used to best organize objects in Control Center.

Objects can also be moved between folders by dragging and dropping one or more objects in the System Configuration window. Cameras for example are usually dragged from this folder into the relevant locations once they are created. Alternatively, shortcuts can be created and placed in the locations instead, which provides the ability to reference a camera in more than one location where location floor plans overlap for instance.



Swapping and Replacing Devices

Device Manager allows you to swap and replace devices without having to reconfigure the dependencies for the new devices.



You can:

- Swap individual devices. For example, two cameras may be mis-wired in your subsystem and you want to swap them around.
- Replace existing devices with new devices. For example, you may want to replace some end of life cameras with new cameras.
- View device dependencies. For example, any sequences that the existing device is part of.

A Type Permission, Device Manager, allows you to restrict access to the Device Manager.

- You need Read access to view device dependencies but not perform any changes to existing devices.
- You must have Write access to the devices you want to commit changes to.

The following table describes how the configuration information is updated when you swap or replace devices using Device Manager.

Dependencies	Supported	Description
Tile Layouts	Yes	The new device is part of the same tile layouts as the original device.
Sequences	Yes	The new device is part of the same sequences as the original device.
Scenes	Yes	The new device is added to the same scenes that the original device was added to.
GUIs	Yes	Any GUIs configured with the original device now apply to the new device
Shortcuts	Yes	The shortcuts to the original device now resolve to the new device.
GIS Layers	Yes	The new device is part of the same GIS layers as the original device.
Placeholders	Yes	Any placeholders configured for the original device now apply to the new device.
Extension references	Yes	Any extension references applied to the original device now apply to the new device.

Asset groups	Yes	The new device is now in the same asset groups as the original device.
Visible Object Mappings	Yes	The new device now uses the same visible object mappings as the original device.
Video export schedules	No	Video export schedules are ignored. You must change your export schedule after you have swapped or replaced devices, as existing export requests may fail after swapping or replacing devices.
Response Plans	No	If the existing device you want to replace is configured in a response plan, then you cannot replace that device. You must manually remove the existing device from the response plan first.
Alarms	No	Any alarms that are configured for the original device are not applied to the new device. The existing alarms are not deleted but you must manually configure the alarms for the new device.
Triggers	No	You must manually configure triggers for your new device.
Alarm type definitions	No	You must manually configure alarm type definitions for your new device.
Correlated alarm types	No	You must manually configure correlated alarm types for your new device.
Alarm type modifiers	No	You must manually configure alarm type modifiers for your new device.
Alert state objects	No	You must manually configure alert state objects for your new device.

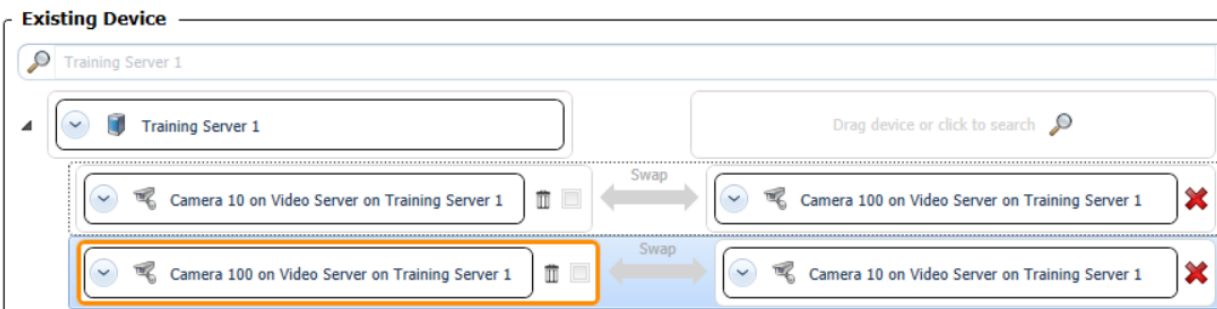
To do this:

1. Go to **System Configuration > Entire Enterprise > My Organization > System Objects**.
2. Select the **Device Manager** tab. Alternatively, you can right-click on the device you want to replace and select **Device Manager**.

3. In **Existing Device**, search for the device you want to swap or replace. The device and all its connected devices display. **Note:** Searching for a server object shows all directly connected devices under that object.
4. Select **Dependencies** to see how your existing device is configured. This allows you to see the configuration information that will be updated when you replace or swap the devices.

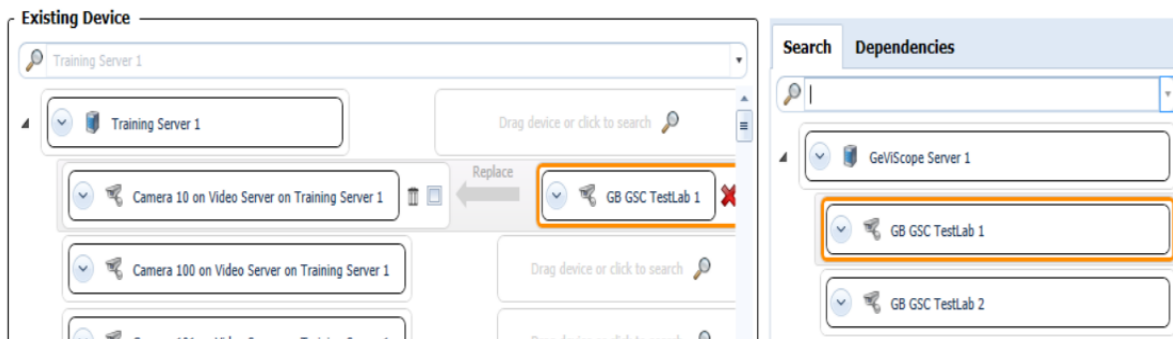
To swap devices:

In **Existing Device**, within the list of connected devices, drag one device alongside another to swap the devices around.




To replace devices:

- a. Select **Search** and enter the name of the new devices.
- b. Drag the new devices from the **Search** tab alongside the device you want to replace in **Existing Device**.



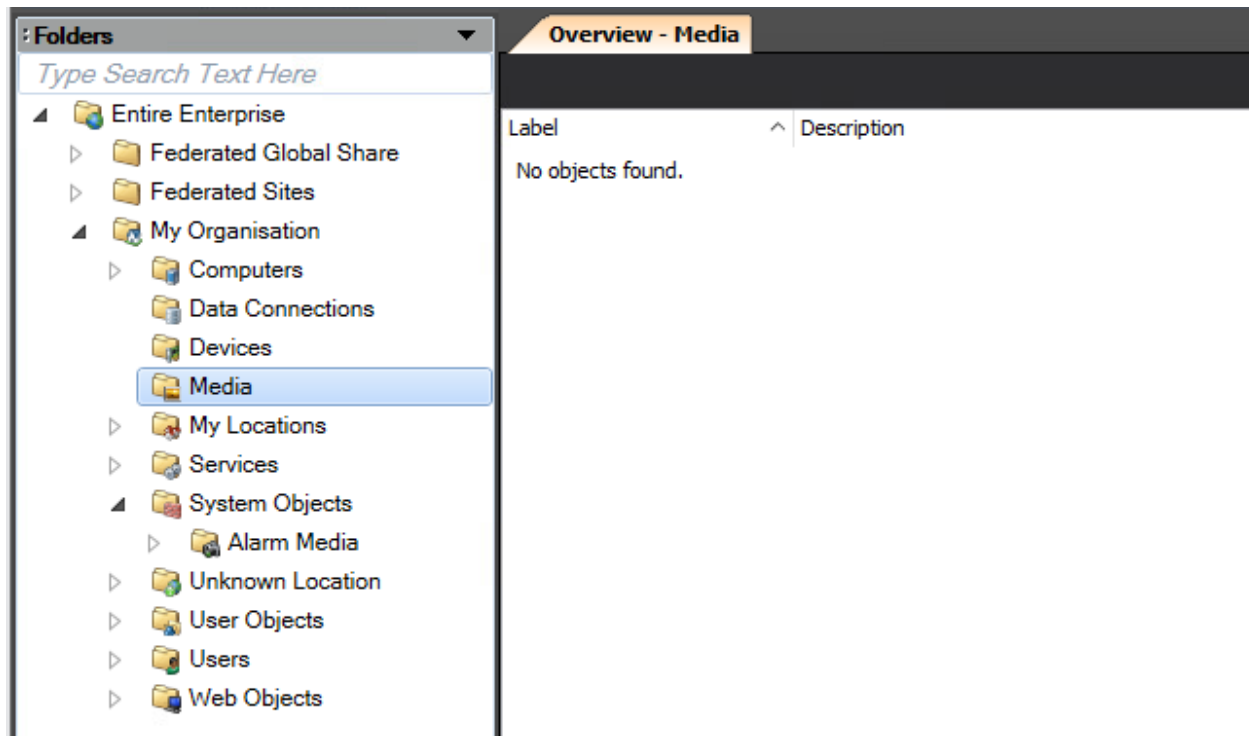
5. Select **Dependencies** to see how your device configuration will be updated when you replace or swap the devices.
6. Select **Rename Devices** if you want the label of the existing device to be renamed with the label of the replacement or swapped device. For example, you may have a camera labelled **A1** and you want to replace camera **A1** for a camera labelled **A2**. If you want:
 - o Camera **A1** to be re-labelled **A2**, select the **Rename Devices** box.

- Camera **A1** to keep the label **A1**, leave the **Renames Devices** box deselected.
7. If you want your existing device to be deleted, once the device has been replaced or swapped with another, select next to .
 8. Select **Continue**. The **Summary** page describes all the dependencies and/or deletions for the devices you have selected.
 9. If you want to make changes, either:
 - Select **Back** to return to the previous screen, or
 - click away, make any changes required to your device dependencies, and then return to Device Manager.
 10. If you are happy that the summary information is correct, select **Confirm** to commit your changes.

Media

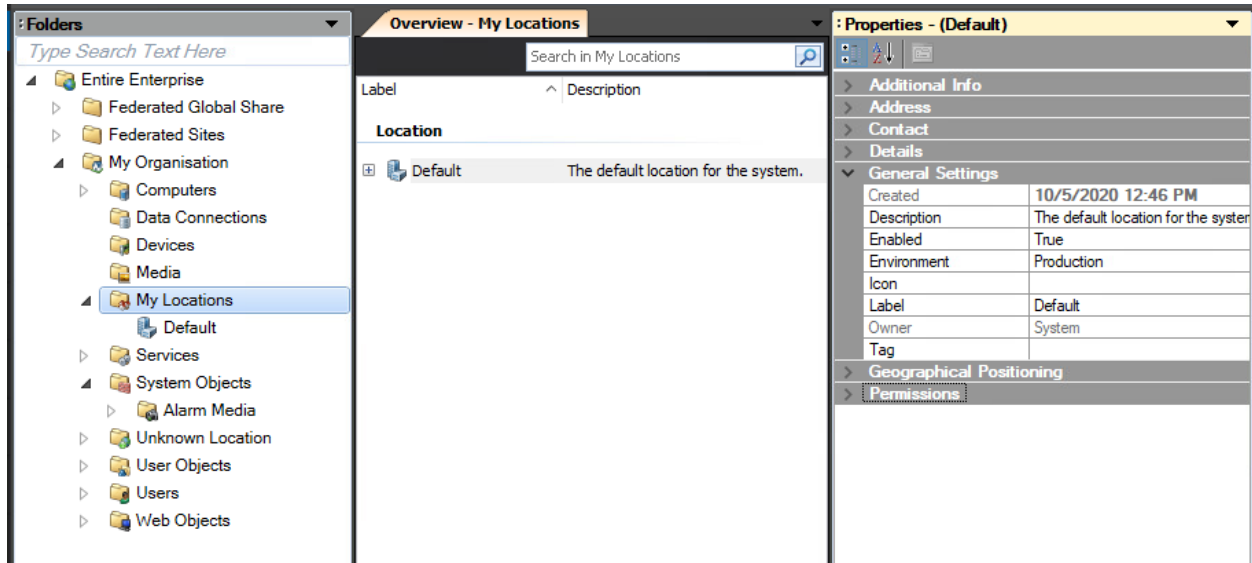
The Media folder does not contain any objects by default, however you must use this folder to store any media files within the solution. This may include images for maps and floor plans or generated reports.

A copy of the file is held in the Control Center configuration database. However, as this may consume most of your disk space, an alternative to storing floor plans in Control Center is to reference images on a network drive that can be used in any maps (Default GUI for a Location) as part of the solution.



My Locations

By default, a location called Default is available when you access the Control Center Client for the first time. Rename the default location and ensure that it appears as the top-most location in the Locations hierarchy. By default, a Geographic Scene is created and associated with the default location. The default scene uses the Open Street Map layer to show the World map. Always create all locations in this folder. Typically, you have a single top-level location and then several locations below that. The System Explorer references the top-level location and show all locations and assets within that location.












Default Icons per Location Type

Each Location Type in Control Center includes a specific default icon for that location type to assist visualization of the location types when they are plotted on a scene.

Currently, you cannot amend the default icons, however you can replace a default icon with a custom icon.

The default icons will depend upon which icon set is selected in **Global Settings>Styling**. The following table lists the default icon for each location type.

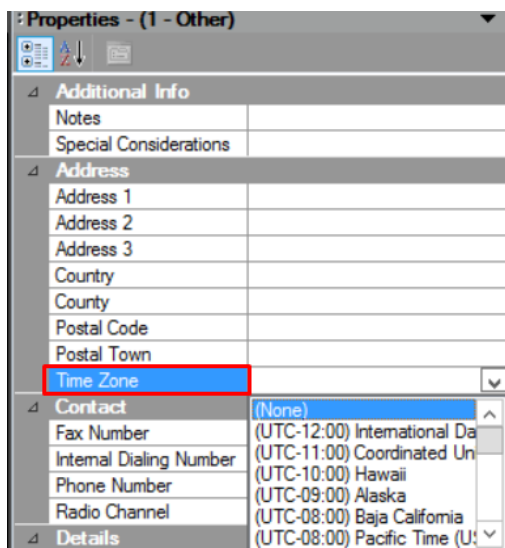
Location Type	High Detail Icon Set	Icon Name
Other		Office_building
Country		earth
Region		window_earth
Site		pin_orange

Building		Office_building
Floor		table
Room		Layout_east
Zone		Office_building
Customer		Office_building

A commissioning user can also specify default colors for point plotting and to specify which map zoom level settings will show or hide various Location Types.

Time Zone Support for Locations

Using the Time Zone property in Locations, you can indicate the Time Zone of the location.



The Time Zone property in Alarm Stacks enables you to show the time when an Alarm was created, which is local to the Location that the Alarm is attached to.

This property is also available to commissioning users in the scripting interface.

Services

The Services folder contains all objects representing the various Control Center services running within the solution. This feature is useful to directly interact with the services from within Control Center.

Label	Description	Type	Last Modified	Extra Information
Alarm Types Service				
Alarm Types Service	Alarm Types Service	Alarm Types Service	10/5/2020 12:46:26 PM	
Connection Manager Service				
Default	Connection Manager Instance 'Default'	Connection Manager Service	10/5/2020 12:46:26 PM	
Core Service				
Core Service	Core Service	Core Service	10/5/2020 12:45:57 PM	
Federated Service				
Federated Service	Federated Service	Federated Service	10/5/2020 12:46:27 PM	
Geographic Information Service				
Geographic Information Service	Geographic Information Service	Geographic Information Se...	10/5/2020 12:46:26 PM	
Notification Service				
Notification Service	Notification Service	Notification Service	10/5/2020 12:46:21 PM	
Rules Engine Service				
Rules Engine Service	Rules Engine Service	Rules Engine Service	10/5/2020 12:46:26 PM	
Security Service				
Security Service	Security Service	Security Service	10/5/2020 12:46:26 PM	
Video Export Service				
Video Export Service	Video Export Service	Video Export Service	10/5/2020 12:46:26 PM	

System Objects

The System Objects folder contains core objects which are integral to a Control Center solution. The GUIs created in this folder are useful throughout the system. By default, the following System Objects are available in the system:

Objects	Description
Alarm Media	Includes the snapshots of handled alarm types.
Alarm Types	Includes a wizard for configuring alarm types and alarm stack views.
Dashboard	Displays the default system dashboard that is displayed on the Overview page by default. The following gadgets are displayed with their respective data: <ul style="list-style-type: none"> Core Server Device States by Device Type

	<ul style="list-style-type: none"> • Alarms by Alarm Type • Device States • Alarms by State • Device State
Date/Time Schedule	<p>By default, the following Date/Time Schedules are available in this folder:</p> <ul style="list-style-type: none"> • 24 x 7 Allow – The default schedule used for all objects. • Alarm Maintenance – The schedule used for alarm maintenance task in Control Center. • System Maintenance – The schedule used for maintenance tasks in Control Center.
Display Area	<p>Includes the following system display areas:</p> <ul style="list-style-type: none"> • System Alarm Stack – Displays the lower display area. • System Left – Displays the left-hand side display area. • System Main – Displays the main display area. • System Main Right – Displays the main right display area. • System Popup – Displays the Popup display area. • System Right – Displays the right-hand side display area.
Enterprise Settings	<p>The default enterprise settings for the local system which includes the information saved in the Global Settings > Enterprise Settings tab.</p>
Graphical User Interface (GUI)	<p>Includes the following default GUIs:</p> <ul style="list-style-type: none"> • Administrator Interface – Contains the ribbon bar GUI control and is automatically shown in the default display window. You can access it by clicking the Control Center button. Note that no configuration is required for this UI. • Alarm Stack – Contains the Alarm Stack grid GUI control, which automatically shows alarms based on the views configured in the system. The Alarm Stack GUI must be configured within the user interface. • Main Menu – Includes the main items on the menu for configuring the Custom Menu items property on the ribbon GUI control.

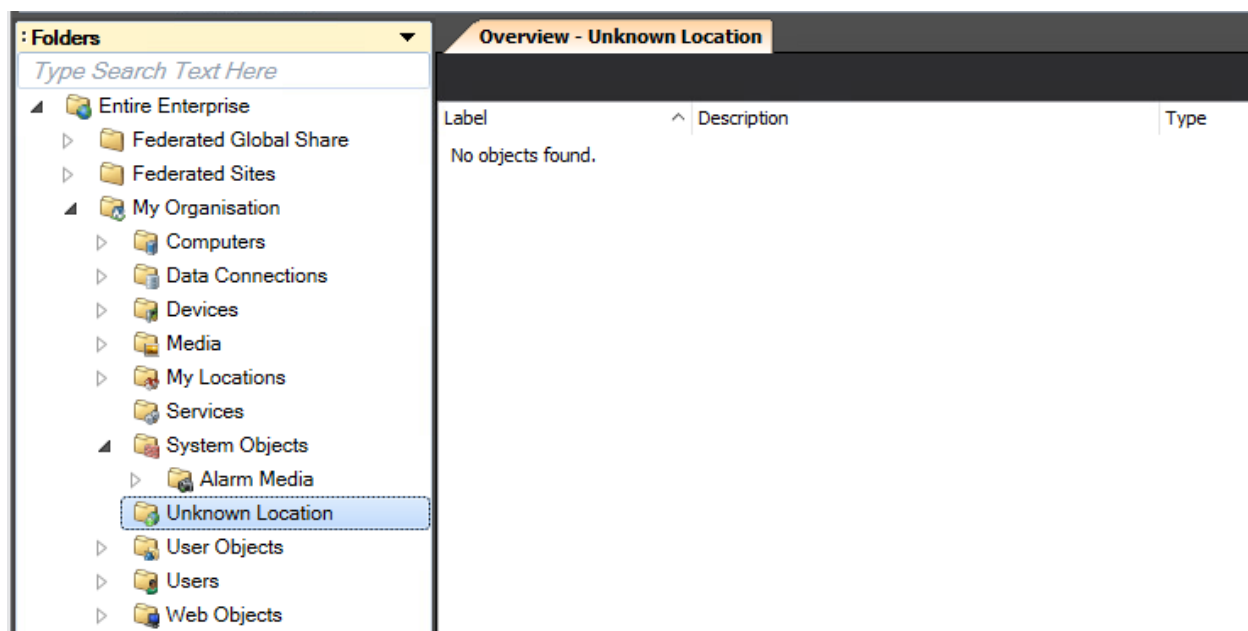
	<p>No further configuration is required to display the GUI however; you can show the main menu by setting the Interactivity Mode property on the Windows Client object in System Configuration window > Computers.</p> <ul style="list-style-type: none"> • Map – Contains a map control that is used as the standard map surface. Use this map when changing the location in the System Explorer. Additionally, you can configure the map to react to user actions. For more information, see Mapping. • System Explorer – Contains the System Explorer GUI control. By default, appears on the left of the default display window. <p>The System Explorer GUI must be configured to specify the base location and other properties. No further configuration is required to display the GUI. However, the System Explorer can be shown by setting the Interactivity Mode property on the Windows Client object.</p>
Hot Key Mappings	<p>Displays the default set of system hot key mappings within the system that can be globally set across all clients that connect to the server. You can also modify the existing mapping and define additional shortcut keys for other areas in the system.</p>
Modern Client Theme	<p>Displays the default theme available for the Modern Client. You can either customize the existing theme or create a new set of themes for the Modern Client.</p>
Report Template	<p>The Admin Interface uses the following two device report templates for generating reports for the device status:</p> <ul style="list-style-type: none"> • Device Online Current Status • Device Online History <p>Both templates can be edited to include additional information such as the company logo, header, footer, and so on.</p>
Tile Layout	<p>The following default tile layouts are created by default:</p> <ul style="list-style-type: none"> • System Alarm Stack - Contains the Alarm Stack GUI that is used to show the alarm stack. • System Blank 1 Way - A default tile layout to show a single tile layout.

	<ul style="list-style-type: none"> • System Blank 4 Way - A default tile layout to show a tile layout with 4 tiles. • System Blank 9 Way - A default tile layout to show a tile layout with 9 tiles. • System Map - Contains the Map GUI that is used to show the map.
--	---

Typically, additional folders are created within the System Objects folder to contain most of the functionality added to the solution. For example, if you have a Visitor Log and a Webpage Viewer feature commissioned into the solution, then two folders would be created in the System Objects folder to contain a logic for each feature. System Objects typically include several VRPs and GUIs.

Unknown Locations

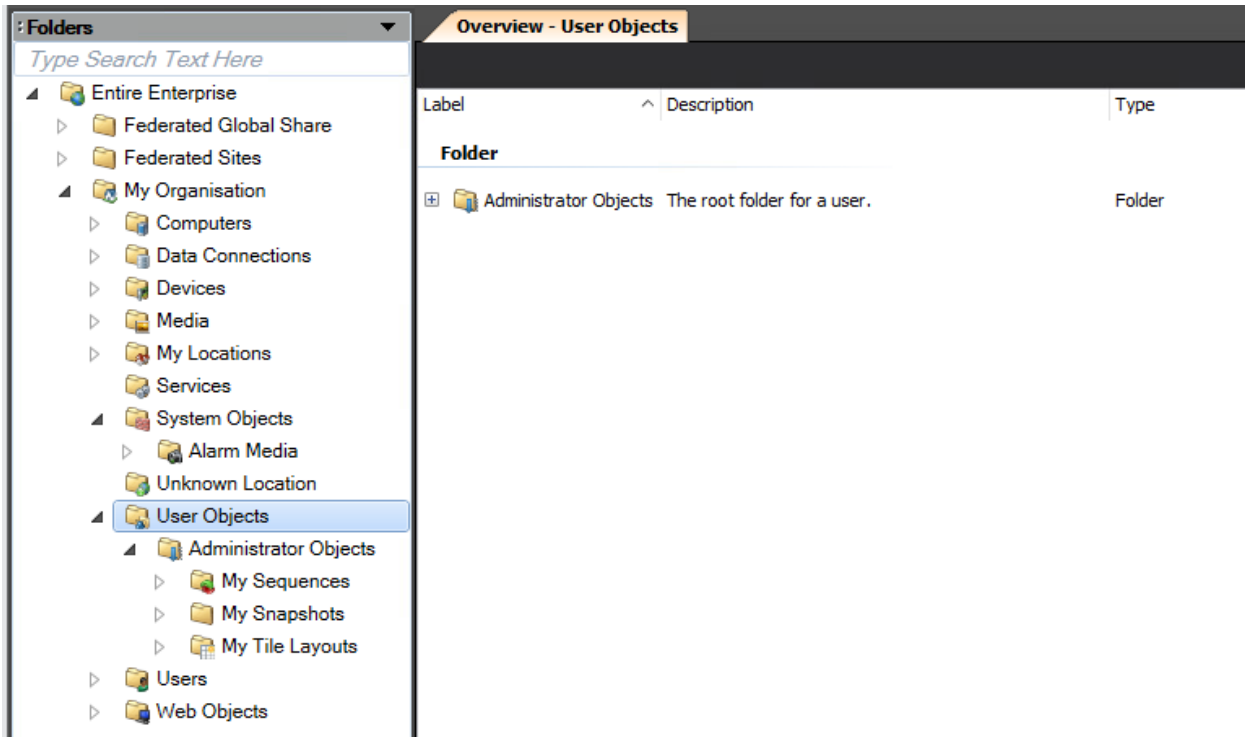
The Unknown Locations folder does not contain any objects by default and is not commonly used for solution centric logic. Typically, objects which are redundant and need to be deleted, or test objects that need to be moved are created here.



User Objects

The User Objects folder includes a folder for each user in which user related objects are held. Currently, this includes all sequences and tile layouts created by that user which are not made available for all users.

By default, the Administrator user can view all user objects folder. Other users will only be able to view their object user objects folder.



Label	Description	Type
Folder		
Administrator Objects	The root folder for a user.	Folder

Users

The Users folder contains several default Groups and the Administrator user object. The default credentials for the Administrator user are:

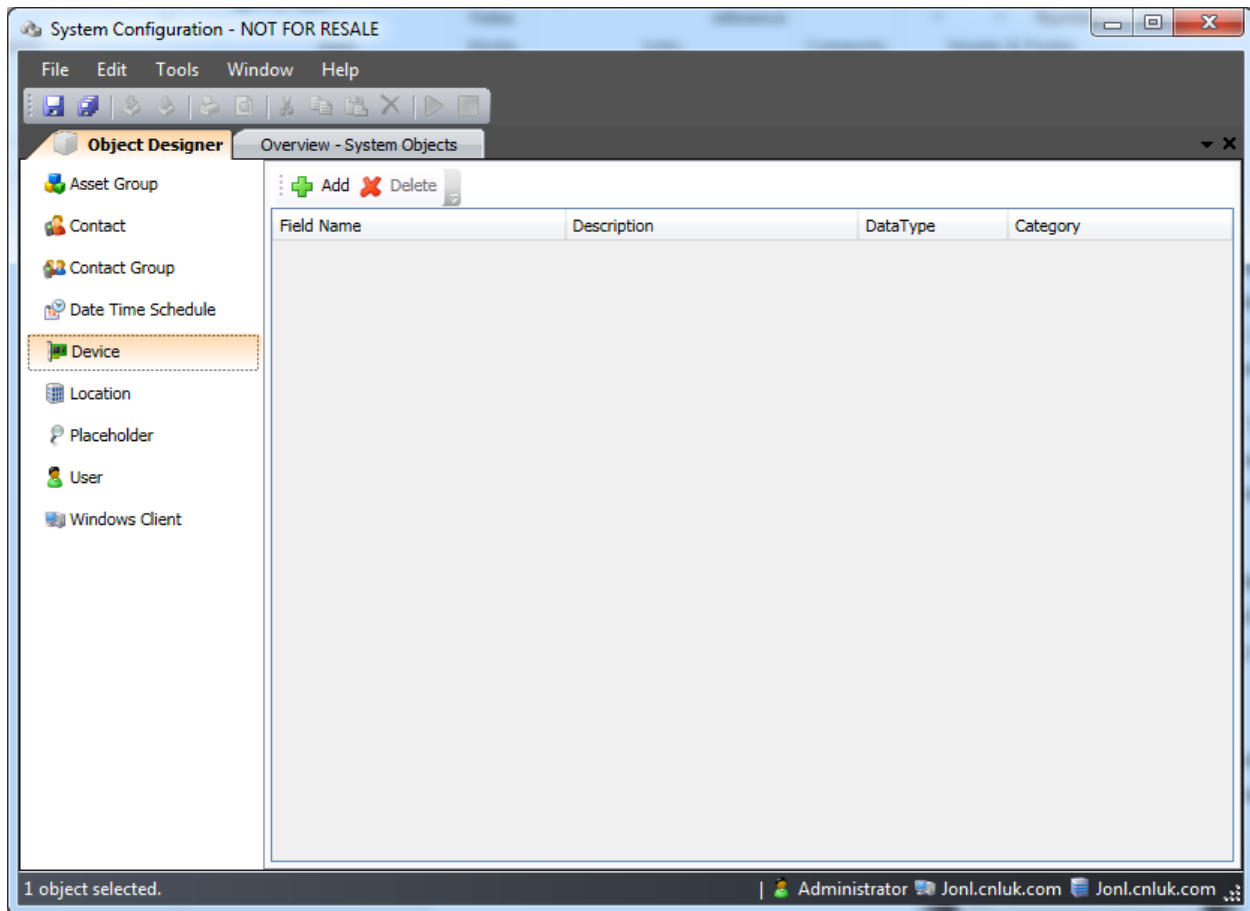
- Username: root
- Password: configured on login

Additional Users and Groups can be created in this folder as required. If you need to configure many users, use folders to organize them logically.

Label	Description	Type
Group		
+ Account Administrators	Account Administrators can create user accounts	Group
+ Administrators	Administrators have complete and unrestricted acces...	Group
+ Backup Operators	Backup Operators can perform Database functions, a...	Group
+ Device Administrators	Device Administrators can create devices	Group
+ Mobile Client Users	Mobile Client Users can have access to mobile clients	Group
+ Response Plan Designers	Response Plan Designers by default have access to t...	Group
+ Users	Users are prevented from making accidental or intent...	Group
+ Video Export Administrators	Video Export Administrators can manage exporting of...	Group
+ Web Portal Users	Web Portal Users can have access to web portal	Group
User		
+ Administrator	Built-in account for administering the system	User
+ System	Built-in account for running the system	User

Object Designer

Control Center contains several standard object types. The standard fields defined for each object type can be seen in the Property Grid by selecting an object.

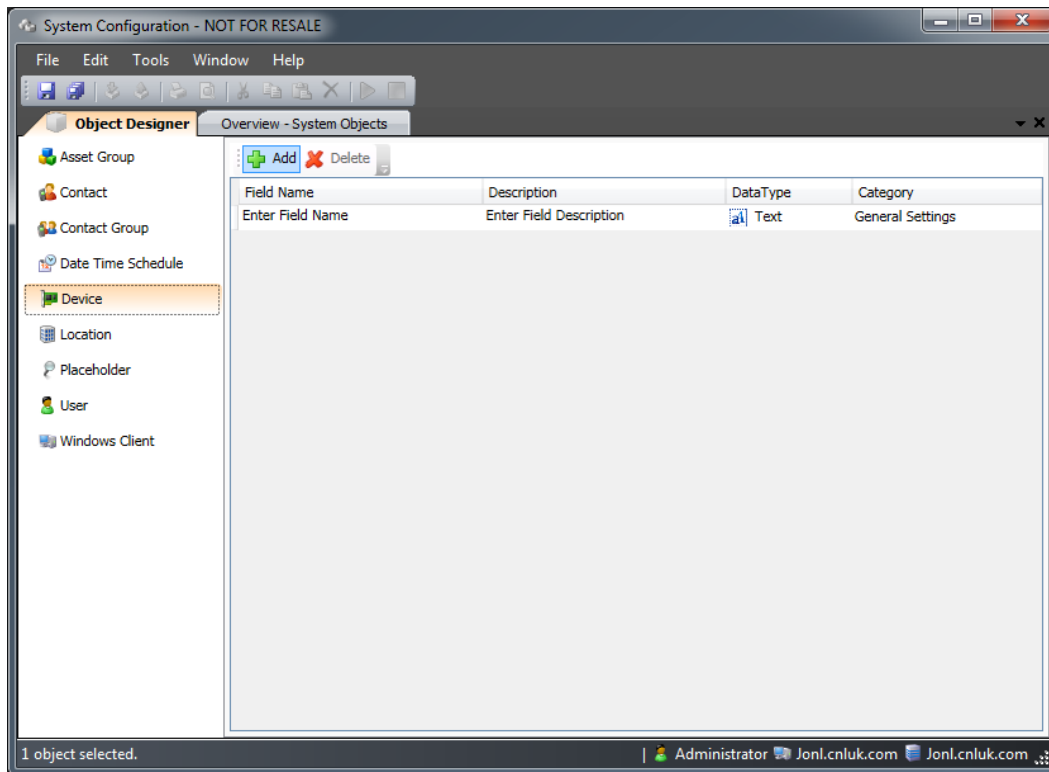


Adding a Field

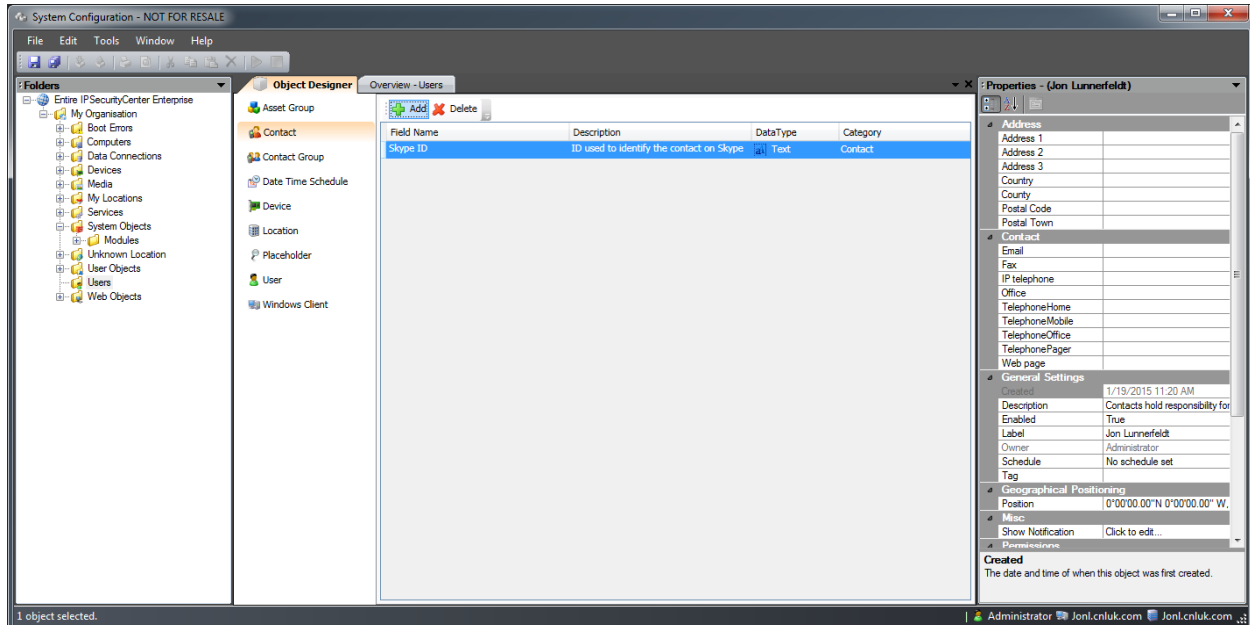
Additional fields can be added to some object types, for example, you can add additional contact fields to the Contact object type.

To add a field to an object type:

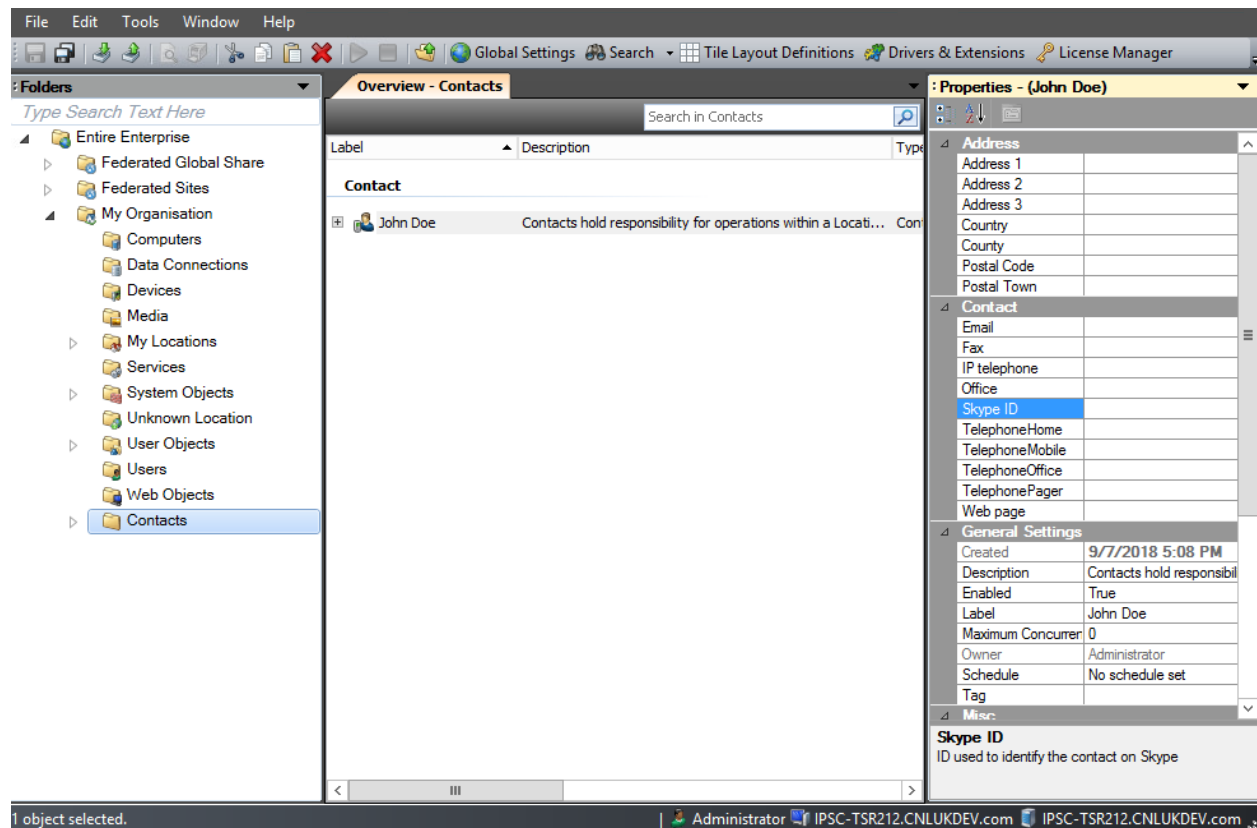
1. On the toolbar, click the **Object Designer**.
2. Select the object to be modified.
3. Click **Add**. A new row is added to the list of fields.



4. Change the Name, Description, Data Type and Category to fit with the requirement.

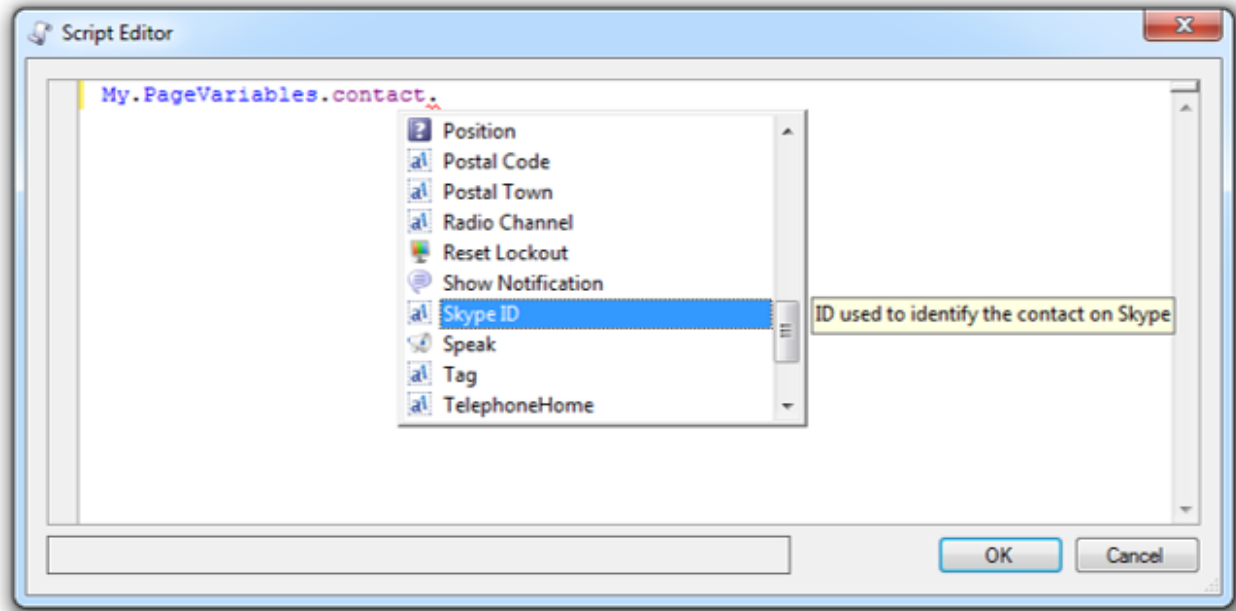


5. Close the **Object Designer**. The new field can be verified by selecting an object of the type in the **System Explorer**. The new field appears in the **Property Grid**.



Using a Custom Field

There are no user controls in the user interface that expose custom fields, however custom fields can be accessed from Response Plans and from the Graphical User Interface event pages. To access a custom field, you must first create a variable of the type and then use the variable. For example, in the following screenshot, custom fields are used while editing a script shape in a response plan.



GIS Layer Manager

GIS Layer Manager is where you configure the GIS layers for your Control Center solution. Typically, a new GIS Map layer is added when you first set up your Control Center solution or when new mapping sources become available. Control Center supports adding the following layers to a map:

- Open Street Map
- Bing Maps
- WMS
- WMTS
- KML
- Trail Point

For adding and deleting a GIS Layer, see [Configuring GIS Map Layers](#).

Service Monitor

The Service Monitor provides a visual representation of the various services running within your Control Center solution. It shows the status of each service and allows you to change the status of a service within Control Center. For example, you can view the memory and CPU consumption of each of the processes in Control Center, stop and restart processes, and so on.

The Service Monitor is the first of several features aimed at providing improved tools for maintaining a Control Center solution.

Name	Process Name	Machine Name	State	CPU	Memory	Change Status	Process Id
IPSecurityCenter Audit Server	CNL.IpSecurityCenter.Auditing.WindowsService	PRIYA-VM.cnluk.com	Stopped		0 KB		0
IPSC Streaming Server	CNL.IpSecurityCenter.Driver.Streaming.Cli	PRIYA-VM.cnluk.com	Stopped		0 KB		0
IPSC Client Watchdog	ipsccrowd	PRIYA-VM.cnluk.com	Stopped		0 KB		0
IPSecurityCenter Monitoring Service	CNL.IpSecurityCenter.Monitoring.WindowsService	PRIYA-VM.cnluk.com	Running		6.58 MB		1796
IPSecurityCenter Connection Manager Service	CNL.IpSecurityCenter.Driver.ConnectionManager.WindowsService	PRIYA-VM.cnluk.com	Running		5.13 MB		1700
IPSecurityCenter Notification Service	CNL.IpSecurityCenter.Notifications.WindowsService	PRIYA-VM.cnluk.com	Running		5.87 MB		2120
IPSecurityCenter Server	ipscserver	PRIYA-VM.cnluk.com	Running		3.23 MB		2520
IPSecurityCenter AlarmTypes Service	CNL.IpSecurityCenter.AlarmTypes.WindowsService	PRIYA-VM.cnluk.com	Running		3.99 MB		1256
IPSecurityCenter Report Server	CNL.IpSecurityCenter.Reporting.WindowsService	PRIYA-VM.cnluk.com	Stopped		0 KB		0
IPSecurityCenter Video Export Server	CNL.IpSecurityCenter.VideoExport.WindowsService	PRIYA-VM.cnluk.com	Running		54.9 MB		2708
IPSC Video Control Manager (VCM)	CNL.IpSecurityCenter.Driver.VideoControlManager	PRIYA-VM.cnluk.com	Stopped		0 KB		0
IPSecurityCenter ONVIF Service	CNL.IpSecurityCenter.Driver.Streaming.Onvif.WindowsService	PRIYA-VM.cnluk.com	Stopped		0 KB		0
IPSC Windows Client	ipscrc	PRIYA-VM.cnluk.com	Running		9.21 MB		4060

Machine Name	P-SR19-SQL17-1.dev.cnluk.com						
CPU	 12.09 %						
Available Memory	9376.65 MB						

Name	Process Name	Machine Name	State	CPU	Memory	Change Status	Process Id
Connection Manager Service (Default)	Everbridge.ControlCenter.Driver.ConnectionManager.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		97.05 MB		7176
Windows Client	Everbridge.ControlCenter.WindowsClient	P-SR19-SQL17-1.dev.cnluk.com	Stopped		0.00 MB		0
Video Control Manager (VCM)	Everbridge.ControlCenter.Driver.VideoControlManager	P-SR19-SQL17-1.dev.cnluk.com	Stopped		0.00 MB		0
Rules Engine Service	Everbridge.ControlCenter.RulesEngine.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		272.52 MB		8716
Security Service	Everbridge.ControlCenter.Security.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		168.02 MB		9788
Audit Server	Everbridge.ControlCenter.Auditing.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		102.31 MB		6536
Monitoring Service	Everbridge.ControlCenter.Monitoring.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		90.20 MB		7572
Federating Service	Everbridge.ControlCenter.Federation.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		236.83 MB		8696
Client Watchdog Service	Everbridge.ControlCenter.ClientWatchdog.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Stopped		0.00 MB		0
Core Server	ipscserver	P-SR19-SQL17-1.dev.cnluk.com	Running		558.14 MB		2300
Alarm Types Service	Everbridge.ControlCenter.AlarmTypes.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		456.75 MB		6668
Streaming Server	Everbridge.ControlCenter.Driver.Streaming.Cli	P-SR19-SQL17-1.dev.cnluk.com	Stopped		0.00 MB		0
Video Export Server	Everbridge.ControlCenter.VideoExport.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		195.70 MB		7264
Notification Service	Everbridge.ControlCenter.Notifications.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		226.77 MB		4432
GIS Service	Everbridge.ControlCenter.GIS.WindowsService	P-SR19-SQL17-1.dev.cnluk.com	Running		211.64 MB		4140

The Service Monitor displays the following information:

Name	Description
Process Name	The name of the Control Center process.
Machine Name	The machine that is running the Control Center process.
State	The running status of a service. For example, if you stop the Control Center AlarmTypes Service in the Services dialog, the state of the service will show as stopped in the Services Monitor.
CPU	The CPU consumption indicated by horizontal dotted lines. Double dotted line indicates a rise in CPU consumption.
Memory	The memory consumption of each of the services. The increase in memory consumption is indicated by a red up arrow and a decrease in memory is indicated with green down arrow.

Change Status	Hovering over this cell shows the Stop and Restart buttons that can be used for stopping and restarting the respective processes. For a stopped process, only Start button is displayed.
Process Id	This is the Process Id generated by Windows for each of the Control Center processes/services.

To make effective use of this feature, ensure that you have all the Control Center components installed.

Searching

Searching for objects is one of the most essential features in Control Center that can be performed in various areas of the system using the Search Objects window. Depending on the context of the search, some of the boxes on the Search Objects window may be pre-filled.

The Search Objects window can be loaded in two different modes:

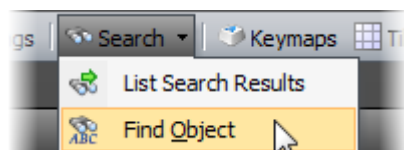
- **Standard** - The search results are shown within the dialog.
- **Compact** - The search results are shown upon submitting the search dialog. The latter option is useful for listing out search results in the System Configuration window.

To perform a search:

1. Specify the types of object to be found and the locations to search within. The results can also be narrowed further by specify part of the label or description.
2. Select the required object from the list of objects found matching your search criteria.

Find Object

Find Object is the standard search option that appears throughout the system when an object is required, or it can be shown via the toolbar in the System Configuration window.

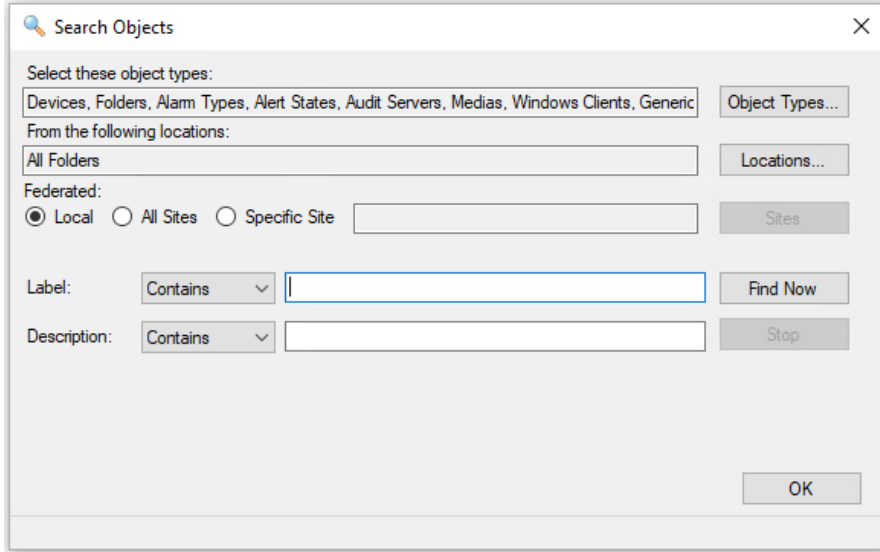


Searching for an Object Using the Object Type Picker

The Object Picker dialog supports filtering of object types in search.

To perform a search:

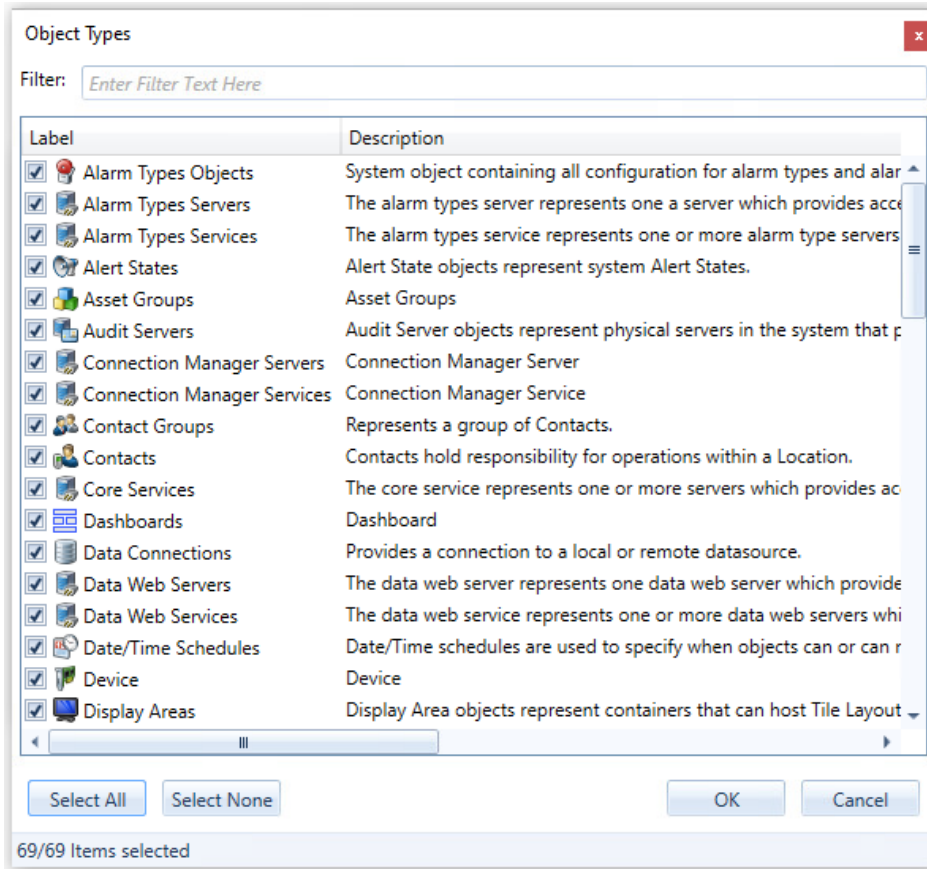
1. From the toolbar, click **Search** to display the **Search Objects** window.



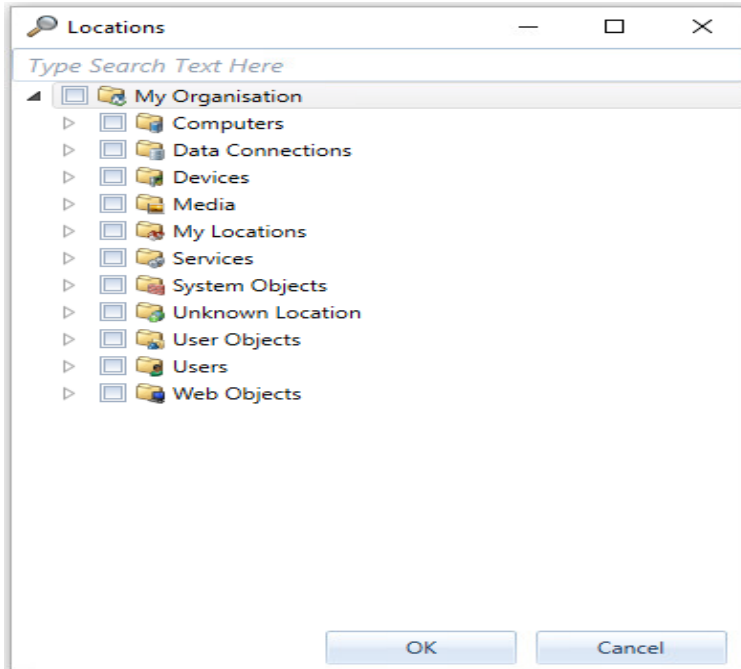
2. In the first box, specify the objects types to search for.

The object type may be pre-selected depending on the screen from which you called the Search Objects window; if it is pre-selected move on to the next step.

3. Click **Object Types** to display a list of objects then specify one or more types by which to search. The following figure shows an example of the list:



4. Click the check box next to the object type to search by, and then click **OK**. The search form will display the object types selected.
5. In the second box, specify the folders or locations in which to search for objects. The location may be pre-selected depending on the screen from which the Search Objects window was shown; if it is pre-selected move on to the next step.
6. Click **Locations** to display a tree view of all folders and locations. The following screen shows an example of the tree view:



Use the checkboxes in the tree view to select the required folders. Use the + and - buttons to expand and collapse branches of the tree view as necessary. Click OK when all required folders are ticked. The search window will display the list of selected locations.

7. Select from one of the following Federated options:
 - **Local** – Searches for all objects of the selected Users' Object types on the Sender site and returns on the Receiver's site.
 - **All Sites** – Searches for the selected Users' Object types on Sender and Receiver sites.
 - **Specific Site** – Searches for all Objects of the selected Users' Object types on a specific site.
8. Perform the search by clicking **Find Now**.
9. Use the label and description controls to refine the search further by specifying part of the object's label and/or description. Click the **Find Now** button to re-run the search.

To specify part of the label:

1. From the drop-down list next to the Label box, select from the options to refine the search:
 - **Contains** – Specify a part of the object's label.
 - **Is Exactly** – Specify exactly the object's label.
 - **Starts With** – Specify the first one or more characters in the object's label.

2. Type the label text in the adjacent box.

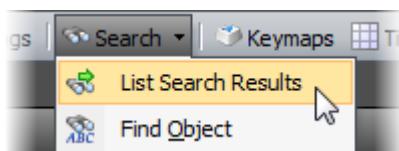
To specify part of the description:

1. From the drop-down list next to the **Description** box, you can refine the search by selecting one the following options:
 - **Contains** – Specify a part of the description's label.
 - **Is Exactly** – Specify exactly the description's label.
 - **Starts With** – Specify the first one or more characters in the description's label.
2. Type the description text in the adjacent box.
3. Select the Include disabled objects checkbox if you would like the search results to include objects that have been disabled.
4. In the list of matching objects found, make your selection by using one of the following methods:
 - Double-click the required object.
 - Click the required object to highlight it, then click **OK**.
 - Click **Select All** to select all objects in the found list, then click **OK**.
 - Click **Select None** to deselect all objects in the found list.

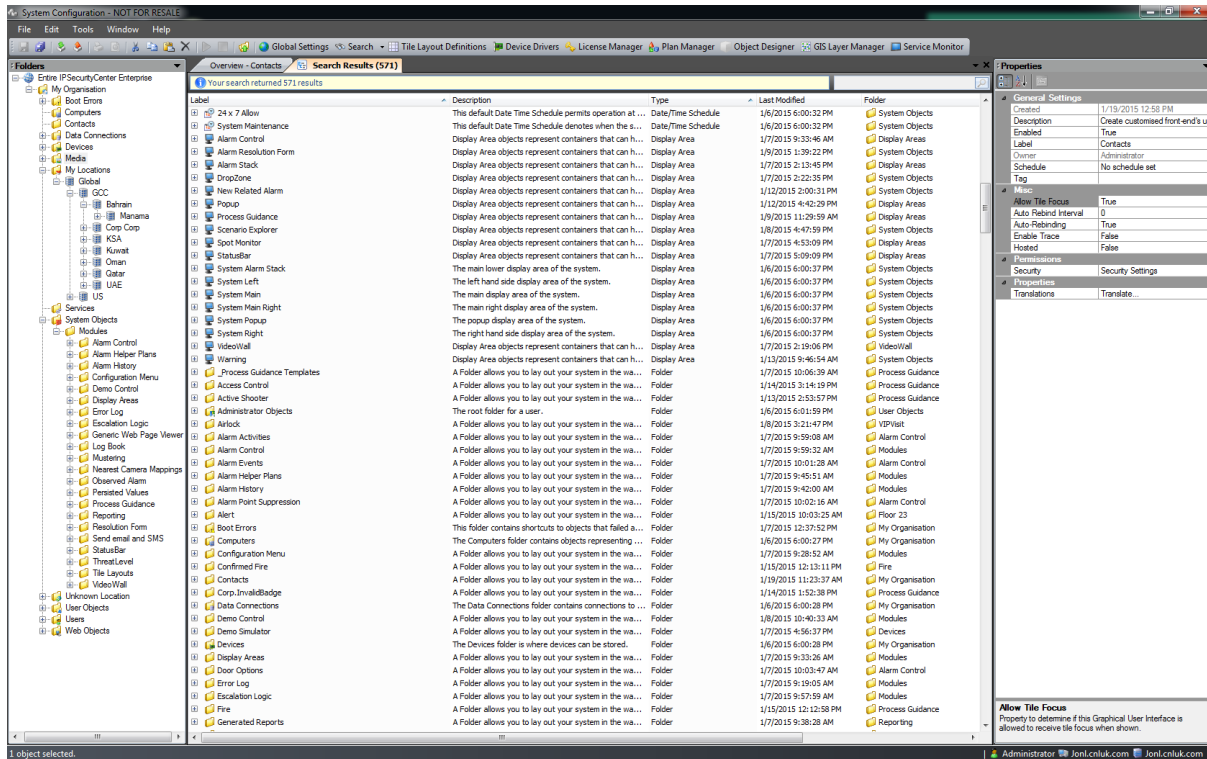
Upon completing step 7 above, the user interface will return to the location from the Search Objects window. If the search is performed from the toolbar button or context menu in System Configuration, then the system will navigate to show the selected object. If the Search Objects window was invoked from an editor for example, from a VRP shape or GUI control, then the search results will be returned to the editor. The property being specified will determine if one or many results are selected.

List Search Results

The System Configuration window also allows for a search of objects shown as a list within the Overview Tab. This is the default option when the Search button is clicked.



The search procedure is the same as with Find Object however when running the search then the results will show in a new tab in the background.

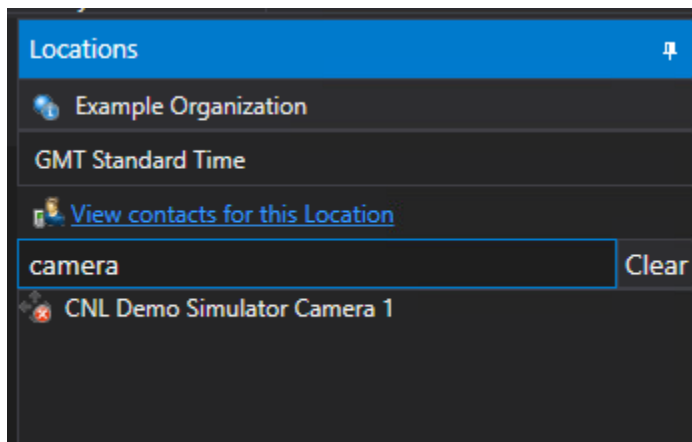


The Search Objects dialog can then be closed and the objects in the list of results can be interacted with, such as open a designer, set properties, etc.

This is particularly useful when setting properties on many objects distributed across many folders.

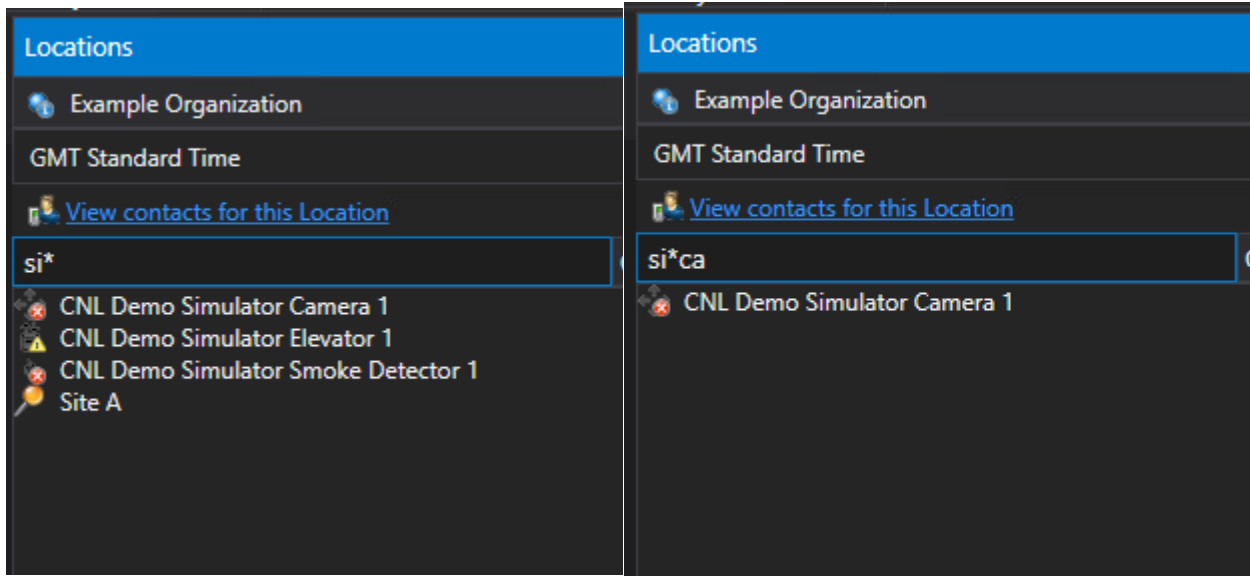
System Explorer Wildcard Support

The System Explorer Search bar supports search using Wildcard terms such as *, ? and #.

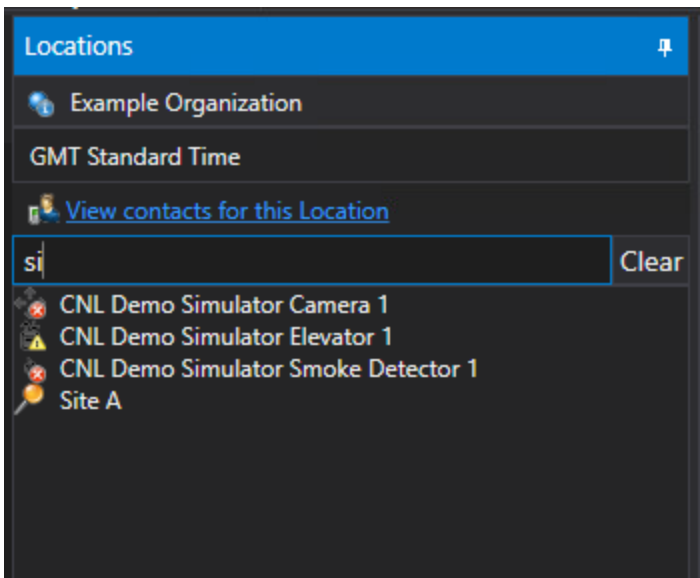


For example, in the search box the * character can be used as a wildcard so that 'Cam*ra' returns all strings containing 'Cam' and 'ra'. The wildcard '*' also matches zero or more

non-space and space characters so that, for instance 'Cam*ra' returns both 'camra' and 'cam Agra'.



Search is case insensitive, for example, searching for 'CAMERA' will match 'CaMeRa'. Search automatically includes a wildcard search for the beginning and ending of search phrases, therefore searching for 'amer' will match 'camera' and 'America'.



When the label for an object includes the character '*' this shall be found when the user enters the '*' character. For example, searching for 'camera *' will return 'camera 1' as well as 'camera *1'.

The wildcard character '?' matches one instance of a character so that the search string 'ca?era' matches 'camera' and 'canera' but not 'cammera'.

The wildcard character '#' matches any numeric character (0..9) so that the search string 'camera #' matches 'camera 1' and 'camera 8' but not 'camera b'.

Spaces at the beginning and end of search strings are excluded in the search so that the search string ' camera ' returns the same results as the search string 'camera'.

Search Shape in Response Plans

Use the Search shape to populate a target variable with objects in the system based on the specified search criteria. The type of object to search for is based on the type of the target variable. In addition to the target variable to populate with the results, the shape also requires a search value by which to search, an operator, and the property to search. The operator provides a multiple choice of different operators which includes 'equals', 'less than', 'greater than', 'starts with', 'contains', and so on. The available properties to select from are determined by the type of the target variable. For example, specifying a location variable as the target variable results in the property to search including items such as 'label', 'address 1', 'address 2', 'location ID', and so on.

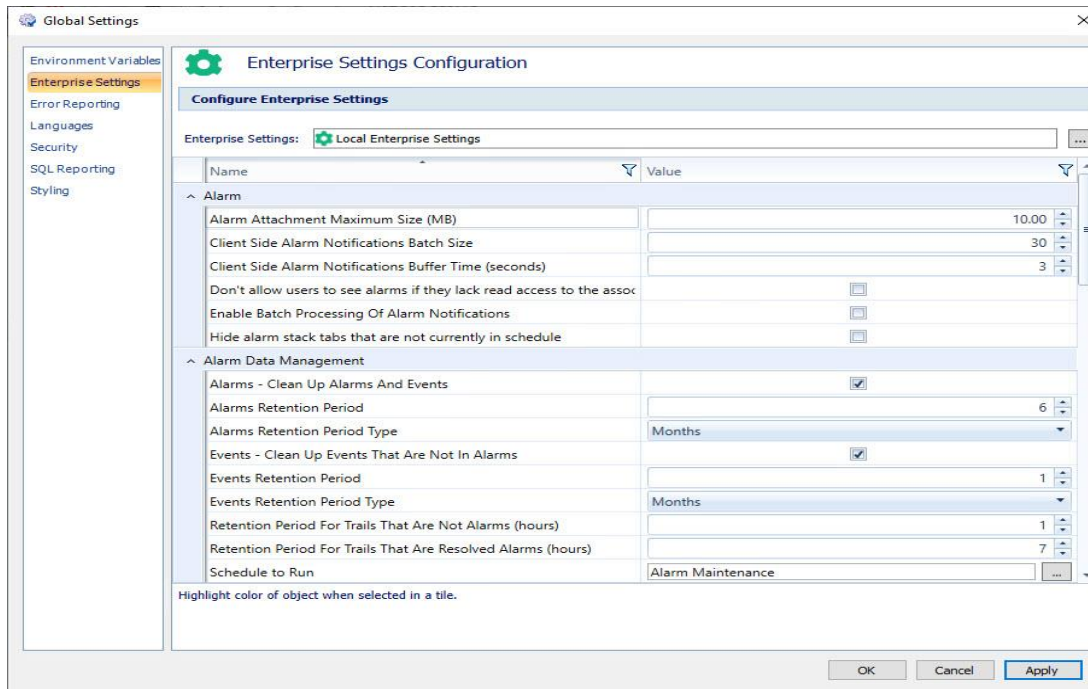
To search objects across Control Center, including federated objects from a VRP, such as Contacts across all Federated systems, you can specify the properties Remote Federation Service and Search Only Local Site that are specific to searching across Federated systems.

Optional	
Include Child Folders	False
Remote Federation Serv	Remote Federated Service
Search Folder	
Search Only Local Site	True
Required	
Case Sensitive Search	True
Property to Search	Unspecified
Search Operator	Equals
Search Value	
Target Variable	

If multiple results are returned by the search and a list variable has not been specified as the target, then the first item in the set of results will be used to populate the target variable.

Enterprise Settings

Enterprise Settings contain settings that are global to federated sites. The settings can be configured centrally and published. The Enterprise Settings used at each site can be configured in the Enterprise Settings tab in Global Settings.



Batch Processing of Alarm Notifications

Clients have to orderly and repetitively fetch notifications and other information related to alarms for all the alarms in the alarm stack. This results in the client reaching out to the server, back and forth several times, performing the same process, and increasing the network traffic. This might cause a lot of overhead on the already loaded network. To reduce this traffic and increase efficiency of processing the alarms, Control Center has incorporated an option in **Enterprise Settings** to reduce the network traffic by grouping the notifications to the server every 3 secs. This option is disabled by default. You need to enable it, if batching of alarm notification is to take place.

Sending Emails From Control Center

By configuring your Email Server settings in Global Settings, you can send outgoing emails with attachments from Control Center.

To do this:

1. Go to **System Configuration**.
2. From the tool bar, select **Global Settings**. The **Global Settings** dialog displays.
3. Select **Enterprise Settings**.
4. Enter your **Email Sending Preferences** as follows:
 - **Username**. The username of the Control Center Email account that you want to use to send emails.

- **Password.** The password of the Control Center Email account.
- **Friendly Name.** The display name of the Control Center Email account.
- **Email Address.** The unique address of your Control Center Email account.
- **Attachment File Size Limit (MB)** – set the file size limit for email attachments. The attachment file size limit should be the same as your company’s attachment file size limit. If this option is not set, then the attachment file size is unlimited.

This property only applies to video clips.

If you do have an attachment file size limit on your Email server and you do not set the **Attachment File Size Limit (MB)** option, and you try to export a video job whose attachment file size exceeds the limit on your Email server, then, even if you select the **Send via Email** checkbox, and the status of the job is **Successful**, the email is not sent. If you check the **Additional Information** column for your export job, a **See tasks for more warnings** message is displayed. If you double-click this, a **Could not attach to email (exceeded maximum attachment size)** error is displayed for your job.

5. Enter your Email server details as follows:

- **Server address** – Enter the machine name or IP address of your Email server.
- **SMTP Port** – Enter the port number used by your Email server. The default is 25.
- **Authenticate** – Select this checkbox if you want the email recipient’s username to be authenticated with Email server.
- **Using SSL** – Select this checkbox if you are using SSL to encrypt your email messages.

Dynamic Permissions

The Dynamic Permissions functionality enables users to view session permission / group membership changes implemented instantly without having to restart the Windows Client. For example, when you move around users into different groups, you can manage which locations, scenes, devices and alarms are visible to those users without having to restart the client each time you make such changes.

An ideal scenario is when an organization is required to split permissions to multiple levels, whereby the local team is responsible for security of a set of locations and devices, and the global team is responsible for a wider security of assets. As the global team may not have access to or visibility of any of the assets owned by the local team, the local team must manually provide the global team to have access to the locations, devices, scenes, alarms and so on. This can be repetitive for the local teams that have defined rules and times of day as to when such delegations should occur. In addition, the

global users must log off and log back in to acquire the new group membership and therefore the new access rights for the user.

However, with the Dynamic Permissions feature, any session membership changes made in the Client are effective in real time within a countdown of 20 seconds. That is, you can see the permission changes almost instantly. A notification is displayed informing you to acknowledge after which the UI is updated to ensure that the content visible complies with the changes made to group membership.

The Dynamic Permission update only considers membership of Control Center Groups and does not support changes to group membership made in Active Directory or other external system.

The following areas in the user interface will be refreshed automatically after a group membership change takes place:

- Alarm Stack
- Administration Interface
- Currently displayed cameras
- Current GUIs that are user session aware
- Current location and Scenes
- Cameras
- Drop zone controls
- Operator Actions
- System Configuration
- Video Wall displays

The following items are not automatically updated and require commissioning involvement to affect the refresh:

- Currently displayed GUI's that do not get impacted by user permission changes.
- VideoWall displays where the lease was not owned by a user when the membership change occurred.

Configuring User Permissions

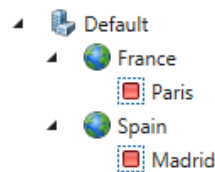
Before making user permission changes, first define locations, sub locations, users, and user groups. Make sure to set up at least two machines with Windows Client. User permissions can be configured in one of the following ways:

- Via Admin Interface
- Via System Configuration (Users and Groups area)

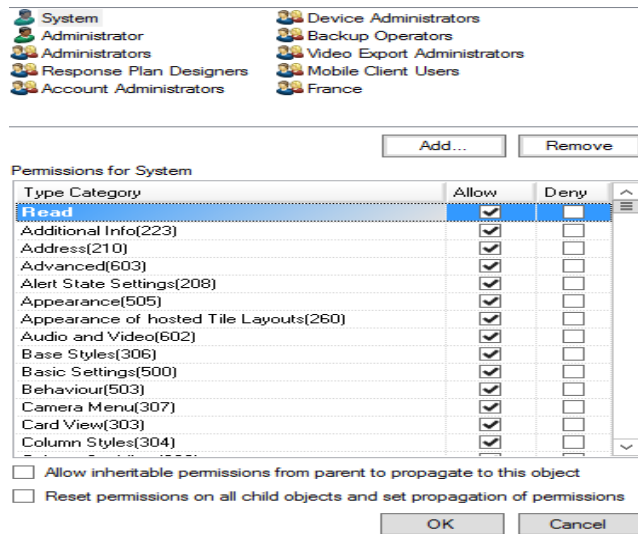
In this this example, user permissions are configured via System Configuration.

To configure user permissions:

1. From **System Configuration > My Locations**, create two main locations: **France** and **Spain** and create two sub-locations for each of the main locations: **Paris & Madrid**. For example:



2. Associate each of the locations and sub-locations with appropriate scenes.
3. Plot devices into each of the scenes as required.
4. Create two users specific to locations created above: **France** user and **Spain** user. Users are created.
5. Create two user Groups: **French** Group and **Spanish** Group.
6. Add two groups in the following way:
 - a. Right-click **System Configuration** and select **New > Group**.
 - b. Rename it, for example **France** Group. Create another group, for example, **Spanish** Group in the same way. Both groups are created.
7. Provide users with the permissions to see their respective groups. For example, make sure the Spain user is a member of Spanish group only and France user is a member of France only. To do this, follow these steps:
 - a. With the **France** location selected, in the **Properties** pane, click **Security Settings**.
 - b. Select the **Users** group and click **Remove**. The **Users** group is removed from the **France** location. Navigate to the **France** location and remove the **Users** group from the **Security Permissions**. The **Users** group is removed.
 - c. Click **Security Settings** again and then click **Add** to assign the **French** User group to the **France** location.



- d. Follow the same steps for removing the **Users** group from **Spain** location and adding the location to the **Spanish** group.
8. Log in to the second client as the French user with appropriate credentials.
9. From the **System Explorer** tree, only locations and devices related to France should be displayed. The Spain related locations and devices are not displayed.
10. Now, log off from the second client and log in as a **Spain** user.
11. View the **System Explorer** tree. Only the locations and devices related to Spain are displayed. The locations and devices related to France are not displayed.
12. Now log in to the first client as the regular root user and view the **System Explorer** tree. All the locations and devices are displayed in **System Explorer**, for example both France and Spain should appear.

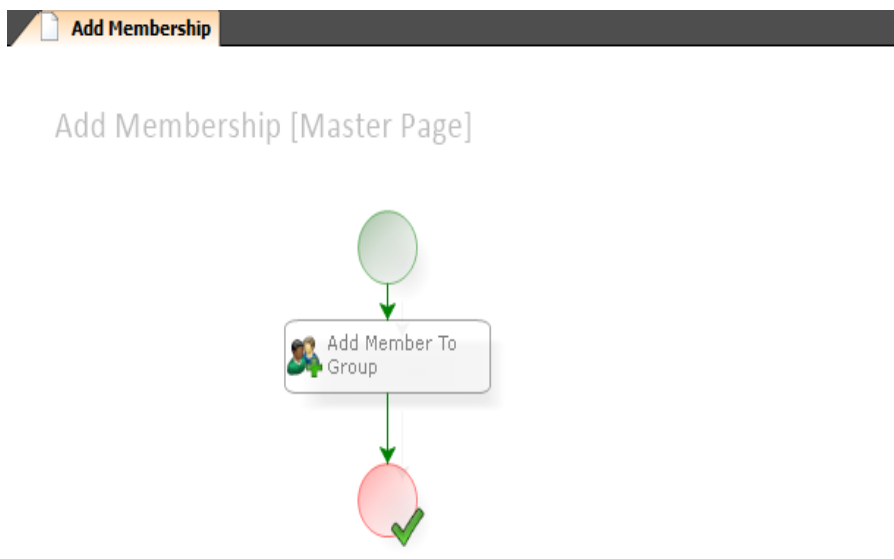
Moving Users to Another Group

Moving users from one group to the other displays a notification message.

To move users from one group to the other:

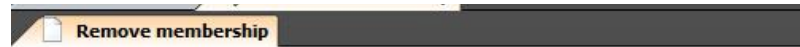
1. In **System Configuration**, create 2 response plans and name them as follows:
 - o **Add Membership**
 - o **Remove Membership**
2. Create **Add Membership** response plan:
 - a. Right-click anywhere on the **Overview** pane and select **New > Response Plan**.
 - b. In the designer, select the **Add Member to Group** shape and edit the following properties:

- **Member To Add** – Select the user that you want to add to the group selected above, for example, Spain User.
 - **Group To Add To** – Select the group that you want to add membership to, for example, France.
 - **Session Membership Changed** – Enter the message description that will be displayed to the logged in user when their session membership changes
- c. From **System Shapes**, drag and drop the **Add Member To Group** shape on the designer area.
 - d. Double-click the **Add Membership** response plan to edit it.
 - e. Rename it to **Add Membership**.

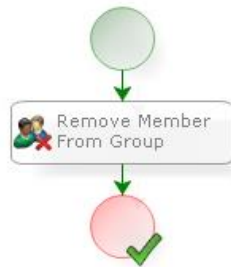


3. Create **Remove Membership** response plan:
 - a. Right-click anywhere on the **Overview** pane and select **New > Response Plan**.
 - b. Rename it to **Remove Membership**.
 - c. Double-click the **Remove Membership** response plan to edit it.
 - d. From **System** shapes, drag and drop the **Remove Member To Group** shape on the designer area.
 - e. In the designer, select the **Remove Member to Group** shape and edit the following properties:
 - **Session Membership Changed Description** – Enter the message description that will be displayed to the logged in user when their session membership changes.

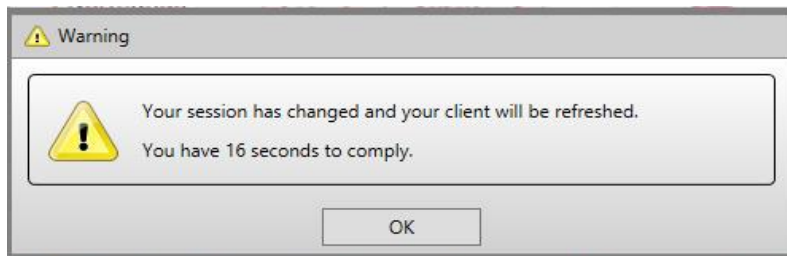
- **Group To Remove From** – Select the group you want to remove the membership of, for example, France.
- **Member To Remove** – Select the member you want to remove from the above selected group, for example, Spain User.



Remove membership [Master Page]



4. Run one of the response plans. A message displaying the time count is displayed in the Warning message window. Click **OK** or wait for 20 seconds. The window disappears, and the changes take effect.



5. View the System Explorer tree to verify if the Control Center Client is refreshed. The France Location is removed from System Explorer tree.
6. Search for the France locations or devices in System Explorer tree. The System Explorer shows **No Records available** error message and the map area will show the following message:



Error you don't have read permissions to view the scene

7. The interface refresh will remove visibility of all or any of the following areas depending on the user permissions:

- Alarms Stack – Will be refreshed to only alarms that the user has permissions to are displayed.
- Alert State – Only alerts that are part of the alarms that the user has permissions to are displayed.
- Tile Layouts – If a user session change affects the tile that a camera is displayed on, then the tile will be refreshed with an error message indicating that the user can no longer view the video from the device due to permission change.

Customizing the Notification Message

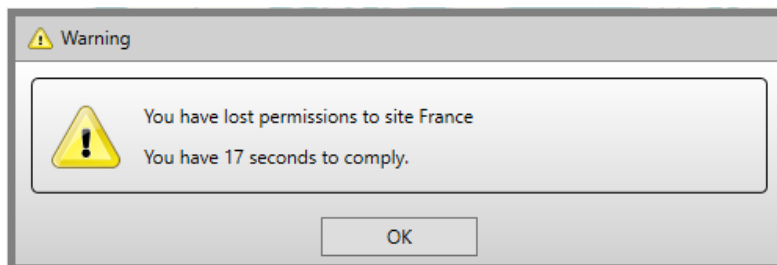
You can customize the text in the notification message to display specific messages. For example, when removing permission for a user to access a certain group, you can customize the notification message to **You have lost permissions to see France**.

To customize the text in the notification message:

1. Open the Remove Membership response plan and navigate to the **Properties** pane.
2. In the **Session Membership Changed Description** field, enter a notification message, for example, type the following text:

You have lost permissions to site France.

3. Run the response plan. A warning message appears with the customized message.



Session Changed Events on Server Devices

The Session Changed event is raised when a user session is changed as a result of a group membership change within System Configuration, Admin Interface, or Response Plan shapes. To raise a session changed event:

1. From the **System Configuration > Computers** folder, expand the **Server** object and then the **Events** folder.
2. Right-click the **Session Changed** event and select **React to Event > Run Response Plan > Create New Plan**. A trigger and a response plan are created for the **Session Changed** event.
3. Rename the response plan, for example, Session Changed.

4. Open the response plan and configure the following:
 - a. From **ActionShapes**, drag and drop the **Dynamic Action** shape.
 - b. Click **Next** until the **Target Object** page and select the target as your computer name.
 - c. On the **Actions** page, click the **Message Box** field and select **Static Value**.
 - d. Type the message **Permissions have been changed**.
 - e. Add a **Finish** shape.
 - f. Save and close the Session Changed response plan.
5. Log in to the Windows Client as another user that has permissions to both locations France and Spain, for example CNL User.
6. From the **System Configuration**, select **Users > CNL user** and in **Properties**, click **Member** of to view the groups, the CNL User is a member of.
7. Select a group and click **Remove** to remove to make the membership changes. A Warning message window displaying the time count appears. Click **OK** or wait for 20 seconds to continue. Meanwhile, on the main client where the **Session Changed** event was triggered, a **Permissions have been changed** notification message is also displayed.

Managing Alarms

Managing alarms is a central feature of Control Center. It allows you to view prioritized alarms and manage these by executing related workflows. An alarm can be manually created or be created as a result of specific data being received from sub-systems or other objects. While managing alarms, users can access related resources such as intercom and CCTV, execute Process Guidance, use maps, generate reports and so on.

Alarms definitions are stored in Alarm Types. An Alarm Type defines what should create an alarm, its title, description, priority, linked workflow and so on.

Alarm Types comprises a wide range of functionality spanning the entire alarm handling process, from processing events and maintaining an alarm stack to resolving an alarm and generating a report.

It allows the user of Control Center to easily define what a new alarm is and what should happen when the alarm is activated and handled by an operator.

Alarm Concepts

The following table describes the key concepts that make up alarm management.

Concept	Description
Alarm	An Alarm is an instance of an Alarm Type that either requires action or has been handled and resolved. An Alarm has a unique identifier, a title, a description and a priority. It can be visible to user sin the Alarm Stack and be linked to a workflow. It can also be linked to a specific device or Alarm Point.
Alarm Handling Group	A definition of the conditions in which a specific user or user group can handle and resolve a type of alarm.
Alarm Point	An object (for example,. Federated Server), Device (for example, Door) or a placeholder.
Alarm Stack	This is the user interface for operators that displays a list of Alarms.
Alarm Stack View	This is a set of configurations for the Alarm Stack that filters what Alarms are visible. There can be multiple Alarm Stack Views in the system, and they can be configured so that not every user can see every Alarm Stack View. In addition, the Alarm Stack View keeps the selected alarm row highlighted when scrolling through other alarms to enable interpretation of alarm values.

Alarm Type	An Alarm Type is a list of rules that determine whether an Alarm is created. Two different categories of Alarm Types exist, Classic Alarm Type and Correlated Alarm Types.
Alert / Alert State	The visual formatting applied to an asset on a map or in the System tree as a result of an Alarm or a manual Alert activation
Classic Alarm Type	Classic Alarm Types operate on a single event as it comes into the Rules engine
Correlated Alarm Type	Correlated Alarm Types operate on one or multiple events. They provide the ability to define alarms that should only occur if several events appear within a specified time and geographical area or if specific events do not occur within a specified period of time.
Collation	Collation groups alarm based on the collation options. Collation occurs once all event matching has occurred and the Rules Engine has created an alarm. The collation rules are used to look for an existing alarm, and if one is found then the events that would make the new alarm will instead be attached to the existing alarm. Both Classic and Correlated Alarm Types support collation.
Event	A single notification from a device or other Control Center objects. The property types on the event are fixed, but the values of those properties are determined at run time. They will be stored in the database and processed against Alarm Types unless they are filtered out in the Connection Manager Event Viewer.
Rules Engine	The Rules Engine is one of the Control Center Windows services. It uses MSMQ to receive events, writes those events into the Pacific database and processes Alarm Types, Correlated Alarm Types, Alarm Type Modifiers, and Triggers. It uses SQL Service Broker and the Notification Service to communicate back to the Core service.
Service Level Agreements	Service Levels can be configured directly in the Alarm Types editor to determine duration and formatting options for all alarms in the system. Up to three service levels can be configured to update the icon, foreground color, background color and font of an alarm in

	the Alarm Stack or play an audio alert after the alarm is enacted. A VRP can also be executed for each service level to facilitate advanced actions for the service level breach. An activity is automatically logged against the alarm when each service level is breached.
--	--

Alarms in the End-User Interface

The following table describes how alarms are displayed in the end user interface.

Name	Description
The Alarm Stack	The alarm stack is a user interface component that provides a view on alarms. A system can have any number of alarm stacks. An alarm stack can have one or more Views on alarms. When you install Control Center , a default System Alarm Stack is created.
System Alarm Stack	The System Alarm Stack provides a single point in the system to configure the event handling and alarm creation logic for Alarm Types. This includes a wizard for creating and editing Alarm Types, a wizard for creating and editing Alarm Stack Views, and editors for managing Activity Types, Resolution Types, and Service Levels. The System Alarm Stack is a stack of Alarms and Views held in the system.

Raising a Manual Alarm

From within a map, you can now right-click:

- an area of a map. This applies to Geographic scenes only.
- an object. This applies to both Geographic and Schematic scenes.

and quickly and easily raise a manual alarm for that map area or device. This is useful because it enables you to respond immediately to events that you can see on your map.

Raising manual alarms depends on your alarm permissions. See [Type Permissions](#).

You can raise more than one manual alarm on object.

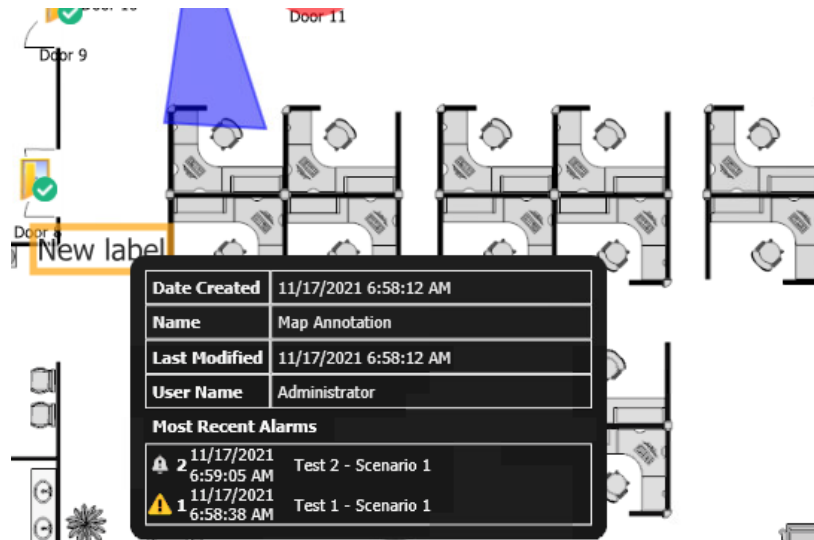
When raising manual alarms on a specific area of a geographic scene, you only raise one manual alarm. In other words, you cannot raise two manual alarms on the same co-ordinates.

When a manual alarm is raised on a device then the device becomes the alarm point and the device's location becomes the location for the alarm.

Once you have raised a manual alarm you can handle it:

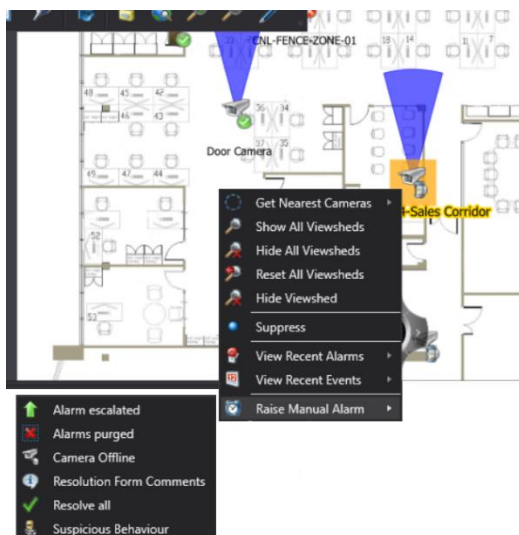
- from your alarm stack view, or,
- if you have any defined, by process guidance, or
- by right-clicking and selecting **Handle Alarm**.

You can also link a manual alarm to a map annotation. If you link an alarm to a map annotation, the information is displayed in the map annotation's tooltip. A maximum of 3 alarms are displayed. See [Linking Alarms to Map Annotations](#).



To raise a manual alarm:

1. Go to **System Explorer** from the **Main** screen.
2. Find the device on your map.
3. Right click the device and select **Raise Manual Alarm**.



4. A list of manual alarm types is displayed.

5. Select the alarm type you want. The **Raise Alarm** dialog displays.
6. Select the alarm type you want and, optionally, add a description. Select **OK**. If you are raising a manual alarm on an area of a geographic map, the icon associated with the alarm type is displayed. If you are raising a manual alarm on a device that has an alert state configured, the manual alarm displays with the configured alarm state, as shown below.



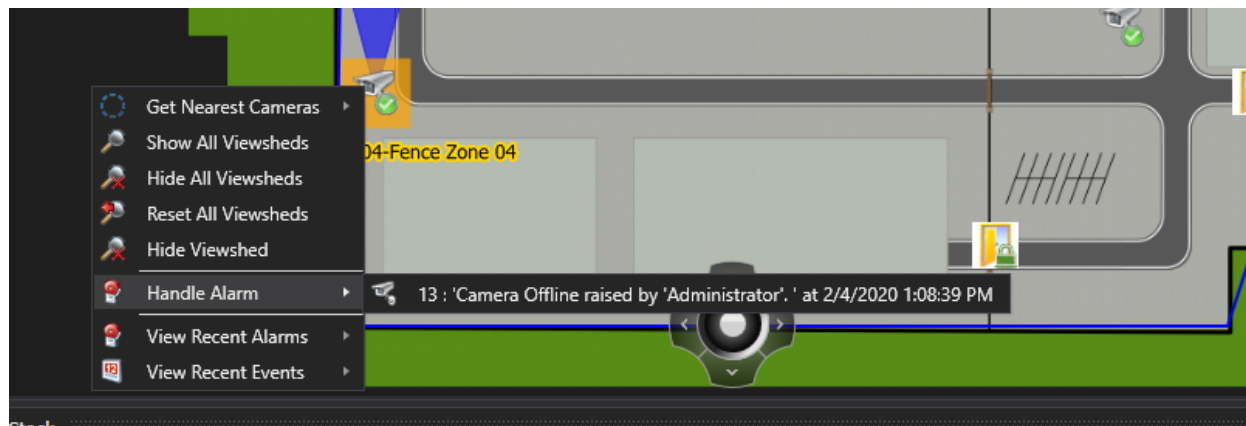
7. You can now handle the alarm in the normal way, for example, by right clicking the device and selecting **Handle Alarm**, from your alarm stack or process guidance window.

Handling an Alarm

In Control Center, alarms can be set for objects, for example, devices, non-devices, shortcuts, asset geofences and hot zones.

You can handle alarms, either from the Alarm Stack or by right-clicking one of the above and selecting **Handle Alarm**. Depending on the Control Center object whose alarms you want to view, you can do this:

- In System Explorer
- From a map, both scenic and geographic, or map annotation
- In System Configuration



Select an alarm to handle it. Depending on how you have configured Control Center, your **Process Guidance** window or another response plan displays, so you can see that your alarm has been handled.

If a Control Center object has more than 10 alarms, the **Handle Alarms** dialog displays. Select an alarm to enable the **Handle Alarm** button. Select the **Handle Alarm** button to display the **Process Guidance** window.

you must have permission to handle an alarm.

Adding Alarm Attachments

Depending on how your Administrator has configured Control Center, you can add attachments when raising and handling alarms. (See [Configuring Alarm Attachments](#) for more information). This is useful for after-action reporting, or when handing over alarm responsibilities to an operator other than yourself. Attachments allow additional information associated with the alarm to be immediately available. For example, you may want to attach a snapshot from a video camera or a file from another system.

You can attach any file type, for example, PDF, Video, Audio and so on.

You must have type permissions to be able to add and view alarm attachments. See [Type Permissions](#) for more information.

In federated Control Center:

- Any alarms and attachments that are created on the local site are automatically federated to the NOC.
- If you want to link media objects to a remote alarm, you must make sure the media originates on the same site as the alarm.

Adding Attachments When Raising Alarms

You can only do this if your Control Center Administrator has configured Control Center to display an alarm attachment display area when raising alarms.

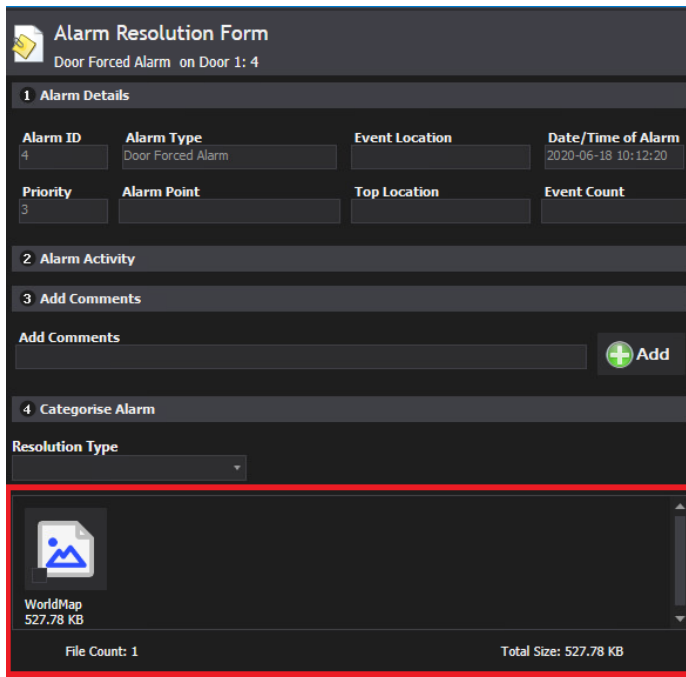
You can add an attachment when raising an alarm.

1. Raise an alarm, for example, by right-clicking an asset on a map and select **Raise Manual Alarm**.
2. Go to the alarm attachment display area.
3. Either:
 - Drag your media from Control Center **System Explorer** to the alarm attachment display area.
 - Browse to the location of the external file and drag the file to the alarm attachment display area.
 - Select **Add** and browse to the location of the external file.

Adding Attachments when Handling Alarms

You can use the Alarm Resolution Form (if you have Process Guidance or an Alarm Resolution Form configured in Control Center) to add attachments when handling an alarm.

1. Handle your alarm, for example, by right-clicking an asset on your map and selecting **Handle Alarm** or by double-clicking an alarm in your **Alarm Stack**.
2. From the **Alarm Resolution Form**, browse to the alarm attachment display area.
3. From the alarm attachment display area, you can:
 - Add attachments by:
 - Dragging your media from Control Center **System Explorer** to the alarm attachment display area.
 - Browse to the location of the external file and drag the file to the alarm attachment display area.

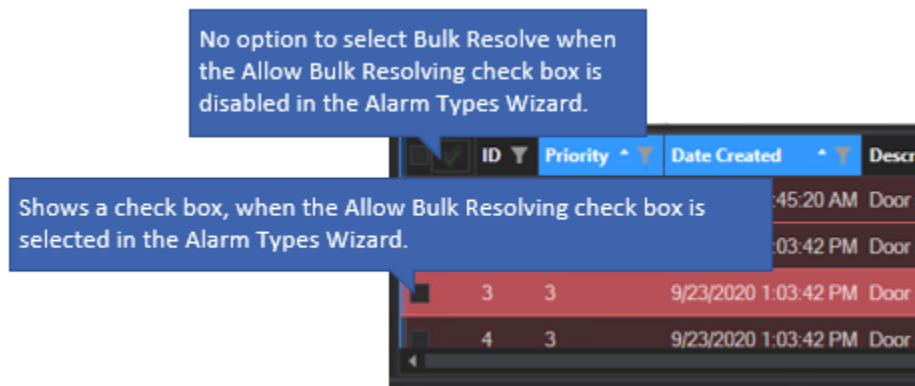


- Select **Add** and browse to the location of the external file.
 - Select an attachment and select **Open** to view an attachment.
 - Select an attachment and select **Save** to save the attachment to your local computer.
 - Select an attachment and select **Delete** to delete the attachment.

Bulk Resolving Alarms

You can bulk resolve alarms. To do this:

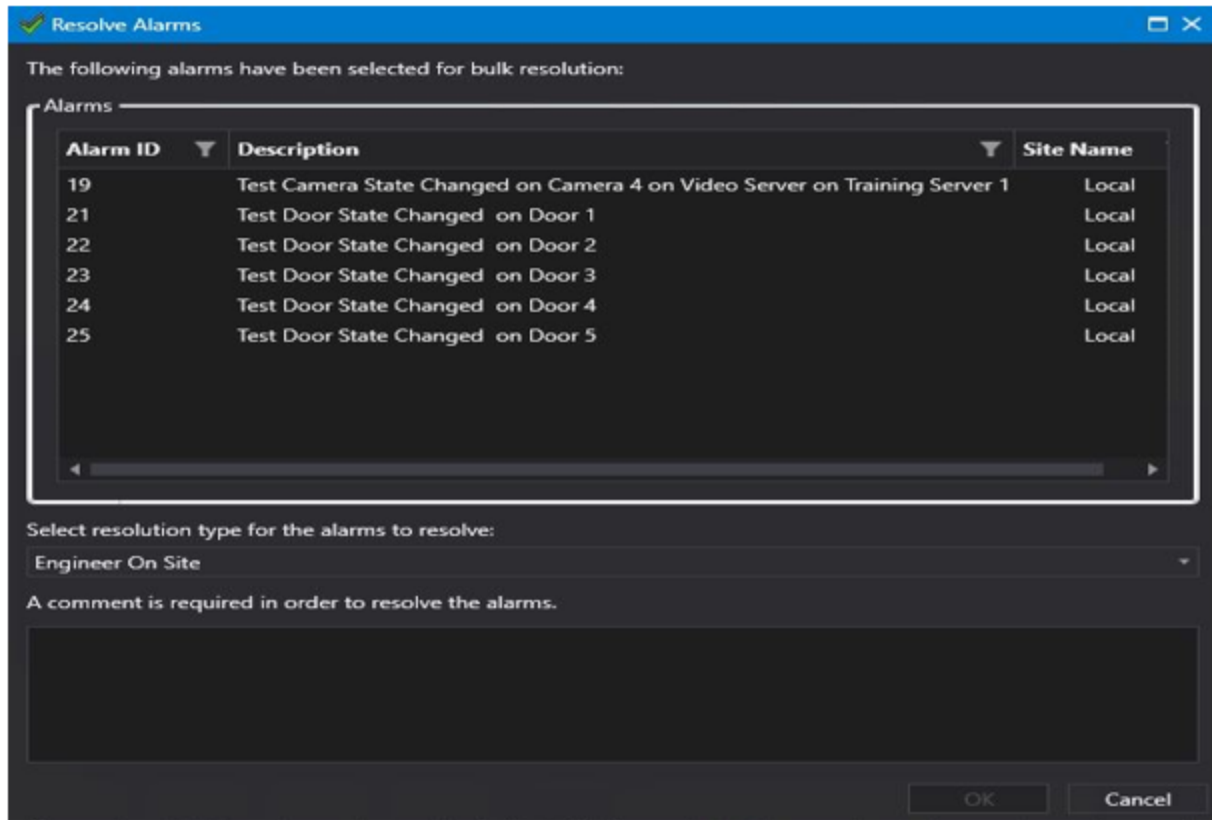
1. From the **Alarm Stack View**, view the alarms that are displayed. Notice the check box that appears in front of the alarms in the **Alarm Stack view** for the alarms that have the **Allow Bulk Resolving** option selected in the **Alarm Types** wizard.



2. Select the alarms you want to bulk resolve. You could select one, more or all of them to be resolved.
3. Click on the green tick on the left corner of the **Alarm Stack** toolbar. The **Resolve Alarms** window opens up. A list of all the selected alarms to be resolved is displayed.



4. Choose the resolution type for the alarms from the drop down menu and enter the comment as required.



The selected alarms are resolved.

Notes:

- On upgrading from an earlier version of the software, an administrator must enable the Allow Bulk resolution of Alarms security policy in addition to enabling it in Alarm Types and Alarm Stack views. By default, the Allow Bulk resolution of Alarms security policy does not have users and groups added.
- When working in a Federated environment, if the Hub site is upgraded to 5.6, and if the Bulk Resolve Capability is enabled, then the users can bulk handle alarms at the Hub site. However, if the Node site is not upgraded to 5.6, then the Bulk Resolution Capability is not available to the users for resolving the alarms coming from the Node site.

Filtering in Alarm Stack View

You can filter alarms in the alarm stack using the filter options by one or more columns to show multiple alarms of the same criteria or locate specific alarms from an otherwise long list of alarms.

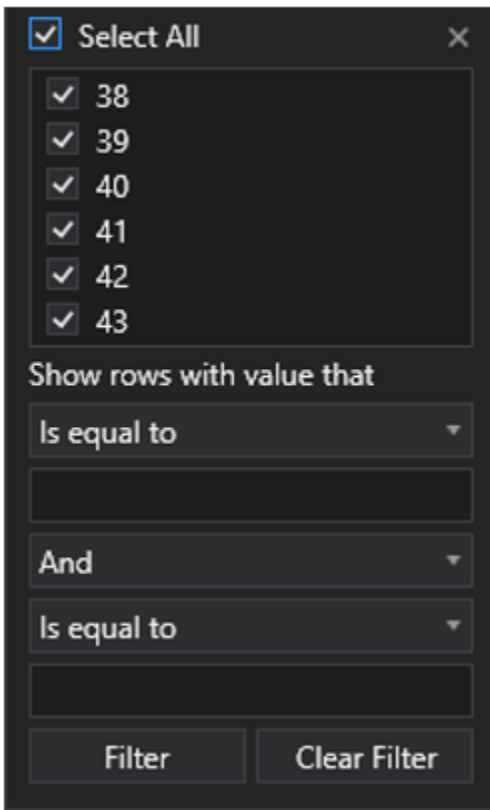
For example, you can filter the Alarm Stack to show any of the following:

- All alarms Training Server

- All priority 1 and 2 non-training server alarms where the service level is equal or greater than 2
- All priority 3 and 4

To filter alarms:

1. In the Alarm Stack View, click the funnel icon next to the column header whose alarms you wish to filter, for example, select ID. The following filter dialog displays.



2. Select a filter option, then type the required value based on the filter type and click Filter. The filter values are applied to the alarm stack view and only relevant items are displayed. The following filter options are available:

Filter Option	Applicable to:
<ul style="list-style-type: none"> ○ is equal to ○ is not equal to 	All filterable types
<ul style="list-style-type: none"> ○ Starts with ○ Ends with 	String

<ul style="list-style-type: none"> ○ Contains ○ Does not contain ○ Is contained in ○ Is not contained in ○ Is empty ○ Is not empty 	
<ul style="list-style-type: none"> ○ Is less than ○ Is less than or equal to ○ Is greater than ○ Is greater than or equal to 	Numeric types, DateTime, TimeSpan, and all types that use these operators
<ul style="list-style-type: none"> ○ Is null ○ Is not null 	All filterable nullable types

The funnel icon appears enable in the Alarm Stack View to indicate the filter is active. To clear the filter, select Clear Filter.

Pinning and Minimizing the Alarm Stack

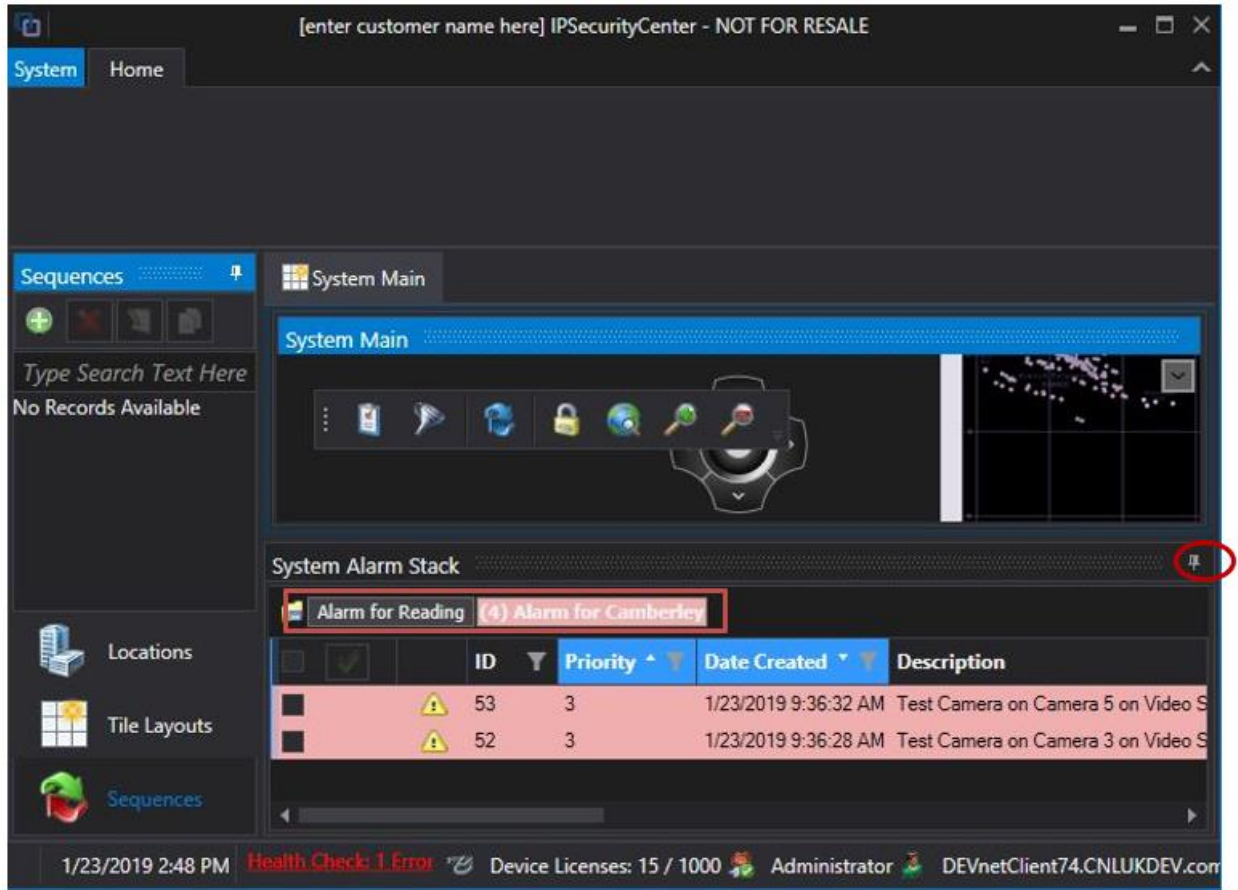
The System Alarm Stack display area is normally docked below the System Main window. If the alarm stack is allowed pinning, you will be able to minimize the Alarm Stack, either by clicking on the Pin on the top right corner of the window or by setting the **Is Pinned** property in the Setup Display window to **False**.

However, in minimized state, when a new alarm gets populated in the stack the title bar of the alarm stack starts to blink to alert you. You can choose to hover over the title bar to temporarily expand the window and view the alarms and then click anywhere on the application to collapse it.

If the window needs to be restored to its original state, you need to click on the title bar of the window and pin it.

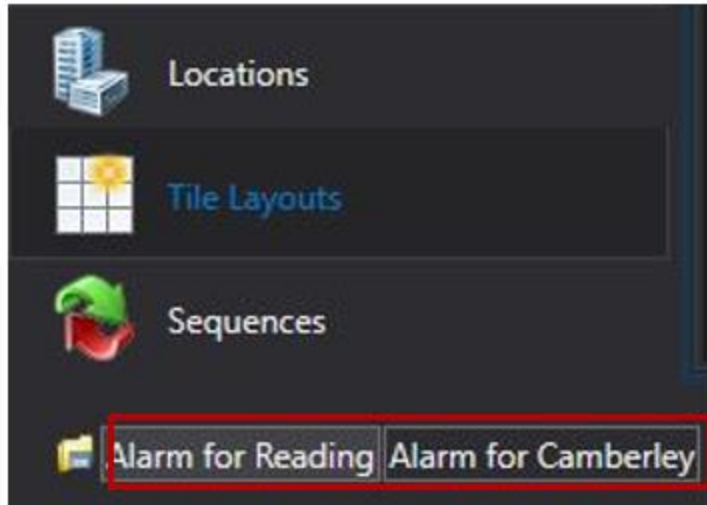
System Alarm Stack Pinned

When the alarm stack is pinned, it remains expanded and all the alarms generated can be viewed in the alarm stack. You could also represent locations in the form of tabs or combine one or more locations into a group to be displayed in the alarm stack. Only those alarms for the selected location/group will be displayed in the stack. If an alarm for the other location/group is generated, you are alerted by a flashing tab and the count of alarms displayed against it. The color of the tab can be selected while creating groups.

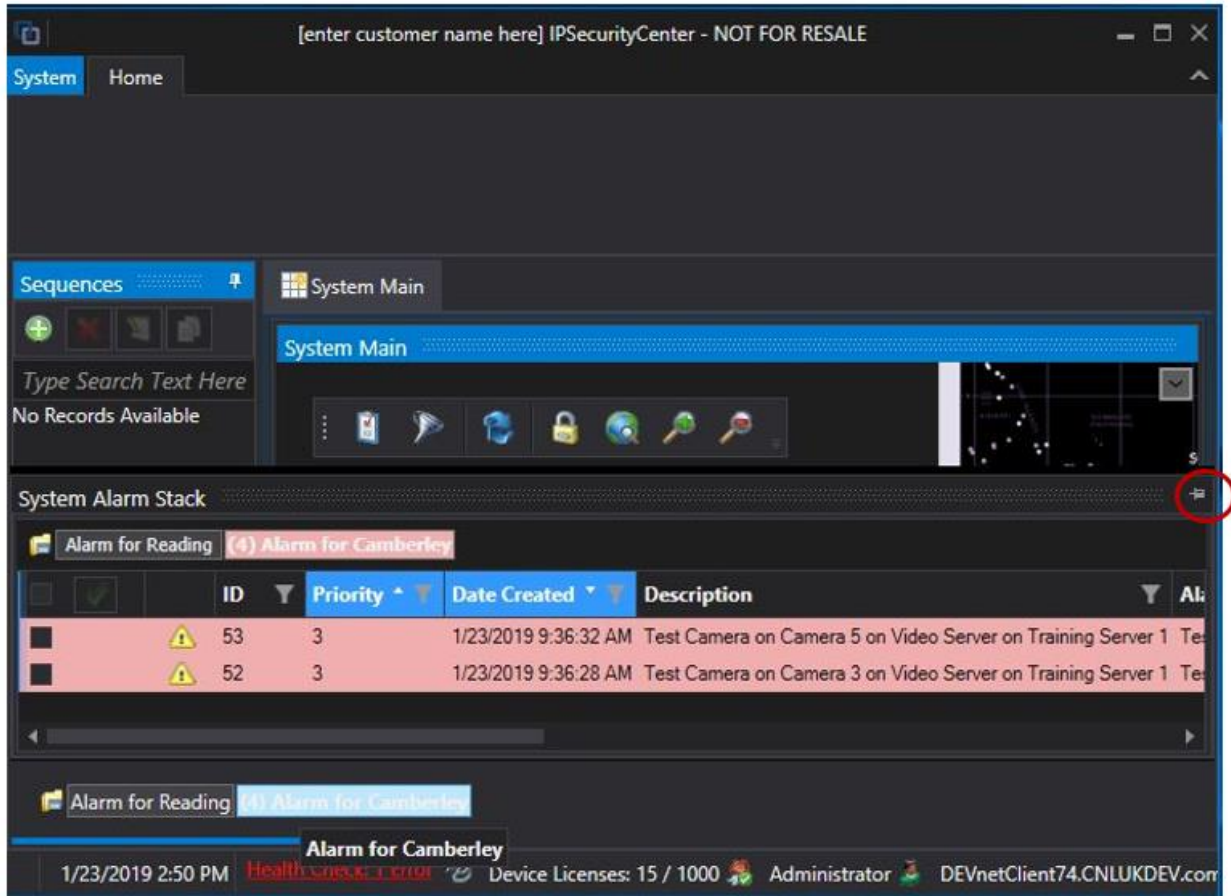


System Alarm Stack Minimized

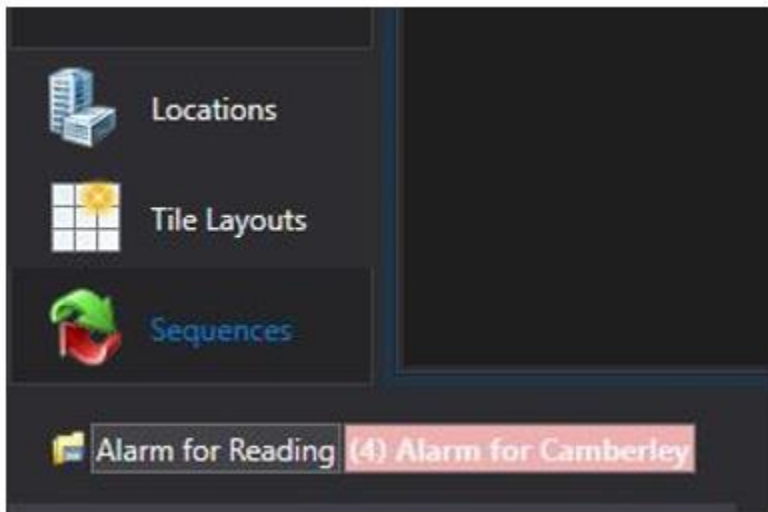
The system alarm stack can be minimized to a tab by clicking on the pin on the top right corner of the window or by setting the property **Is Pinned** to **False** in the System Display window. This is typically known as unpinning the window.



When an alarm arrives, you are notified of it with a flash on the tab. If working with groups, where one or more locations with a common criterion are grouped together, alarms arising from any of the location in the group causes the tab to flash to alert you. You can then hover the mouse to have a glimpse of the alarm stack or choose to pin it by clicking on the pin in the title bar.



In the minimized state, only the alarms generated for the group that isn't selected is made to flash. If you need to view the alarms for the selected group, then click on the group or the locations under it for viewing any specific alarm for it.



Viewing Alarm and Alerts in Maps and System Tree

An Alert State provides a way to define a visual indicator that can be used to draw your attention to something that requires action, for example an alarm, however, an Alert State can also be applied to an object without the existence of an alarm.

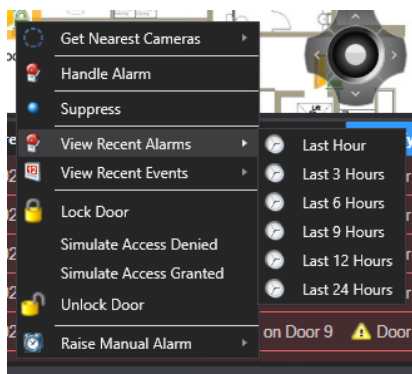
When an Alert State is applied to an object in the system, for example, location, device, or asset geometry, the Alert State visual preferences are applied to the System Tree and the currently visible Scene if the alerted object is visible. In addition, the parent location(s) of the object can also be set to show in alert. Only the alert state color is shown in the System Tree, not the blinking. When the alert on an object is cleared because an alarm has been resolved, the visual state of the object returns to normal.

Viewing Recent Alarms and Events for Devices

The System Explorer provides filtering options for viewing alarms and events based on when they occurred over the course of 24 hours. You can right-click on a device and filter by the most recent alarms and events that occurred in the last 24 hours.

To view alarms that occurred over the course of last 24 hours:

1. Go to **System Explorer** and right-click on a device for which you would like to view the recent alarms for. The following filtering options appear:



2. Click **View Recent Alarms** and select from the options to view by the required duration. The following summary page appears.

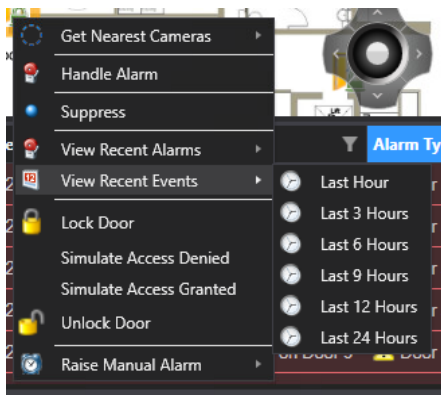
Recent Alarms for 'Door 27'										
From Date		To Date								
10/1/2020 5:43 AM		10/1/2020 2:43 PM								Refresh
ID	Priority	Date Created	Description	Alarm Point	Location	Status	Event Count	Resolving User	Resolution Type	Date Resolved
50	3	10/1/2020 2:37:09 PM	Door state changed on	Door 27	Example Organization	Unhandled	1			
49	3	10/1/2020 2:37:08 PM	Door state changed on	Door 27	Example Organization	Unhandled	1			
48	3	10/1/2020 2:37:06 PM	Door state changed on	Door 27	Example Organization	Unhandled	1			
47	3	10/1/2020 2:37:04 PM	Door state changed on	Door 27	Example Organization	Unhandled	1			
44	3	10/1/2020 2:35:51 PM	Door state changed on	Door 27		Unhandled	1			

3. Additional filter options appear on the **Summary** page to filter the alarms by the following options:
 - o From Date

- To Date
- ID
- Priority
- Date Created
- Description
- Event Count
- Resolving User
- Resolution Type
- Date Resolved

To view events that occurred over the course of last 24 hours:

1. Right-click on a device and click **View Recent Events** followed by the required duration.



2. Selecting the Last 24 hours option displays the following summary page.


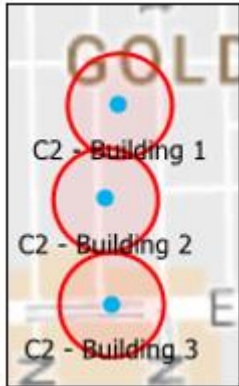
Received Date Time	Description	Alarm Point	Location	Event Count
10/1/2020 8:53:43 AM	Device State Changed	Door 7	Building 11	1
10/1/2020 8:53:43 AM	Custom State Changed	Door 7	Building 11	1
10/1/2020 8:53:42 AM	Device State Changed	Door 7	Building 11	1

3. Similar to **Alarms Summary** page, you can also filter events using the additional options on the **Events Summary** page.

Configuring Alert State Properties

The Alert State has the following properties:

Alert State	Description
-------------	-------------

Alert State Blink Rate	Allows control of the frequency at which the alert halo applied to the resource flashes. The value is the number of times per second that the halo flashes. When the value is set to 0, the halo appears without flashing. This only applies to the resource in the System Explorer tree. For backwards compatibility, the default for a new alert state is 1 per second.
Alert State Halo Radius	The Alert State Halo Radius can be set to small, medium or large. Medium is the default setting for new or upgraded Alert States. The radius of the large Alert State is twice that of a medium radius Alert State. The small Alert State is half the radius of the medium Alert State. 
Alert State Halo Transparency	Allows control of the transparency of the Alert State Halo that is applied to the resource. Valid values for this property are decimal between 0 and 1 where 0 is fully transparent and 1 is fully opaque. The default transparency is set at 0.6. Regardless of the value set for the transparency, the Alert Halo appears with a border that defines the edge of the Halo, for example. 
Color	The color used to indicate that the resource is in this alert state. The icon for the resource on the map is surrounded by a halo of the selected color for the duration of the alert. Also, if the

	resource appears in the System Explorer, that row is also highlighted in the selected color.
Duration	The duration in seconds for which a resource remains in the alerted state. When this value is set to 0, the resource being alerted remains in alert until the alert state is cleared.
Icon	The icon that is associated with the selected alert state. The icon for the resource changes to this icon for the duration of the alert. You can choose not to set an icon for an alert.
Parents to Alert	Determines whether parent locations are alerted when the resource is put into alert. This property enables the choice of parent location types to alert when this Alert State is applied to an object. Parents are evaluated by examining the location that is the immediate parent of the object being alerted, and the immediate parent of that location and so on until the entire list of parents is established. Locations in the list of parents with the selected location type also have the alert state applied to them. When the Alert State is cleared from the resource, all parent locations that were alerted also have the Alert State removed.
Priority	Enables association of a numeric priority to an alert state. A location may contain many devices and is therefore subjected to multiple simultaneous Alert States. When multiple Alert States are applied to an object only, then the highest Priority Alert State is shown. Valid values for this property are positive integers only. Therefore Priority 1 is the highest priority you can set.
Text	The text associated with the selected alert state. This text is pre-pended to the existing label text for the duration of the alert.

Alarm Alert Filtering on Maps

The alarm alert filter enables you to suppress the required alarm alerts that appear on the map based on the selected filter conditions, for example, to declutter the map halos on the global map. You can also apply a filter to show only alarm alerts that are displayed in the alarm stack for a selected site or display alerts based on its priority value. The alarm alerts that appear on the map may change based on the location selected in System Explorer if the Alarm Stack view has been set up to use location-based filtering.

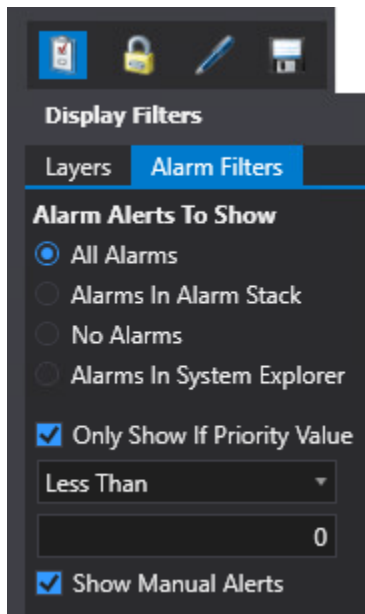
This is particularly useful when viewing maps on systems that are being federated to avoid a cluttered view especially when displaying large size alerts on the global map.

Before configuring the alarm alert filter, ensure you have configured the following options:

- A Schematic or Geographic scene that is associated with a location.
- Create an alarm type and configure it to Locations and Devices.
- Configure the alert state via the Alarm Types Wizard.

To filter alerts associated with alarms on the map:

1. From the **Map** area, click  and select Alarm Filters.



2. Select from the following **Alerts to Show** filter options to filter the visible alarms in the Alarms Stack:
 - **All Alarms** – Displays all the existing alarm alerts on the map. Use this setting to also remove the existing filter except when one of the check boxes remains checked.
 - **Alarms in Alarm Stack** – Displays all alarms in the Alarm Stack.
 - **No Alarms** – Hides all alerts from the map. Note: This setting does not take effect on manual alerts.
 - **Alarms in System Explorer** – Displays alerts from the System Explorer.
 - **Only Show if Priority Value** – Select this option followed by one of the conditions from the drop-down, and then specify the priority value to

determine what alerts should be displayed on the map area. The following conditions are available in the drop-down:

- **LessThan** – The priority value of the current alerts should be less than the value specified here for the alerts to be displayed.
- **LessThanOrEquals** – The priority value of the current alerts should be less than or at least equal to the value specified here for the alerts to be displayed.
- **Equals** – The priority value of the current alerts should be equal to the value specified here for the alerts to be displayed.
- **GreaterThanOrEquals** – The priority value of the current alerts should be greater or equal to the value specified here for the alerts to be displayed.
- **GreaterThan** – The priority value of the current alerts should be greater than the value specified here for the alerts to be displayed.
- **Only Show Alarm Alerts** – Select this option to show only alarm alerts, which means any manual alert that was showing previously will disappear from the list.

The icon is displayed in blue once the filter is applied.



To clear or reset the Alarm Alerts filter setting, select the **All Alarms** option. However, you cannot clear the existing filter, if one of the check boxes is checked.

Alarm Configuration

Alarm Types are configured using a wizard. This process allows the user to configure an alarm in the system based on an event from an object and then determine other criteria for creating and handling the alarm.

An Alarm Type defines an event in the system and includes properties to determine how an alarm of that type is created. The first properties of an Alarm Type specify the conditions under which the alarm is created; these include which type of device or specific devices to monitor, which event on the specified device type or devices to monitor, which location the alarm type relates to and finally which schedule the alarm type applies to.

The Alarm Types wizard enables you to determine the following:

- Label, description, and priority
- If the alarm type is a manual alarm type or initiated by an event
- The type of object or device

- Specific objects or devices in the system to monitor and the type of event to monitor
- Which location(s) the alarm type is for
- During what time period the alarm should be created by defining a date/time schedule
- Conditions to further filter events
- Options to determine the alarm point for each event (with advanced options to cater for complex alarm point classifications)
- Description of the alarm, which can be easily controlled
- Specification of the method for collating events together
- Which values to populate custom columns with
- Which response plans to run when the alarm is created, handled, modified and resolved

Defining an Alarm Type


This exercise guides you to create a sample alarm type and the various steps involved in the whole process.

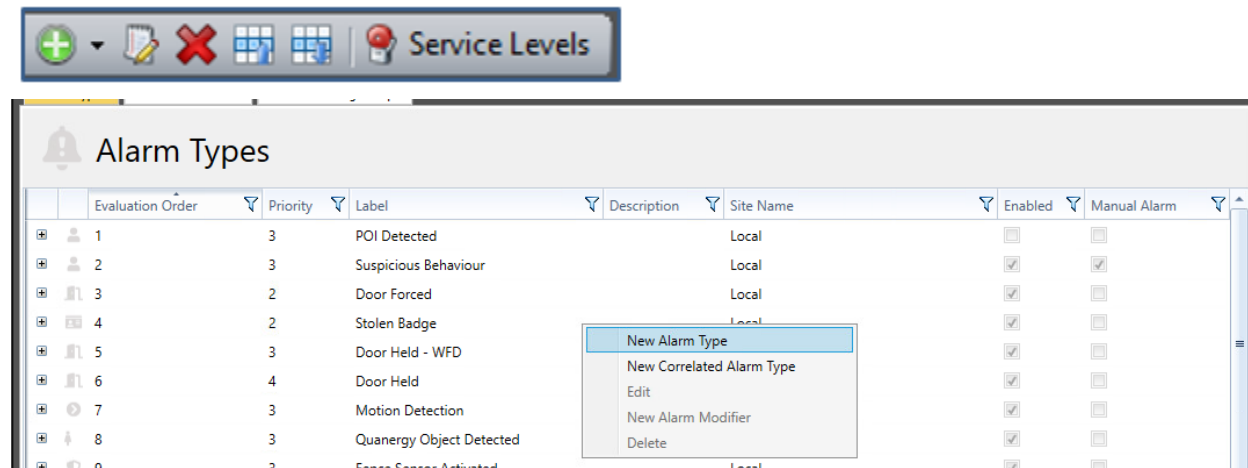
The alarm type and grids created in this chapter are for tutorial purposes only and are not intended to fit an exact requirement. Use these steps as a reference point and delete the alarm types and grids that are not applicable.

To define an Alarm Type:

1. Open **System Configuration > System Objects**.
2. In the **Overview** tab, double-click **Alarm Types**. The **Alarm Types Editor** appears.

Evaluation Order	Priority	Label	Description	Site Name	Enabled	Manual Alarm
1	3	POI Detected		Local	<input type="checkbox"/>	<input type="checkbox"/>
2	3	Suspicious Behaviour		Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	2	Door Forced		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	2	Stolen Badge		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	3	Door Held - WFD		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	4	Door Held		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	3	Motion Detection		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	3	Quanergy Object Detected		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	3	Fence Sensor Activated		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10	1	Fire Alarm - Remote		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11	1	Smoke Detected		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	1	VA Blacklist Hit		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
13	2	Overcrowding		Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	3	Access Denied		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
15	1	Panic Button Activated		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
16	3	Microwave Sensor Activated		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
17	2	Unauthorised USB Detected		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18	3	ITA Alert		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
19	2	Door Forced		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
20	1	Perimeter Breached		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- From the toolbar, click  and select **Add Alarm Type** or right-click in the **Alarm Types Editor** and select **New Alarm type** from the context menu. The Alarm Type wizard opens. The Alarm Types wizard is a single interface to create and edit alarm types. The wizard comprises a series of dialogs to define the alarm type parameters and how the alarm behaves in Control Center.



Defining Basic Information

The **Basic Information** page is used to name and prioritize the alarm.

Alarm Types Wizard

Basic Information


Label:

Description:

Enabled

Priority:

Override Priority With Alarm Point's Priority

Icon: 

Manual Alarm

1. Enter the Label as, for example, **Test Alarm**. It is the name that is displayed in the alarm stack as an identifier for the alarm.
2. Enter a short description of the alarm, for example, **Alarm used for out-of-hours activity in the marketing office**. This is not mandatory and can be left blank.
3. **Enabled** is selected by default.

Alarm types that are not enabled are not considered in alarm categorization.

The **Priority** field determines the priority for the alarm when it is created in the alarm stack. A fire alarm may be assigned a higher priority than an invalid access attempt to help users manage alarms based on their importance, for example. The priority of the alarm set is displayed for each alarm in the list in the **Alarm Types** section.

	Evaluation Order	Priority	Label	Description	Site Name	Enabled	Manual
⊕ ⚠	1	6	test Alarm		Local	False	False
⊕ 📄	2	3	TEST_ACS		Local	False	False
⊕ +	3	3	New alarm group		Local	True	False
⊕ 🚪	1	2	Test Door	An example of the Correlated Alarm	Local	True	False

4. For alarms that are associated with an alarm point (device or placeholder) you can define that the priority should be set based on the alarm point priority. Priority for an alarm point can be configured using the **Priority** property available on any device or place holder object. To configure the priority for a device or placeholder, select the object in **System Configuration** and change the **Priority** property in the property grid.

: Properties - (4 Placeholders)	
General Settings	
Created	
Description	
Enabled	False
Environment	Production
Icon	
Label	
Owner	System
Priority	5
Schedule	No schedule set

5. To make the alarm type use the **Priority** property, check the **Override Priority with Alarm Point's Priority** checkbox.

6. Confirm that the priority of this alarm is set.
7. When an alarm appears in the Alarm Stack Grid, a unique graphical icon can be displayed to signify the alarm type. Existing system icons and any custom icons imported through the Icon Manager can be selected. A yellow warning triangle with an exclamation mark in the center appears in the Alarm Stack View by default.
8. Click [...] to select from the available icons and click **OK**.

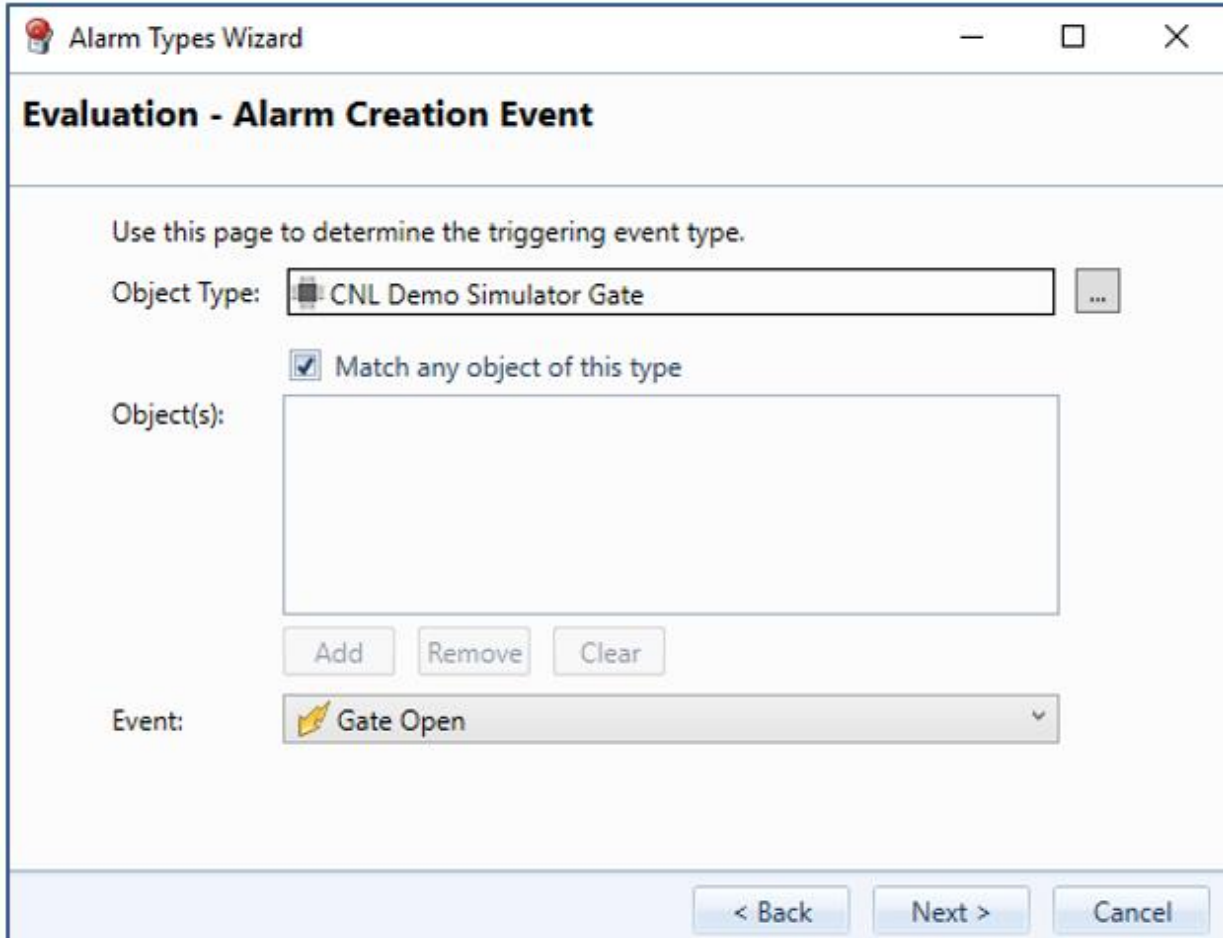
If no icon is selected, a red cross icon appears.

9. The **Manual Alarm** setting allows this alarm to be run manually, for example, they can be used for observed alarms. Leave the **Manual Alarm** unchecked and click **Next**.

Alarm Creation Event

This space is used to define the Object/Device Type and the events to be considered for it.

The Alarm Types wizard is equipped with picking up events from any objects as opposed to only devices done previously. In the Alarm Types wizard, on the alarm creation event section, any object type can be selected from the list as shown in the picture below.



Alarm Types Wizard

Evaluation - Alarm Creation Event

Use this page to determine the triggering event type.

Object Type:

Match any object of this type

Object(s):

Event:

Set how this alarm type is triggered using the Event field. The Event field is dynamically populated by events relevant to the device type selected.

1. Use the **Search** button to locate an object type that will trigger the alarm, such as sensor, camera, access point, and so on, and select it.

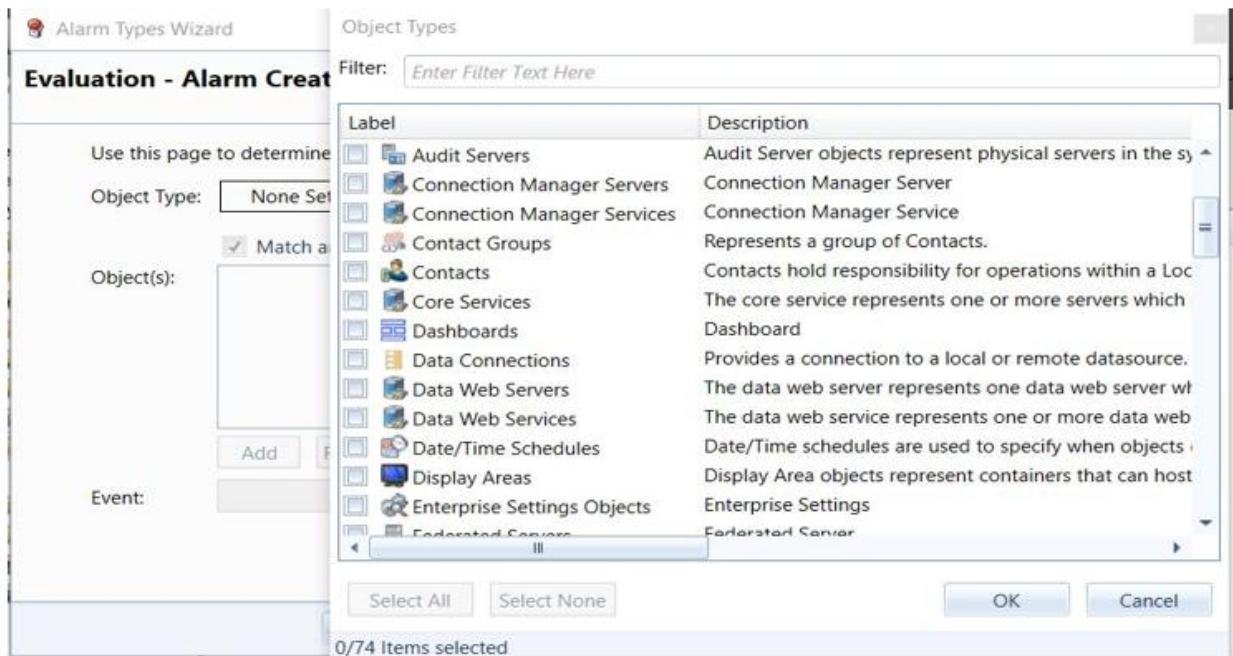
Only devices currently in the system are presented in the dialog.

2. The **Match any device of this type** check box is enabled.

Match any device of this type enables this alarm type for all devices of the type specified by Device/Object Type. Leave this check box enabled to run this alarm type on all devices for the Object Type specified above.



To define an Alarm Type for a specific device, uncheck the **Match any device of this type** option and select the alarm event and then attach this alarm type to a device using the **Add** button.

The Alarm Types wizard is equipped with picking up events from any objects as opposed to only devices done previously. In the Alarm Types wizard, on the alarm creation event section, any object type can be selected from the list as shown in the picture below.



3. Set how this alarm type is triggered using the **Event** field. The **Event** field is dynamically populated by events relevant to the device type selected.
4. Select an event relevant to the object type. The event appears in the **Event** field.
5. Click **Next**.

Alarm Creation Conditions

1. Use the **Search** button  to select the location of the devices to which this alarm type applies, for example Region. The Location field is populated by the selection made.
2. The time of day or week may affect an alarm’s applicability. For example, activity in and out of an access door during business hours is expected, however, activity through an access door during the night or over the weekend might raise an alarm. Alternatively, you could allow 24x7 access. Use the **Search** button  to select the schedules stored in Control Center, for example “24x7 allow”. The Schedule field is populated by the selection made.
3. Select the asset group if any, that the device is a member of. You could search for it by looking up by name or by property.

When you are looking up by property, the drop-down menu gives you various options of property values you could search the asset group on. You could also define custom properties to be included here. You could specify a condition by a property value of an asset group, that is evaluated when a device belonging to the asset group raises an event configured in the alarm.

4. The **Physical State of the Alarm Type** is a user-defined field used to determine the physical state of the alarm when created in the alarm stack. This can later be modified to indicate a change in the physical state based on subsequent events. For example, an access control alarm might be created with the physical state of **Open** which would indicate the state of the door when the alarm is created. The state can then be modified to **Closed** when the corresponding event for the same door is received. In this example, the initial physical state of **Closed** would be specified on this page.
5. Finally, the threat level can be specified as a condition or left for any threat level to be considered for triggering an alarm.

Alarm Creation Event Conditions

Additional conditions can be applied to alarm types to further refine their applicability. For example, an alarm type may be set to raise an alarm if a door is accessed outside normal working hours. However, security personnel patrolling the premises and presenting their key fobs at access doors should not raise an alarm.

An alarm type can require several conditions to be met. Keep adding conditions to refine the query. By default, **Event Conditions** is always empty. You could choose not to specify any conditions here and proceed to the next step and it is considered a valid configuration.

If you choose to define the condition and select **Add**, the above screen is displayed. You could select an event or object property to specify a condition and select **OK**. The condition is added to the list.

Conditions Queries

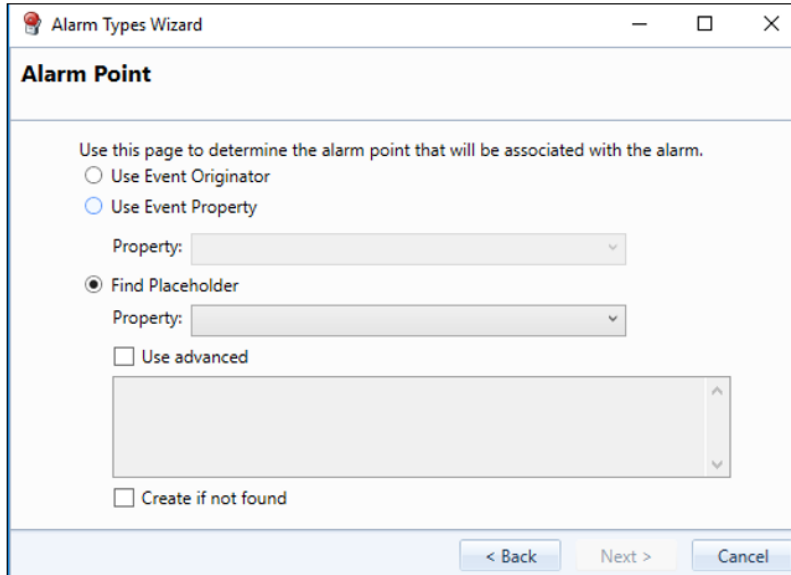
This provides, for instance, the ability to evaluate an event property value that matches a custom property of the device that triggered the alarm.

Field	Purpose
Source	The Source is the event or alarm point (device) property that we want to evaluate.
Operator	Defines the validation condition operator, for example, equals. Options include: equals, notequal, lessthan, lessthanequal, greaterthan and greaterthanequal.
Destination	The destination is the value we want to compare with. This can be a dynamic value such as a value from the event or Object (device) or a constant value (for example, Denied).

Click **Next** to continue.

Alarm Point

The Alarm Point is displayed in the Alarm Stack as a column. By default, the Alarm Stack displays the Event Originator as the Alarm Point. An example of this would be of an event originated from a door, for example, a Door Forced event.



The screenshot shows a window titled "Alarm Types Wizard" with a sub-header "Alarm Point". Below the header, there is a text instruction: "Use this page to determine the alarm point that will be associated with the alarm." There are three radio button options: "Use Event Originator", "Use Event Property", and "Find Placeholder". The "Find Placeholder" option is selected. Below "Use Event Property" is a "Property:" dropdown menu. Below "Find Placeholder" is another "Property:" dropdown menu. There is a checkbox for "Use advanced" which is unchecked, followed by a large empty text area with a vertical scrollbar. At the bottom, there is a checkbox for "Create if not found" which is unchecked. At the very bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

You could also specify **Event Property** as an alarm point. An example of this would be if the event contained a reference to an alarm point. For instance, a **Door raised a Reader Tamper** event and the event contained a reference to a specific reader.

In some cases, there is no pre-defined object to raise the event from. A basic integration might only provide a generic event source that raises all events. The event might contain a property such as Door ID. This can be used to create a Placeholder. This is an object representing a more specific device, for example, a door. A Placeholder can be plotted on a map, added to a location and so on, similar to a specific object. In this case, the **Find Placeholder** option can be used to identify the placeholder.

You can also use a script to identify the Placeholder, if for instance two event properties must be used in combination to create a unique reference. Placeholder script only allows the '+' and '&' operators for string concatenation.

If a Placeholder is not found, the **Create if not found** option specifies that the Placeholder should be created. The Placeholder is created in the same folder as the owning device.

Click **Next** to continue. The **Custom Column Mapping** page appears.

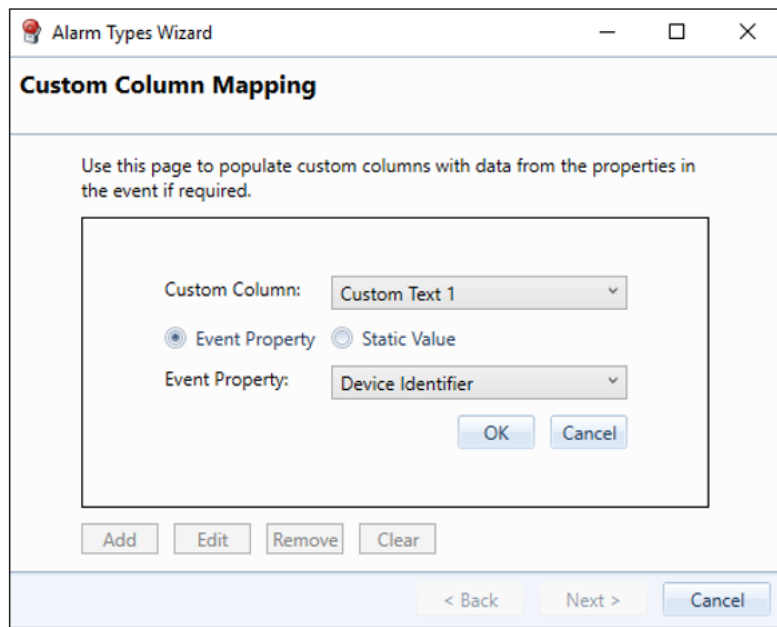
Custom Column Mapping

The Alarm Stack Grid can be customized to include additional information in new columns.

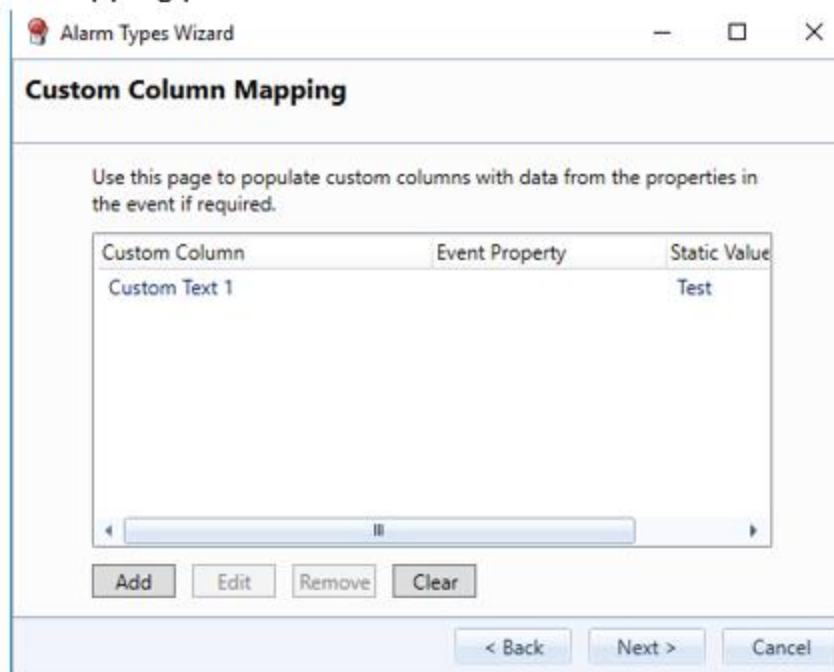
Any event data or static value can be used. An event can include location, access point type, access key, date and time and if the access was successful or not, for example.

Up to three additional data points, of each data type, can be included in the Alarm Stack Grid. (Up to twelve additional columns may be added but cannot exceed three integers, three text items, three Boolean items, and three date/time items).

1. Click **Add**. The **Custom Column Mapping** panel appears.



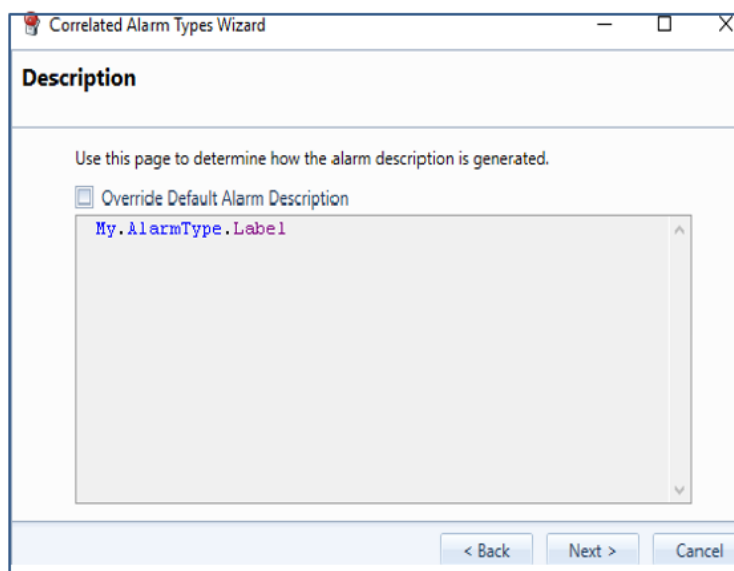
2. Click the **Custom Column** drop down and select the data format required for the additional column to display.
3. Select to populate the column with an event property value or a static value. If **Static Value** is selected, enter the value in the static value field. If event property is selected, the **Event Property** drop down list is populated with the available data held about the event stored in the selected format.
4. Click the **Event Property** drop-down to select a data item and click **OK**. The **Custom Column Mapping** panel now contains the additional column to display.



5. Click **Next**. The **Alarm Description** page appears.

Alarm Description

To override the default **Alarm Description**, use the script editor to write custom script. Select the **Override Default Alarm Description** checkbox to enable the script editor.



The description column in the alarm stack can be set using the script editor based on properties from the alarm type, alarm point and the event.

Click **Next**. The **Collation and Alarm Actions** page appears.

Enabling Bulk Resolutions of Alarms

To resolve bulk alarms, you must first enable the bulk resolve settings in the Alarms Type wizard.

1. From **System Objects**, double-click the **Alarm Type** that you want to allow bulk resolving for. The **Alarm Type** wizard opens.
2. Click **Next** until you are on the **Collation & Alarm Actions** page.
3. Select the **Allow Bulk Resolving** property for the alarm type you want to bulk resolve.

Alarm Types Wizard

Collation & Alarm Actions

Collation:

- Collate by Location
- Collate by Alarm Point
- Collate by Alarm Type
- Collate by Track ID
- Collate by Event Property:

Alarm Actions:

	Response Plan	Alert State
Created:	<input type="text" value="None Set"/>	<input type="text" value="Red"/>
Handled:	<input type="text" value="Template Handled VRP"/>	<input type="text" value="Yellow"/>
Modified:	<input type="text" value="None Set"/>	<input type="text" value="None"/>
Parked:	<input type="text" value="None Set"/>	<input type="text" value="Blue"/>
Resolved:	<input type="text" value="None Set"/>	<input type="text" value="Clear Alarm Point Alert"/>

Threat Level:

Allow Bulk Resolving

< Back Next > Cancel

4. Click **Next** until you are on the last page and then click **Finish**. The Alarm Type is created with the **Bulk Resolve** option enabled.

Notes:

- On upgrading from an earlier version of the software, you must enable **Allow Bulk resolution of Alarms** security policy in addition to enabling it in **Alarm Types** and **Alarm Stack Views**. By default, the **Allow Bulk resolution of Alarms** security policy does not have users and groups added.
- When working in a federated environment, if the Hub site is upgraded to Control Center Version 5.6, and if the **Bulk Resolve** capability is enabled, then the users can bulk handle alarms at the Hub site. However, if the Node site is not upgraded

to Control Center Version 5.6, then the **Bulk Resolution** capability is not available to the users for resolving the alarms coming from the Node site.

Collation and Alarm Actions

To reduce the number of alarms appearing in the Alarm Stack, it is useful to collate events by their Location, Alarm Point, Alarm Type, Track ID, or by Event Property.

For example, two cameras located in a long corridor generate motion detection events and detect something as movements are detected on the passageway. Instead of displaying in the Alarm Stack Grid twice, these two events can be collated. In the Alarm Stack, one alarm item appears with two events referenced.

In the same way, events with the same Location, Alarm Point or Alarm Type are collated into one alarm.

When multiple events are collated into one alarm, the alarm created response plan is only run once, when the first event occurs.

Care must be taken when collating Alarms. Alarms collated by Location are appended to the first event, whatever the alarm type. A priority 1 event could be collated in the Alarm Stack with events of lesser priority.

Using the example above, the two cameras generating motion detection events would create one alarm with two events. The Generated Alarm Plan and the Alarm Handled Response for the first event would be used.

Collation vs Grouping

You can group alarms. This is configured in the Alarm Stack View editor. Collating events differs to grouping them. Grouped alarms are included in the Alarm Stack in one collapsible section. Collated alarms appear as one alarm.

Alarm Actions

The Alarm Actions allow you to specify a response plan that is executed when the alarm is created, handled, modified, parked, or resolved. Typically, the response plan to show the corresponding alarm process guidance would be specified as the response plan to run when the alarm is handled.

Additionally, you can specify an alert state for each alarm action. When set, the corresponding alarm type will be placed in and out of the alert state according to the configuration when the alarm state is changed.

Alarm Created

The Response Plan configured against the Alarm Created action will execute when any alarm is created.

Alarm Handled

The Response Plan configured against the Alarm Handled action will execute when a user clicks to handle an alarm that is currently unhandled in the Alarm Stack, and the user is not currently handling another alarm. Typically, the corresponding alarm process guidance is specified as the response plan to run when the alarm is handled.

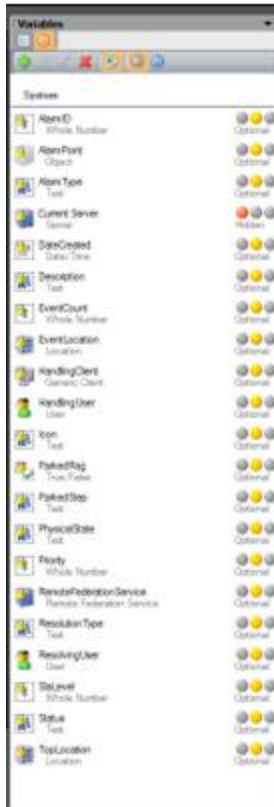
Alarm Modified Alarm Action

The Response Plan configured against the Alarm Modified action will execute when any alarm property is changed, it will however not execute if additional events are linked to the alarm.

In a federated system, a local Response Plan can be configured against the action on all federated sites.

The Alarm Modified action is also available for correlated alarms.

Once a Response Plan has been selected for an Alarm Modified action, relevant variables will be added to the plan automatically. These include Alarm Type, Alarm ID and Site (if federated).



Alarm Parked

The Response Plan configured against the Alarm Parked action will execute when an alarm is parked.

In a federated system, a local Response Plan can be configured against the action on all federated sites.

The Alarm Parked action is also available for correlated alarms.

Alarm Resolved

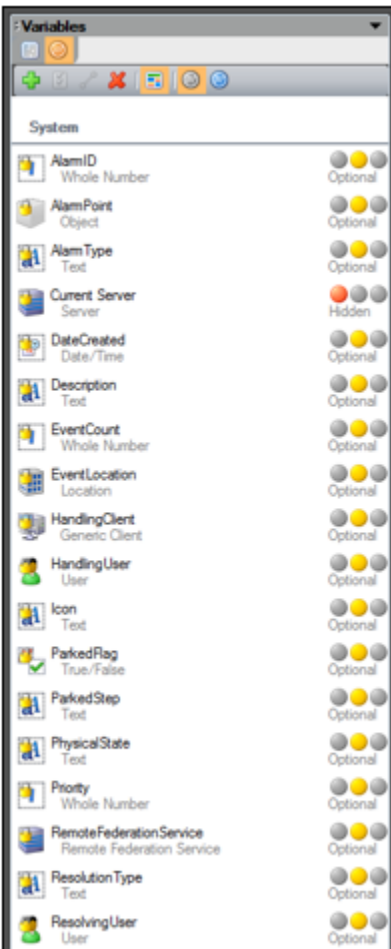
The Response Plan configured against the Alarm Resolved action will execute when an alarm is resolved.

In a federated system, a local Response Plan can be configured against the action on all federated sites.

The Alarm Resolved action is also available for correlated alarms.

Once a Response Plan has been selected for an Alarm Resolved action, relevant variables will be added to the plan automatically. These include Alarm Type, Alarm ID, Resolving

User, Resolution Type and Site (if federated).



Threat Level

You can raise the Threat Level by selecting the options in the drop-down list.

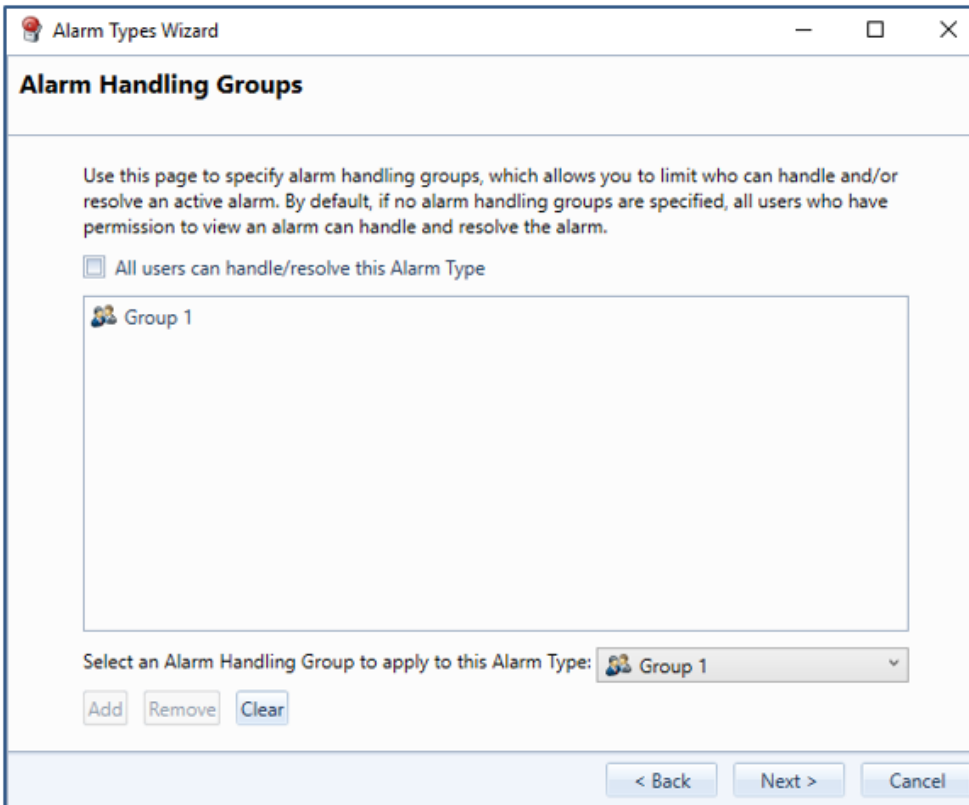
Bulk Resolution

Select the **Allow Bulk Resolving** property for the alarm type you want to bulk resolve. By default, the option is not selected.

Click **Next** to proceed to **Alarm Handling Groups**.

Alarm Handling Groups

From the Alarm Handling Groups, you can specify Alarm Handling Groups to allow only certain user or User group to handle and resolve alarms. In addition, you can configure comprehensive filter conditions for Alarm Handling Groups depending on your requirements. For more information, see [Configuring Alarm Handling Groups](#).



To configure Alarm Handling groups in the Alarm Types Wizard:

1. Select the **All users can handle/resolve this Alarm Type** option, if you want any user to handle or resolve the selected Alarm Type. Alternatively, if you want to specify an Alarm Handling Group to be able to handle the selected alarm type, clear the check box and then add a group manually.
2. Select from the available Alarm Handling groups from the drop down list and click **Add**. You will see the group added in the center panel of the screen.
3. Click **Next** to go to the **Service Level Agreement Overrides** page.

If the Alarm Type is linked to multiple handling groups, then each one of them will be processed to verify if the alarm can be handled.

Service Level Agreements Overrides

Each alarm type can be configured to override the default service levels (see [Bulk Resolving Alarms](#)). By default, each alarm type will be configured to use the default service levels. Alternatively, each level can be disabled or overridden (enabled) accordingly.

Click **Next** to go to the **Summary** page.

Summary

The **Summary** page appears, listing the details of the Alarm Type.

Confirm the Alarm Type details and click **Finish**. The alarm type appears in the **Alarm Types Overview** window.

Editing an Alarm Type

To edit an Alarm Type:

1. Open **System Configuration > System Objects** and double-click **Alarm Types**. The **Alarm Types Editor** appears.
2. Highlight the alarm type in the **Alarm Types Editor** and click the **Edit** button in the toolbar.



3. Alternatively, select the alarm type in the **Alarm Types Editor** and double click or right-click on the empty area and select **Edit**. The **Alarm Type** wizard appears populated with the alarm type data ready to edit.

	Evaluation Order	Priority	Label	Description	Site Name	Enabled	Manual Alarm
+	1	3	POI Detected		Local	<input type="checkbox"/>	<input type="checkbox"/>
+	2	3	Suspicious Behaviour		Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
+	3	2	Door Forced		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
+	4	2	Stolen Back		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
+	5	3	Door Held		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
+	6	4	Door Held		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
+	7	3	Motion De		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
+	8	3	Quanergy		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
+	9	3	Fence Sensor Activated		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Deleting an Alarm Type

To delete an Alarm Type:

1. Open **System Configuration > System Objects** and double-click **System Alarm Stack** in the **Alarm Types** editor. The **Alarm Types** editor appears.
2. To delete an alarm type, highlight the alarm type in the **Alarm Types** editor. Click **Delete** (red circle) in the toolbar.



3. Alternatively, right-click over the alarm type in the **Alarm Types** editor and select **Delete**.

	Evaluation Order	Priority	Label	Description	Site Name	Enabled	Manual Alarm
1		3	POI Detected		Local	<input type="checkbox"/>	<input type="checkbox"/>
2		3	Suspicious Behaviour		Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3		2	Door Forced		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4		2	Stolen Back		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5		3	Door Held		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6		4	Door Held		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7		3	Motion De		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8		3	Quanergy		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Correlated Alarms

Correlated Alarms provide the ability to define alarms that should only occur if one or more events occur/do not occur, based on the conditions specified on the object within a defined time.

When an event comes into the Rules Engine, it is evaluated against the list of Correlated Alarm Types defined within the system. During this process, previous events can be referenced and added into evaluation. Once the Rules Engine has decided that a new Alarm needs to be created, any existing alarms based on these events can optionally be resolved or reset.

	Evaluation Order	Priority	Label	Description	Site Name	Enabled	Manual Alarm
1		1	Correlated Intruder		Local	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2		1	CorrelatedTest		Local	<input type="checkbox"/>	<input type="checkbox"/>

Correlated Alarm Types are listed along with other Classic Alarm Types. You might want to describe them appropriately to distinguish between them in the list.

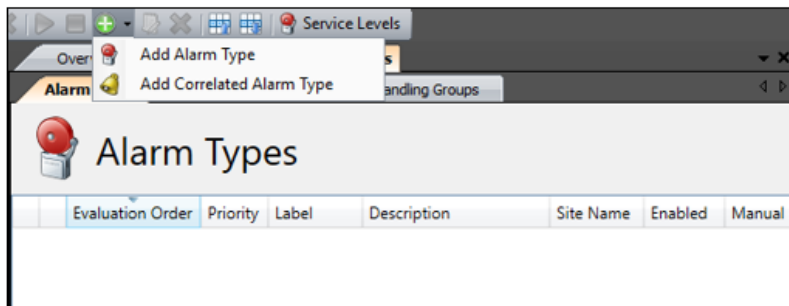
Alarm Types cannot be deleted if there are any alarms in the system of their type. This includes alarms that have been resolved. Alarms should be archived and removed from the live Pacific database if their Alarm Types need to be deleted. This applies to both Classic and Correlated Alarm Types.

With Classic Alarm Types, the order that Alarm Types appear in the list affects the way alarms are created. Each event can only create a single alarm from a Classic Alarm Type and they are evaluated in the order shown in the list. A single event can result in multiple Correlated Alarm Types, so the order shown here is unimportant.

Creating a Correlated Alarm Type

To create a Correlated Alarm Type:

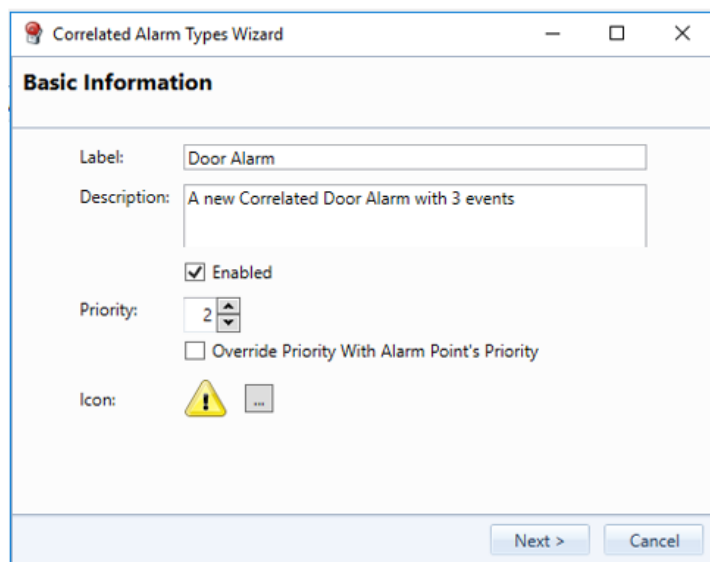
1. From **System Configuration > System Objects**, double-click the **Alarm Types** object. The **Alarm Types** editor appears.
2. Right-click on the empty space in the center pane and select **New Correlated Alarm Type** or click the **Add** button on the **Menu** bar.



A wizard guides you through the process of creating a new Correlated Alarm Type.

Correlated Alarm Basic Information


Use the **Basic Information** dialog to configure the basic information for a new Correlated Alarm Type. The **Label** provided here shows in the **Alarm Type** column of the Alarm Stack.



The **Description** field only shows in the **Alarm Types Management** dialog. This allows for multiple alarm types to appear the same but easily differentiated with further details to it, during commissioning.

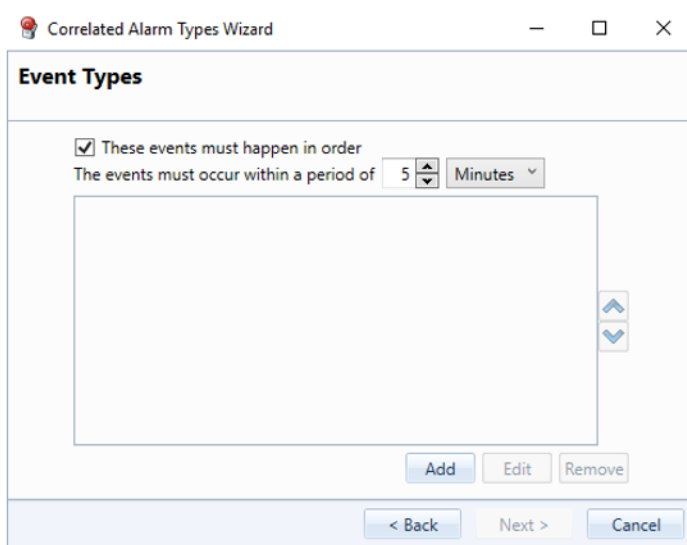
If the **Enabled** box is not checked, the Correlated Alarm Type is not evaluated when a new event comes in. However, events raised while the Correlated Alarm Type is disabled may be correlated into an Alarm created later.

If the **Override Priority** box is checked and the Alarm Point has a value for Priority, that value is used as the priority on a newly created alarm. Otherwise, the value provided here is used.


The icon specified here is used in the **Icon** column of the Alarm Stack. A default icon is provided which can be changed at any point by clicking on the  next to the icon. You can choose any icon from the standard set or custom set and hit **OK**. The new icon chosen is set for the correlated alarm

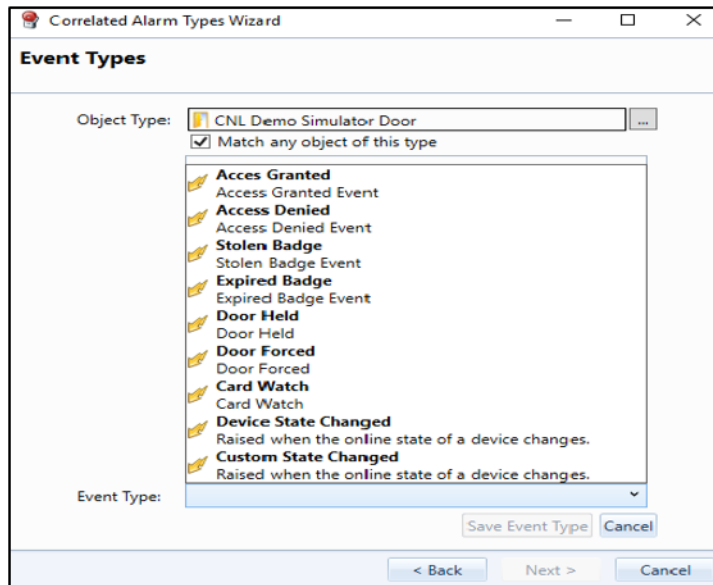
Correlated Alarms Event Types


This screen is used to select what types and sources of event form a part of this Correlated Alarm Type.

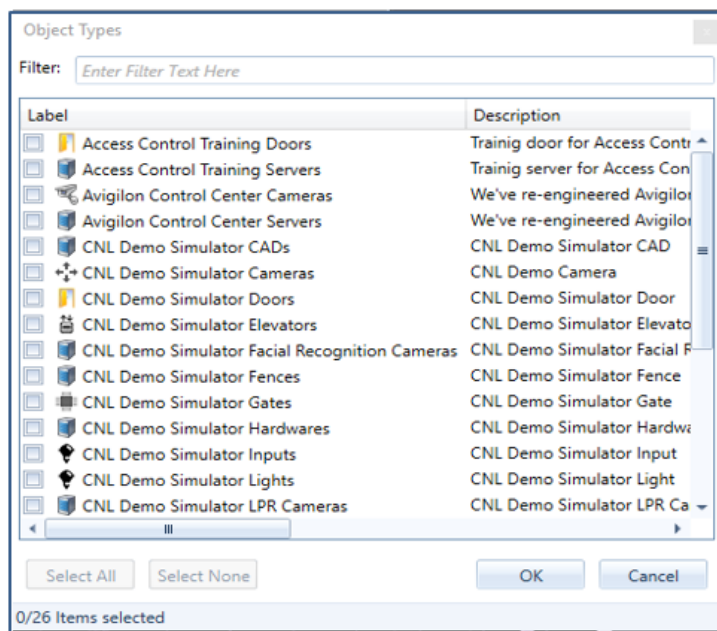


Initially the list is empty, and at least one event must be configured to move on. There is no upper limit to the number of events that can be included. Events added will be displayed in the center box and the order in which they need to occur can be changed by

using the  button on the right. Events can be added by clicking the **Add** button, and entering the details on the following screen.

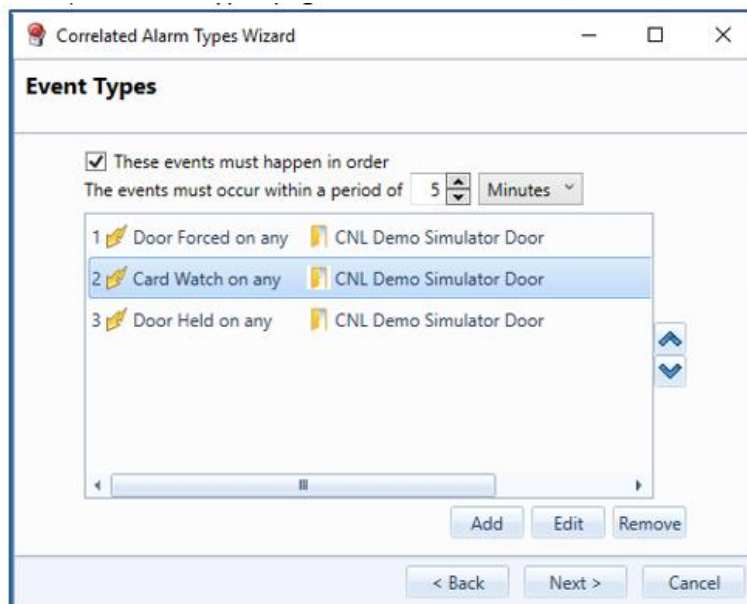


The **Object Type** option is used to pick the device that raises the event of interest. By default, the event will be matched from any source device, but this can be restricted by unchecking the **Match any** box and supplying a list of devices. Clicking the  button, opens the **Object** window from which you can choose an object from the available list and select **OK**.



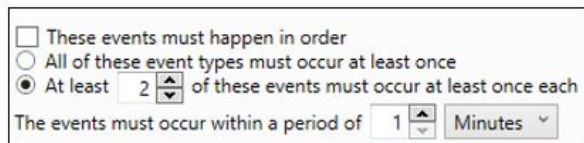
The Event Type can be selected from the available events on that object using the drop-down box at the bottom of the Event Types window. After selecting the event for the object, click on the Save Event Type Button to save the event.

Upon saving the events, the Event Types page will look as shown below.

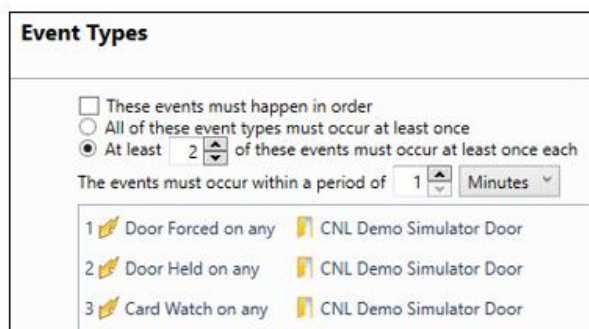


In the above example, a basic correlated alarm is created when all three listed events occur in the exact order as listed above within a 5-minute window. Further conditions can also be configured.

It is also possible to create an alarm where the order of events seems less significant. Deselect **These events must happen in order**. This displays some extra options.



The first radio button causes the alarm to be created when all the events configured, occur at least once within one-minute window from the time the first event occurred, regardless of the order in which they occur.

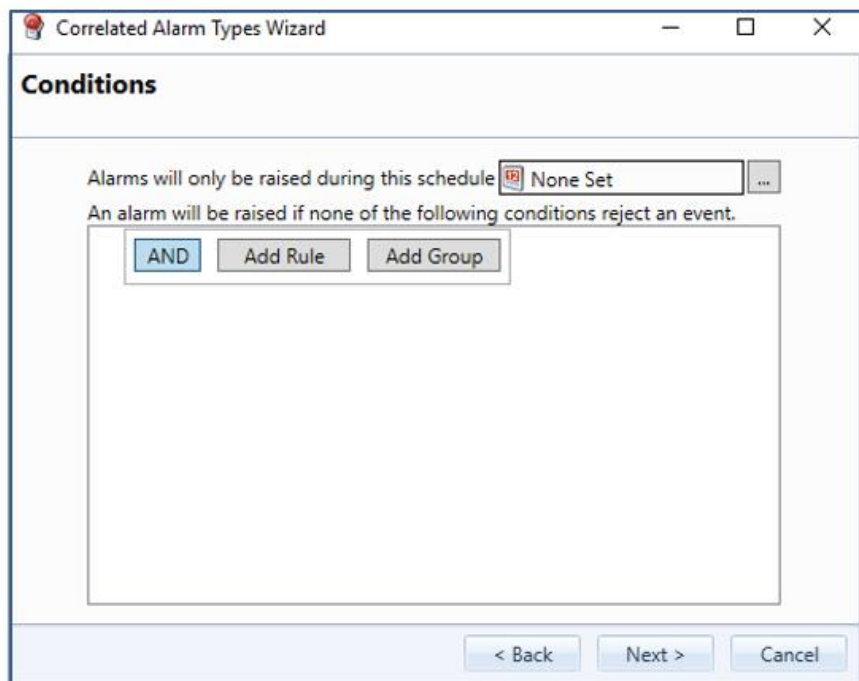


The second option allows for optional events to be included in an alarm. In this example, the alarm will be raised with any combination of 2 or more of the events, that is, a **Door**

Forced event and a **Card watch** event. If a **Door Held** event arrives after the alarm has been created, but within 1 minute of the other events, it will be added to the alarm.

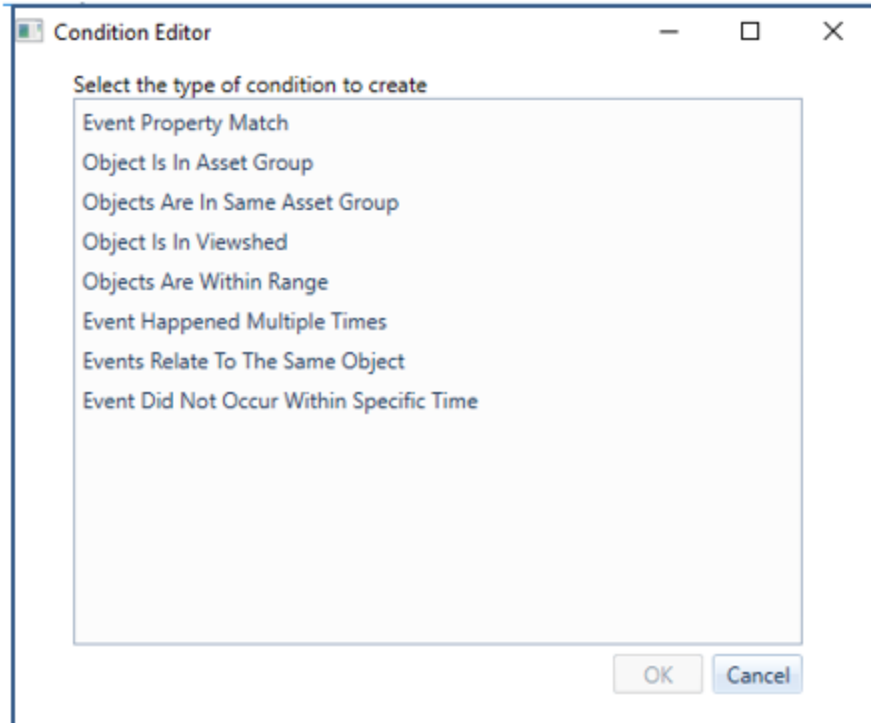
Correlated Alarm Conditions

Unless configured otherwise, any event of the correct type from one of the source devices selected will be taken into consideration in the alarm. The conditions page is where filters can be applied that will remove events from consideration.



The default settings on this page are a valid configuration, so you can continue without changing any settings.

If no schedule is set, alarms will be created at any time. If a schedule is added, an alarm will only be created when the schedule is active. It may include events that occurred before the schedule became active.



Nested conditions are restricted to **Event Property Match**. In other words, when you are configuring nested conditions then the Condition Editor only displays **Event Property Match**.

Correlated Alarms Event Property Match

When creating a correlated an alarm, you can configure a condition that validates against

- a property of an event, or
- a static value in a property of an event.

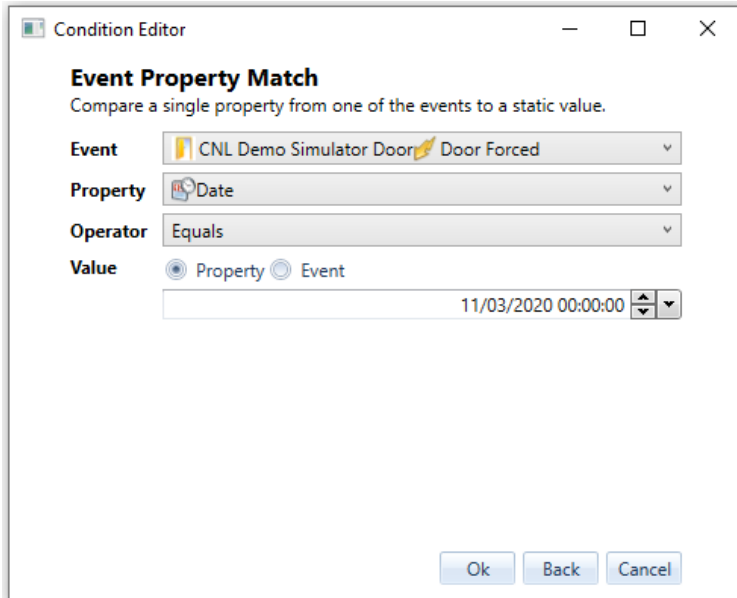
For example, you may want to create

- an alarm if there are door forced events on the same date
- an Intrusion alarm with higher priority if an intrusion alarm and door forced alarm happens in the same Intrusion Zone.

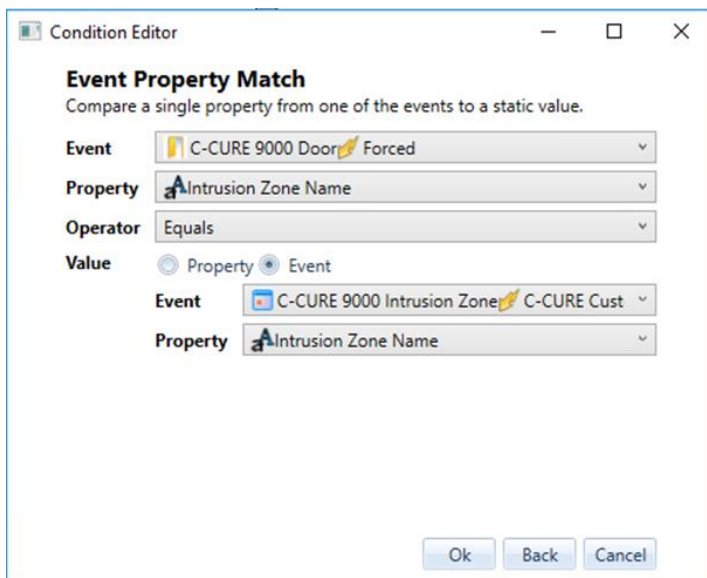
To configure this:

1. From the **Event** drop-down list, select one of the events you specified in the **Events Type** page in the **Correlated Alarms Type** wizard event. This is the event whose properties you want to validate against before creating the alarm.
2. From the **Property** drop-down list, select a property of the event you specified.
3. From the **Operator** drop-down list, select the operator you require.
4. For **Value**, select either:

- **Property.** Enter a static value that you want Control Center to validate against before the alarm is created.

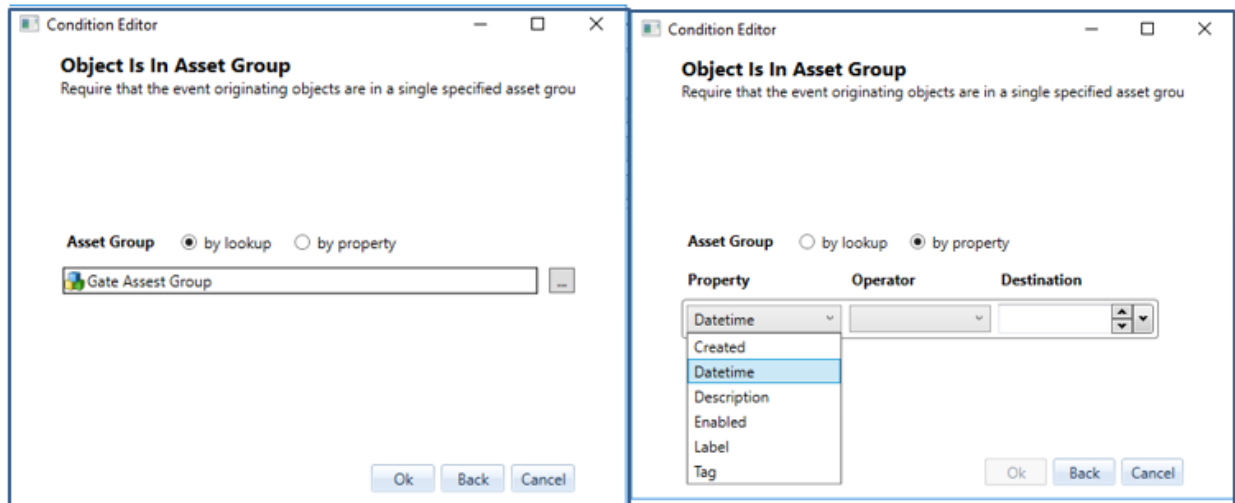


- **Event.**
 - From the **Event** drop-down list, select one of the events you specified in the **Events Type** page in the **Correlated Alarms Type** wizard event. This is the event whose properties you want to validate against before creating the alarm.
 - From the **Property** drop-down list, select a property of the event you specified.



Correlated Alarm Type in Asset Group

This condition has two options as seen in the picture below:



- Asset Group by Lookup:** This condition requires that all events are contained in the specified Asset Group. The desired asset group can be searched and selected here.
- Asset Group by Property:** This condition requires that all objects in the asset group satisfy the criteria specified here. The drop-down menu for the property has various options to choose from, giving a greater flexibility for the user to filter the events, for creation of alarms. The Operator drop-down menu will show options based on the property selected and destination will allow you to input values depending on the property chosen for validation.

This feature comes in handy in a federated environment where the NOC is able to reference the Asset Groups from all its connected sites. Normally alarm types are created at the NOC and published down to all sites. While creating a correlated alarm for an asset group, the assets group looked up would essentially be local to NOC. For referencing the asset groups from all the child sites, you could use **Object Is In Asset Group by property** feature which specifies a generic condition for search. This helps looking for asset groups on all sites matching a property value of the group.

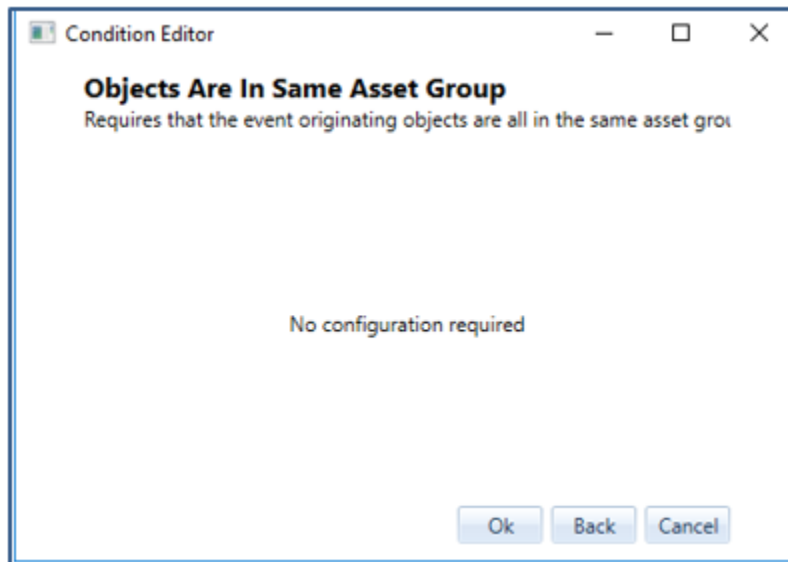
For example, if you have a Door Held event defined on an Object Type, you could configure the alarm type to look for all asset groups from all connected sites and raise an alarm if the Door Held event occur/does not occur from the devices configured within the asset group. Other doors raising the same event will not contribute towards the alarm generation.

The site that owns the device will see an alarm in the alarm stack and is also pushed back to the NOC. If more than one site meets the condition configured in the alarm, the sites

that generated it will display an alarm in the alarm stack and the NOC will have a collection of alarms from all sites.

Objects are in Same Asset Group

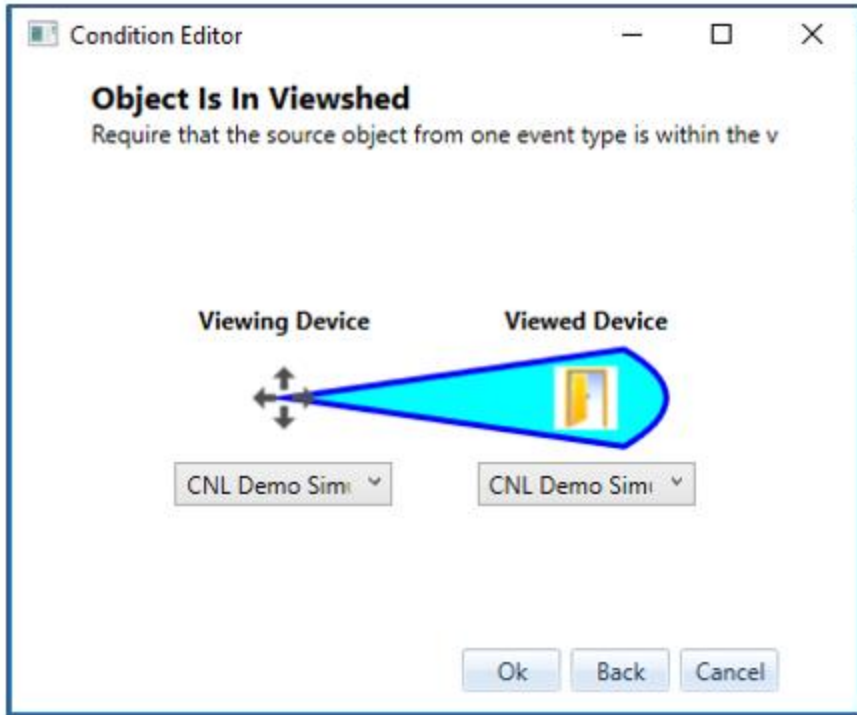
This condition requires all the objects for which the events are being raised, belong to the same asset group. No configuration is required as all the objects are necessarily included here.



An example usage for this could be creating an asset group for all entrances to a building that is monitored by the access control readers and motion sensors surfacing the entrance. An alarm could then be raised if movement is detected and/or the access control detects a door forced event. A combination of events can be configured for various objects in the asset group to tighten up the security around the building.

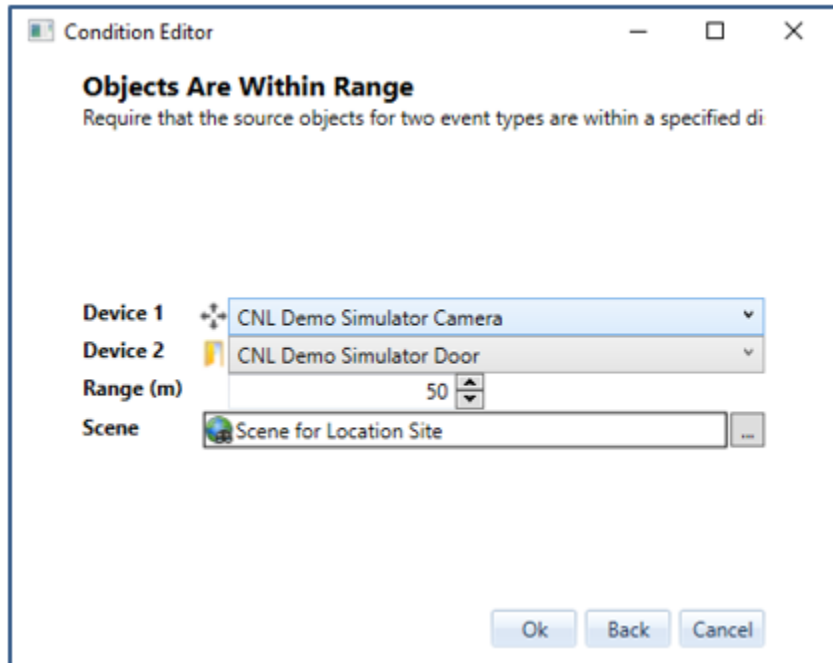
Correlated Alarm Type in Viewshed

This condition uses geographic scene data to check if one device is plotted within the viewshed of another. The condition rejects events from devices that are either not plotted on a geographic map or are not contained within the appropriate viewsheds.



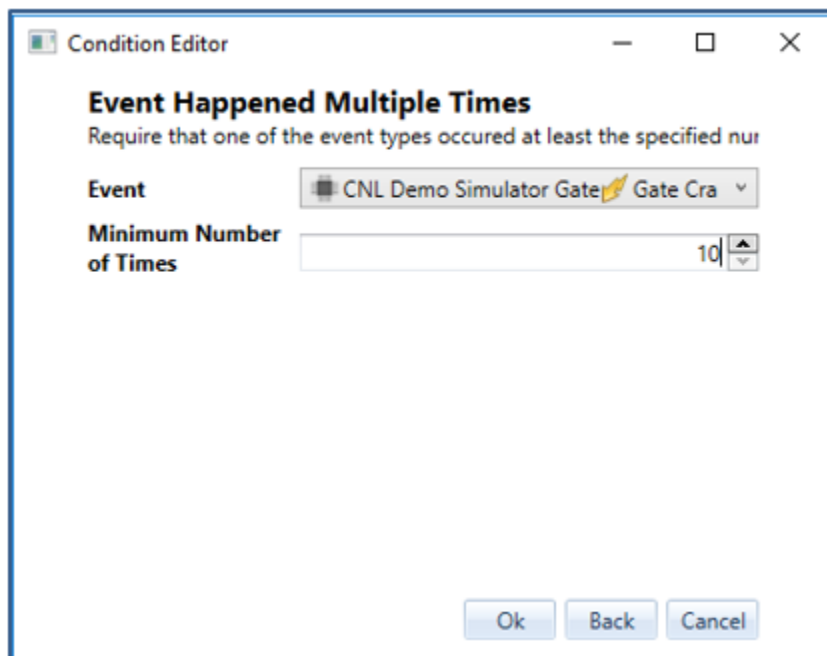
Objects are Within Range

This condition checks for the selected geographic scene where both device types have been plotted and are within the range specified of each other. Events from devices that are not plotted on the selected scene and are not within the specified distance are ignored.



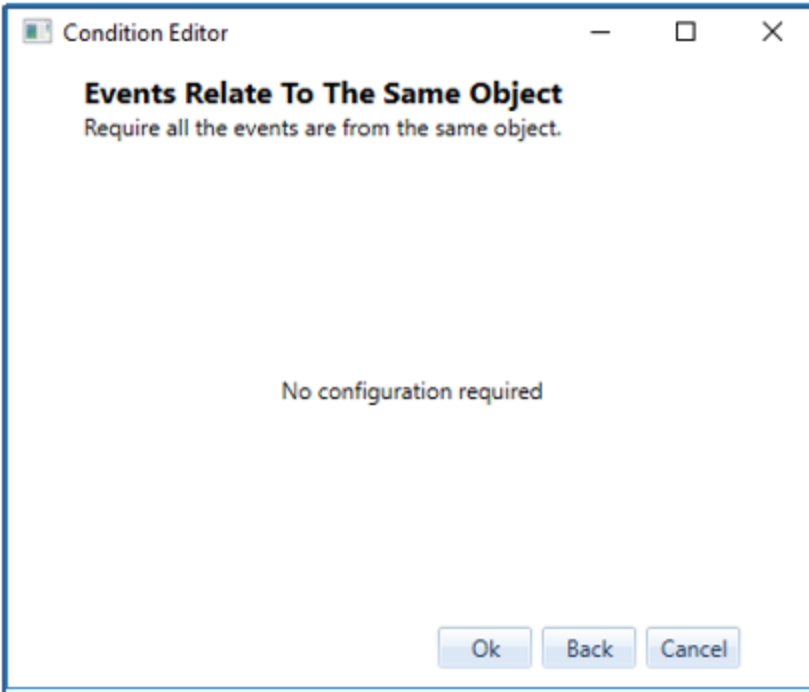
Event Happened Multiple Times

This condition requires that one specific event occurred multiple times within a certain amount of time for the alarm to be created. An example of this could be a fence intruder detection system that is prone to occasional false positives. Someone walking past the fence in close vicinity or attempting to climb the fence would cause multiple events in a short period.



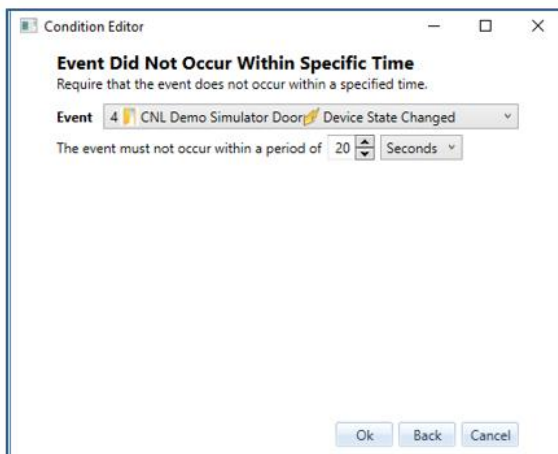
Events Relate to the Same Object

This condition requires the events to be raised from the same object. For example, if Door held event is raised for Door 1, it is expected that the Door closed is also raised for Door 1. This will determine whether or not an alarm needs to be raised against that object if the door is held open for longer than a certain time period.

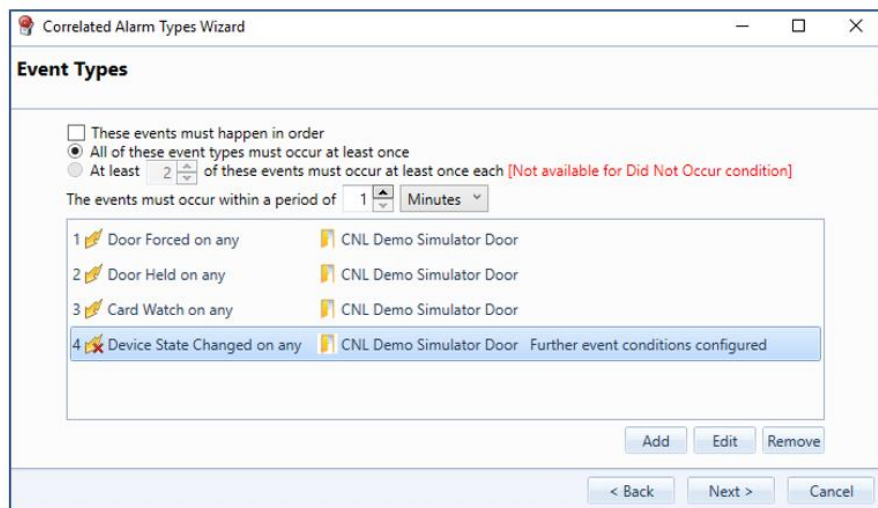


Events did not Occur Within Specific Time

This condition requires an alarm to be generated, if an event specified here does not occur within the configured time.



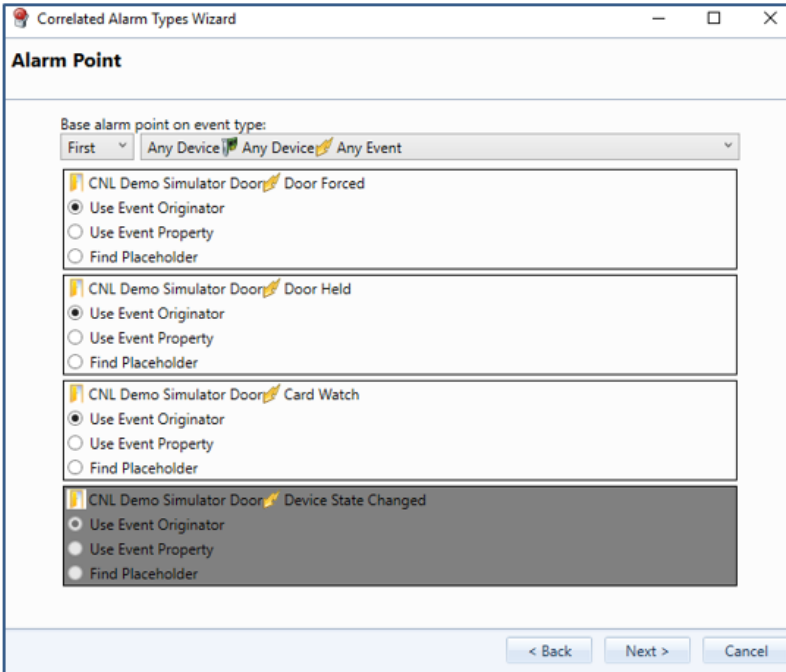
An example situation here being a Door Open event to be followed by a Door Closed event within the specified time to keep the area safe. If the Door Closed event does not occur within 20 sec as mentioned in the picture above, an alarm is created to notify the operator that a certain door isn't closed. The **Event Types** screen will look as shown below.



The **Event Did Not Occur** option is not available for the third option as it is not required for all the events to occur here. So, if the **Event Did Not Occur** event has not occurred, this condition will still be true as all the events are not expected to happen.

Correlated Alarm Points

This page determines the Control Center object that is used as the Alarm Point for the alarm. The first or last event of a single type is picked now, and the alarm is created based on these settings. The Alarm Point is not changed by extra events being raised after the alarm is created but can be changed by configuring an Alarm Modifier.



The alarm point can be based on the following three options:

- **Event Originator:** uses the device that raised the event.
- **Event Property:** uses a device that was referenced as a property on the event. Most device events do not have a suitable property as current best practices for connector coding is not to do this.
- **Find Placeholder:** uses an event property to find a placeholder attached to the device that raised the event.

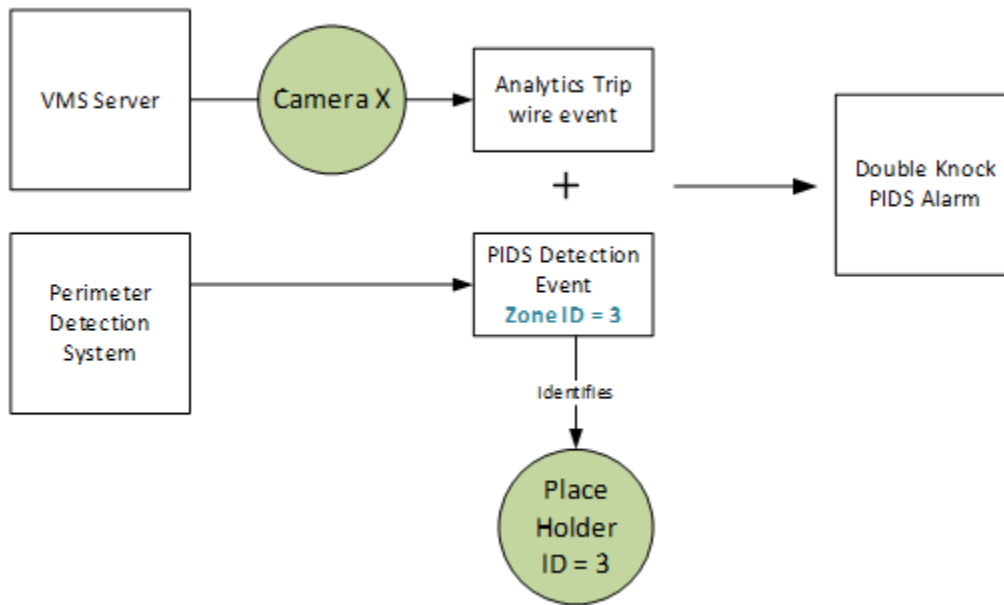


If the **Create if not found** box is checked, missing placeholders will be created in the same location as the device that raised the event.

Note:

1. If the event type selected is not included when the alarm is created through use of the **At least x of these events must occur at least once each** option on the Event Types page the alarm will be created without an Alarm Point.
2. A Correlated Alarm Type is triggered by at least two events from one or many sources. To identify a specific location that the alarm originated from, one of the sources is selected as the alarm point identifier.
3. For many devices, the source of the alarm is the Alarm Point. For instance, if an analytics alarm is raised by a camera, the camera is the Alarm Point.

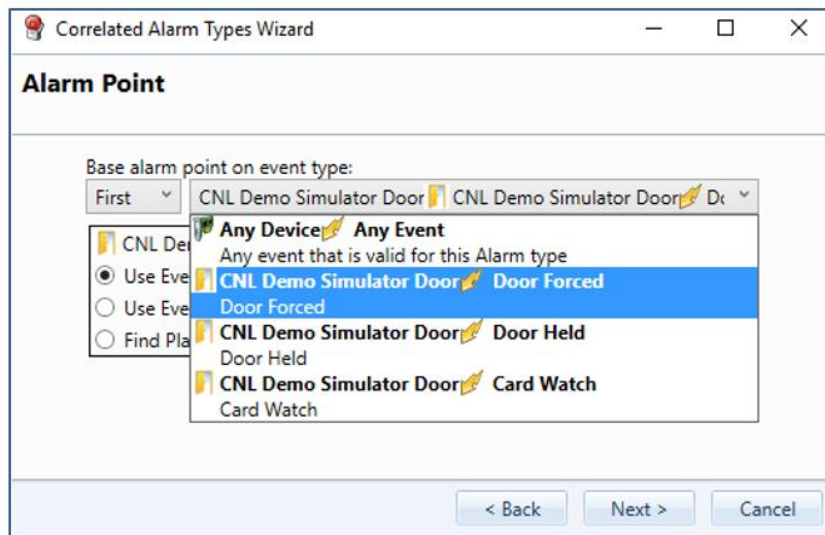
- The event type for **Event did Not occur Within Specific Time** is shown as greyed out. For some devices, the Alarm Point is identified by data received in the event. For instance, a PIDS device can raise an intruder event. The event includes a Zone ID and Control Center uses this data to find a matching Placeholder which will be used as the Alarm Point.



The Alarm Types wizard provides the ability to specify exactly how the Alarm Point shall be identified for each type of event that is linked to the Alarm Type.

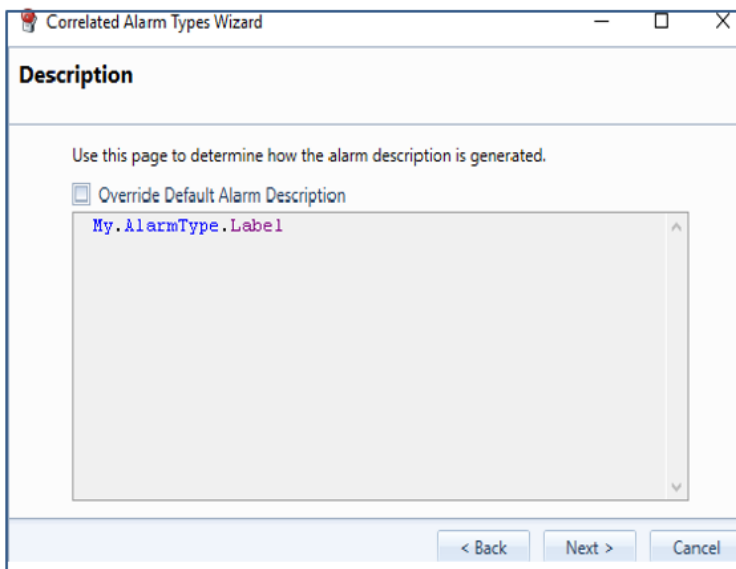
By default, Control Center will use the Event Originator as the Alarm Point. To change this, for instance to find a Placeholder, select the matching radio button at the Alarm Point step in the Alarm Types Wizard.

You could also set the Alarm point based on a particular event type as shown below.



Alarm Description

To override the default **Alarm Description**, use the script editor to write custom script. Select the **Override Default Alarm Description** checkbox to enable the script editor.

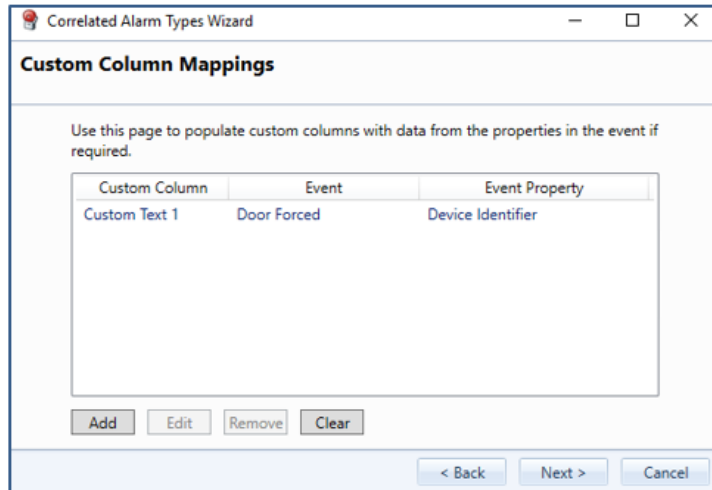


The description column in the alarm stack can be set using the script editor based on properties from the alarm type, alarm point and the event.

Click **Next**. The **Collation and Alarm Actions** page appears.

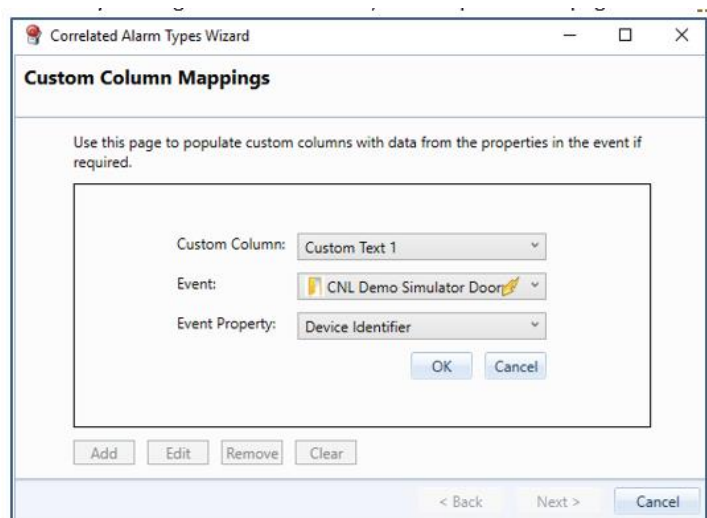
Custom Column Mappings

Custom column mappings set properties on the alarm to contain values from the events that make up the alarm.



The list is empty by default, and this is a valid configuration. The default Alarm Stack View does not show any custom columns to the operator. The values will be stored in the Alarm even if they are not shown and can be read using the Read Alarm response plan shape.

Mappings are created by clicking the **Add** button, which updates the page to look similar to this:



Start by selecting the column that you want to insert a value into. The available event properties will be filtered based on the data type selected for the custom column, that is, Credential Identifier will NOT be available for the **Custom DateTime 1** column. All properties are available for the Custom Text columns.

Once the settings are correct, clicking **OK** will return the page to show the list of mappings, containing the newly added mapping.

Mappings can be edited or removed by selecting them in the list and clicking the appropriate button. The **Clear** button removes all mappings.

Actions

This page determines what happens once alarms are configured against specific events.

Collation

The collation settings determine if a new alarm should be created, or if the events should be added to an existing alarm.

- **Collate by Location** - Uses the location that the alarm point is contained in for grouping the alarms.
- **Collate by Alarm Point** - Uses the Alarm Point selected on the Alarm Point screen for grouping the alarms.
- **Collate by Alarm Type** - Only groups with other alarms of the same type.
- **Collate by Track Id** - Collates alarms from the same Radar track.
- **Collate by Event Property** - Adds drop-down boxes to select which event and property on that event to use for collation. In this example, alarms will only collate if they contain a credential swiped event for the same door.

Collation:

Collate by Location

Collate by Alarm Point

Collate by Alarm Type

Collate by Event Property :

Training Server Credential Swiped ▼

1 Door Identifier ▼

Correlated Alarm Actions

This section allows you to set the Response Plans to run when an alarm is created, or its state is changed.

- **Alarm Created** - Runs only once when the alarm is first created. It does not run when extra events are added through collation.
- **Alarm Handled** - Runs whenever a user handle an alarm that they are permitted to handle. They may already be handling this alarm. The alarm may have been in the unhandled, parked or handled states.
- **Alarm Modified** - Runs when the properties of an Alarm are changed, either by an Alarm Type Modifier or the Modify Alarm shape. It does not run when events are added, or an alarm is handled, resolved or parked.
- **Alarm Parked** - Runs whenever a user parks an alarm. The alarm may have been in the unhandled or handled states.
- **Alarm Resolved** - Runs only once when the alarm is resolved. This is usually the last response plan associated with an alarm, however, it is not recommended to modify an alarm after it is resolved.
- **Alert State** - If an alert state is selected here, it will be applied to the Alarm Point when the alarm is created and removed when the alarm is resolved.
- **Threat Level** - If a Threat Level is selected here, the system wide threat level will be raised to the level selected from a lower level. When the alarm is resolved, the system wide threat level may drop if this alarm was the highest-level threat in the system.

Allow Bulk Resolving

If this is enabled the alarms created for this alarm type can be bulk resolved in the alarm stack instead of resolving it individually.

Existing Alarm Behavior

The following two properties determine what should happen to alarms created by events that are included in this correlated alarm.

- **Forcibly Park** - Sets the alarms to the Parked state if they are currently being handled and raises the Forced Park event on the Alarm Types server, which can be used to stop an ongoing process guidance.

- **Forcibly Resolve** - Sets the alarms directly to the resolved state. This happens regardless of the current state of the alarms.

You can set the above actions to be executed **On Create** or **On Resolve** actions:

- **On Create** - Occurs at the time the correlated alarm is created. It does not happen on collation of additional events.
- **On Resolve** - Occurs when the correlated alarm is resolved through the resolve alarm response plan shape.

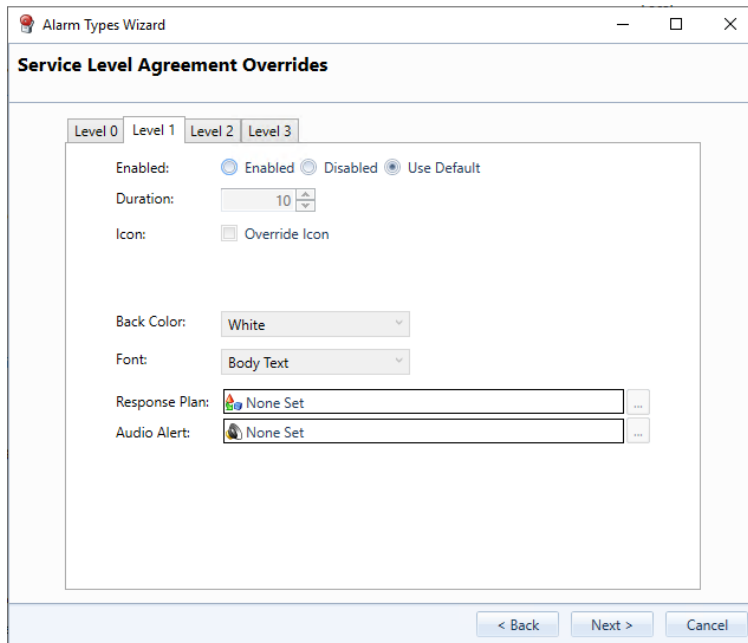
Correlated Alarm Handling Groups

This screen is used to specify which user or user groups can handle/resolve an alarm. If no alarm handling groups are specified, then all users will have permission to handle/resolve the alarms.

If **All users can handle/resolve this Alarm type** is ticked, then all users will have permission to handle the alarm. If you wish to give the permission to a particular group, then deselect the option and select an alarm handling group from the drop-down [alarm handling group must be previously created] and click **Add**. The group name will appear in the center box to indicate that it has right to handle/resolve the alarms. To view the members of the group, go to the **Alarm Handling Group** tab under Alarm Types and double click on the group you wish to check on.

Service Level Agreement Overrides

This page controls formatting of the alarm as viewed in the Alarm Stack.



The default settings are for the alarm to use the system wide defaults. These can be overridden on a per-service level basis.

- **Enabled**
 - **Enabled** - The alarm can breach this service level, and that the settings provided here take effect.
 - **Disabled** - The alarm cannot breach this service level. This does not stop it from breaching higher service levels.
 - **Use Default** - The system wide setting for this service level will apply.
- **Duration** - The elapsed time in seconds since the alarm was created. This is total time, not time since the previous SLA breach.
- **Icon** - Changes the icon displayed in the Icon column of the Alarm Stack.
- **Fore Color** - Apply to all text on the alarm row.
- **Back Color** - Affects the background of the whole row.
- **Font** - Apply to all text on the alarm row.
- **Response Plan** - The response plan runs once on the server when the service level is breached. The response plan variables include the alarm ID, the alarm type name and the service level that was breached
- **Audio Alert** - Plays on all clients that would be able to see the alarm, whether an Alarm Stack is displayed or not. Clients that have no Alarm Stack View that would show the alarm do not play the alert. Audio files must be in .wav or .mp3 format.
 - When audio is selected, the following options are displayed:

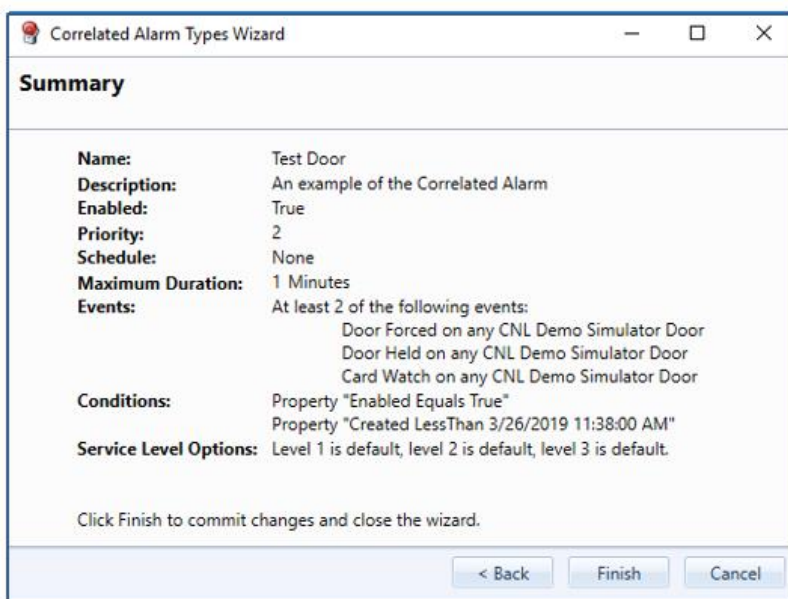
- **Loop Audio** – When selected, the audio alert will play on repeat until stopped.
- **Stop Looping** – Looping audio alerts always stop playing when the alarm is resolved. Additional stopping points can be added to stop audio when the alarm is handled or parked. See [Configuring Audio Alert Snoozing](#) for information on related functionality.

Level 0 refers to the state of the alarm immediately after it has been created, and before any service level is breached. Therefore, it cannot be disabled, has no duration setting, and cannot have a response plan configured.

The system wide default service level settings can be adjusted from the Alarm Types management screen by clicking the Service Levels button on the tool strip.

Correlated Alarm Types Wizard Summary

The **Summary** page provides a brief overview of the alarm configuration. Not every setting is reflected on this page. Clicking **Finish** will save the updated Alarm settings to the server, where they will take immediate effect. Existing alarms of this type will not be directly changed, but events may be added to them following the updated settings.



Correlated Alarms Scenario 1: Rules Engine Goes Down When Events are Being Created

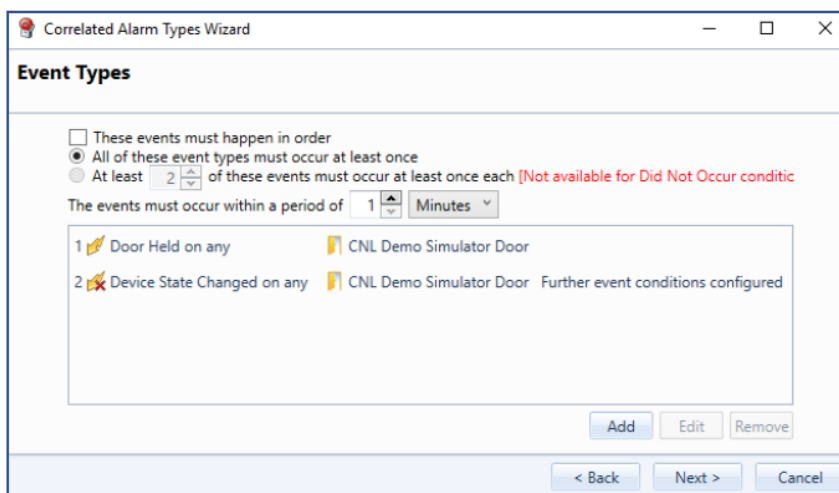
If the Rules engine goes down after event/event(s) have occurred and comes back up after further events defined in the condition set of the correlated alarm has occurred, but within the specified time, correlated alarm is generated. However, if the Rules Engine comes back after the specified time, then no correlated alarm is created. For

example, If you have 2 events configured in the correlated alarm to occur within one-minute time period:

- Door held
- Card watch
- One event occurred, and rules engine goes down, second event occurs, and rules engine comes back up; All happening within the one-minute window specified in the alarm condition, then correlated alarm is created. But if the Rules Engine comes back up after the configured time, no correlated alarm is generated.

Correlated Alarms Scenario 2: Event did not Occur Within Specified Time

A correlated alarm can be generated where the second event is required to happen within a specified period of the first event's occurrence. This feature can also be extended to the Alarm modifier where the alarm is modified if the event did not occur within certain time.



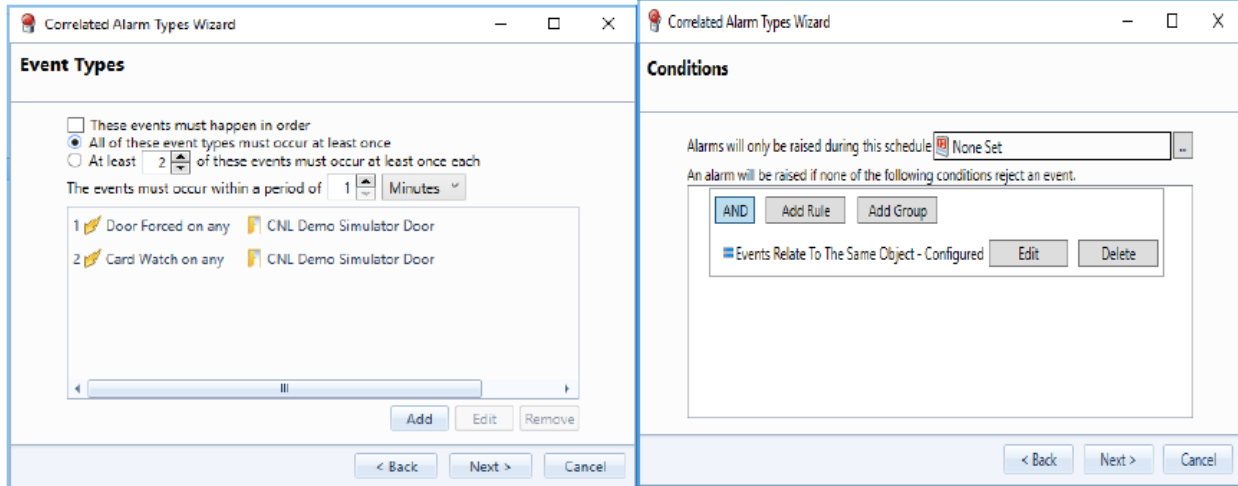
For example, if two events,

- Door Held Event occurs, and an alarm is generated
- A modifier can be configured to increase the priority of the alarm if the Door closed event does not occur within 30 seconds.

The above events are configured for a correlated alarm. The Door held event comes through and Door State Change event does not occur within certain time period, then an alarm is generated. To explain further, if the door is held for longer than 10 secs, then an alarm is created to notify the operator, as the door is expected to be closed within that time period to keep the area safe.

Correlated Alarms Scenario 3: Events Relate to the Same Object

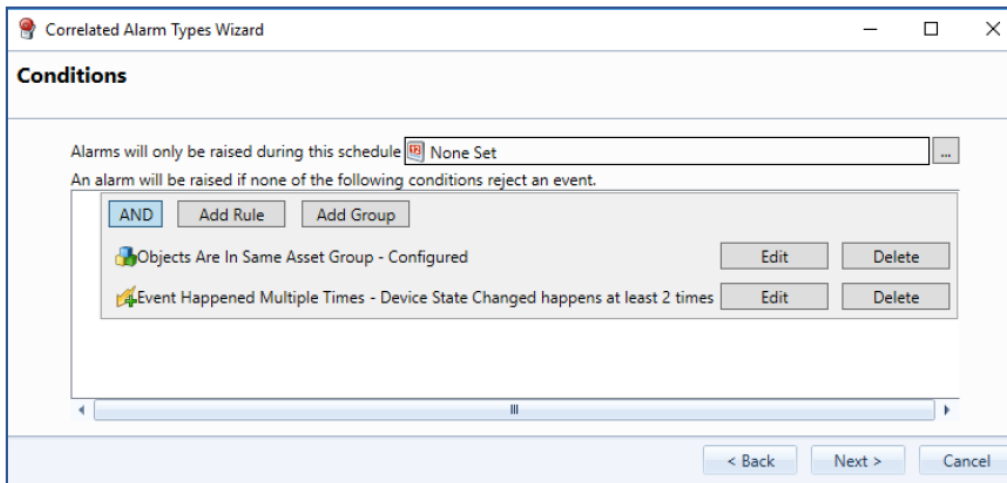
A correlated alarm can be generated when only events related to the same object occur.



For example, if Door forced is created for door 1, and another Door force is created for Door 2, a third event card watch occur for door 1. It is good to infer that door 1 was forced and then a card was presented to gain access, while door 2 is still stands forced. As a result, correlated alarm will be generated for door 1.

Correlated Alarms Scenario 4: Event Happened Multiple Times

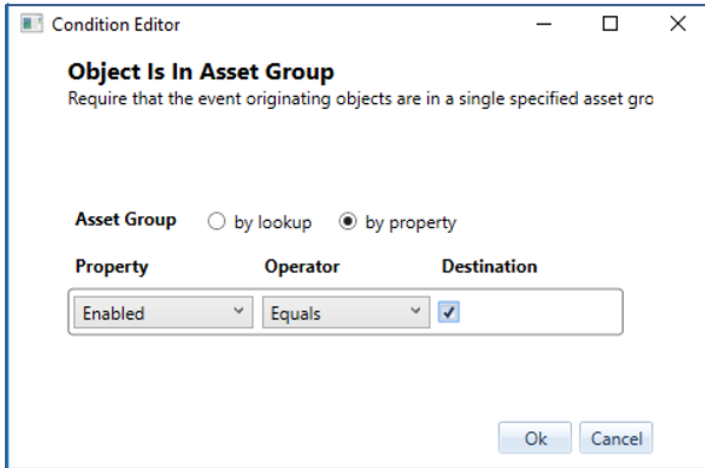
If you wish to raise an alarm only if the event has occurred several times, then add the Event happened multiple times condition. You could also harden the scenario by adding Event relate to the same object or are part of the same asset group. This will ensure the event is coming from the same device or same asset group to be able to generate an alarm.



In real life situations, you can configure an alarm to be raised only when a door forced event occurs certain number of times on the same door.

Correlated Alarm Type Scenario 5: Object is in Asset Group

In a Federated environment, the alarms can be published from NOC to all connected sites. While creating a correlated alarm for an asset group, the assets group looked up would essentially be from the NOC site. For referencing the asset groups from all the child sites, you could use **Object Is In Asset Group** by property. This helps looking for asset groups on all sites matching a property value of the asset group.



Property	Operator	Destination
Enabled	Equals	<input checked="" type="checkbox"/>

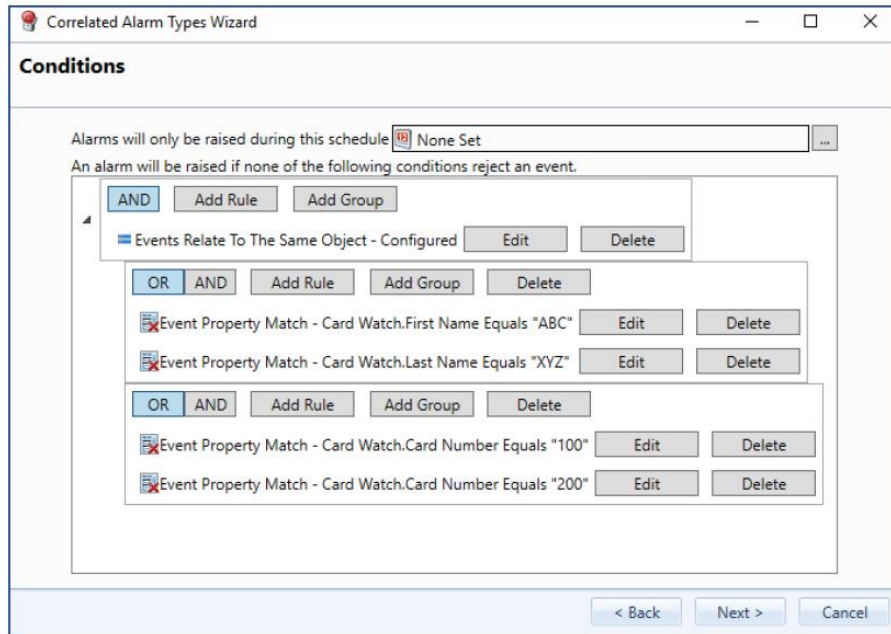
For example, if you have a Door Held event defined on an Object Type, you could configure the alarm to look for all asset groups that are enabled, from all connected sites and raise an alarm if the Door Held event occur from the devices configured with the asset group. Other doors raising the same event will not contribute towards the alarm generation.

The site that owns the device will see an alarm in the alarm stack and is also pushed back to the NOC. If more than one site meets the condition configured in the alarm, the site that generated it will display an alarm in the alarm stack and the NOC will have a collection of alarms from all sites.

Correlated Alarm Type Scenario 6: Events With Conditions

The scenario below is configured to **These events must happen in order** with the following 3 events:

- Door Forced
- Card Watch
- Door Held



It can be further configured by adding more conditions on the conditions page to filter the alarms being created.

Since the first level of the nested condition loop is an AND condition, it is expected that all conditions are necessarily satisfied. An OR condition can be included from second level onwards.

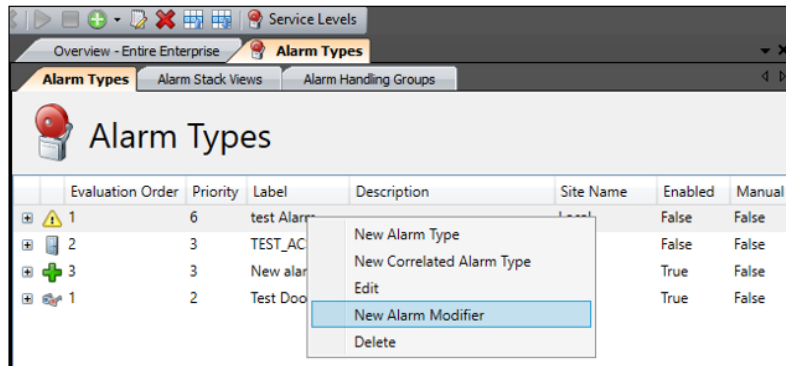
The first condition is linking all events to the same object/device. The nested conditions check for the first/last name and the card number.

A correlated alarm is created if all 3 events are generated and the card watch event can have a first or a last name with card number being 100 or 200.

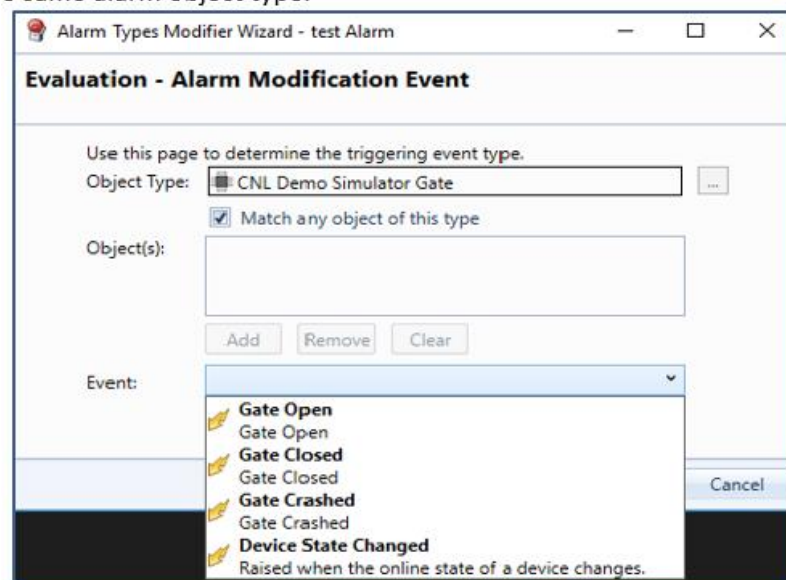
Modifying an Alarm (Alarm Modifiers)

An alarm can be updated as a result of an event being received. A typical usage scenario is to update a Door Held alarm if a door closed event is received. To modify an alarm as a result of an event, create a new Alarm Modifier using the Alarm Modifier wizard.

1. Start by selecting the alarm type in the Alarm Types interface, right-click and select **New Alarm Modifier**. The **Alarm Modifier** wizard opens.

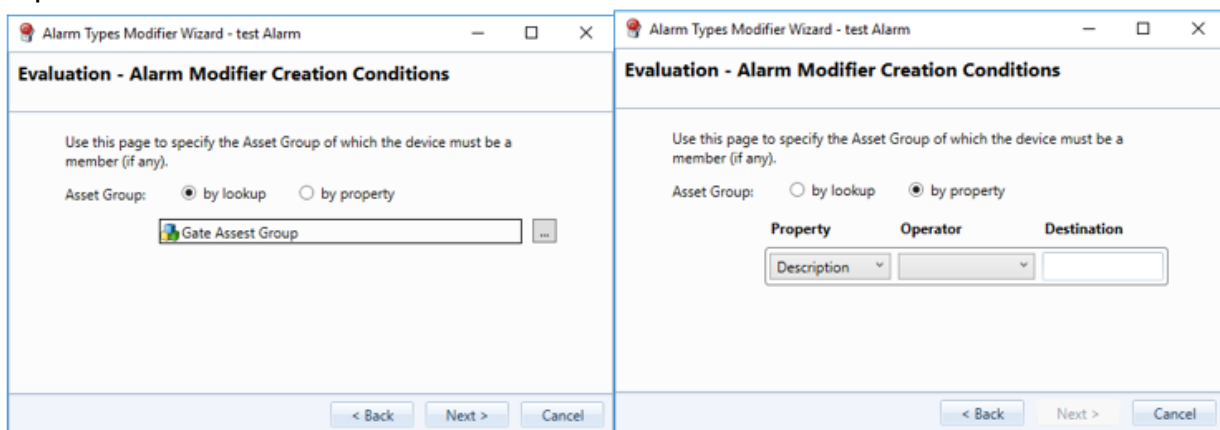


2. **Alarm Modification Event:** In the wizard, specify which event should modify the alarm. Note that the object type will remain the same as the primary alarm, as the alarm modifier created needs to be on the same alarm object type.



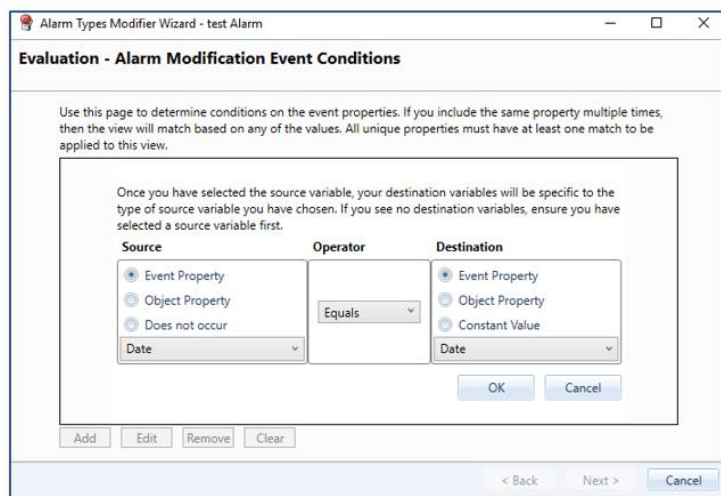
3. **Alarm Modifier Creation Conditions:** This section is used to specify the asset group the device belongs to, if any. You can either, look up for a specific Asset Group or, search by property condition, as shown in the picture below. If the device is not part of any Asset Group, you can click Next to proceed to the next

step.



The object can be linked to the Asset group by searching for various property that defines it.

- Alarm Modification Event Conditions:** This step is to determine the conditions on the event properties/object properties. Click on **Add** to display the above screen. When an option is chosen for the source, the corresponding drop-down menu is shown. The **Does not occur** option monitors if an event does not occur in a certain time period, so you can take relevant action, like increasing the priority of the alarm or displaying a message to the user. Click **OK** to add the condition and then click **Next** to proceed.



- Alarm Property Mapping:** Start by picking the Alarm property from the options available and map it to the event property or a static value and select **OK**. This will modify the Alarm property accordingly when the event with the specified property occurs. Click **Next** to proceed.

The screenshot shows the 'Alarm Property Mapping' step of the 'Alarm Types Modifier Wizard - test Alarm'. The window title is 'Alarm Types Modifier Wizard - test Alarm'. The main heading is 'Alarm Property Mapping'. Below the heading, there is a descriptive text: 'Use this page specify Alarm properties that will be modified with data from the properties in the event if required.' The main content area contains a form with the following elements:

- 'Alarm Property:' dropdown menu with 'Custom Text 1' selected.
- Radio buttons for 'Event Property' (selected) and 'Static Value'.
- 'Event Property:' dropdown menu with 'Device Identifier' selected.
- 'OK' and 'Cancel' buttons.

 At the bottom of the main content area, there are 'Add', 'Edit', 'Remove', and 'Clear' buttons. At the very bottom of the wizard window, there are '< Back', 'Next >', and 'Cancel' buttons.

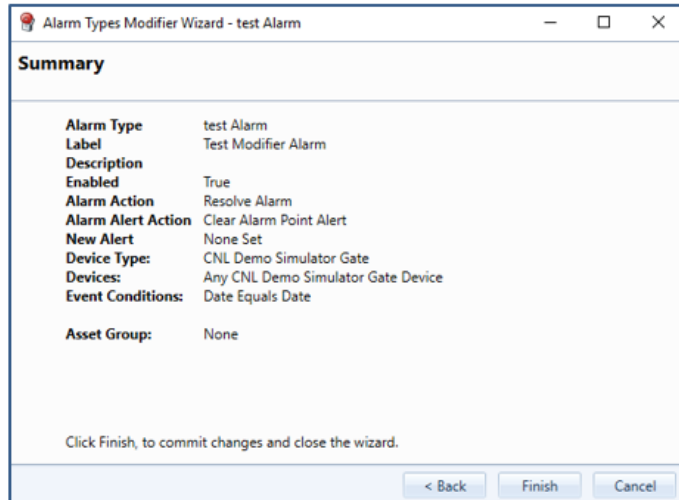
- Alarm Actions:** This is the place to define the actions to be performed on the alarms which meet the modifier criteria. You can choose to Reset, Resolve or Park the Alarm. You can also specify to execute an alert action when the alarm is modified. Alternatively, define a response plan to fire up when the modifier conditions are met. Click **Next** to proceed.

The screenshot shows the 'Alarm Action' step of the 'Alarm Types Modifier Wizard - test Alarm'. The window title is 'Alarm Types Modifier Wizard - test Alarm'. The main heading is 'Alarm Action'. Below the heading, there is a descriptive text: 'Use this page to define actions to be performed on Alarms that match the Modifier criteria.' The main content area contains a form with the following elements:

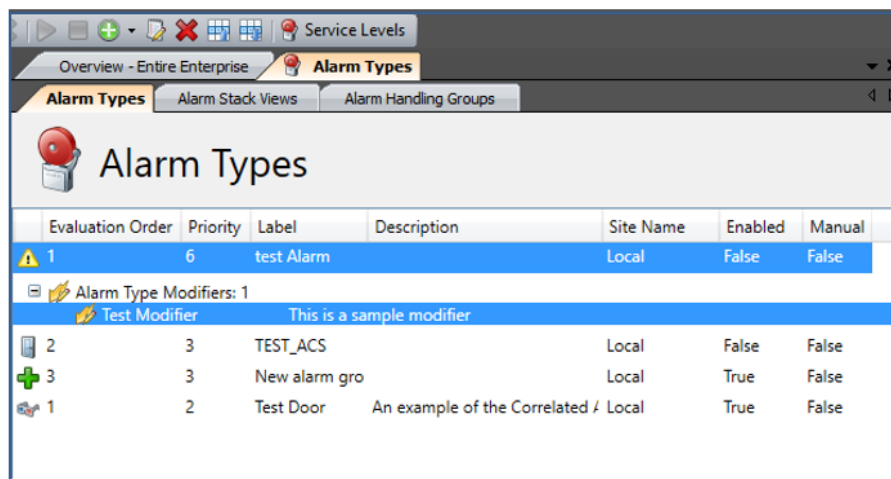
- 'Alarm Action:' dropdown menu with 'Resolve Alarm' selected.
- 'Alarm Alert Action:' dropdown menu with 'Clear Alarm Point Alert' selected.
- 'Response Plan:' text input field with 'None Set' and a small icon to the left, and a three-dot menu button to the right.

 At the bottom of the wizard window, there are '< Back', 'Next >', and 'Cancel' buttons.

- Complete the wizard by verifying the configurations on the **Summary** page and click **Finish**.



The modifier is displayed when you expand the alarm type.



Alarm Type Modifier - Launch Response Plan

You can launch a Response Plan when the conditions of an Alarm Type Modifier evaluate as true. This means that a Response Plan can run without the alarm having to be modified. It can also run if the alarm is modified. The Response Plan that is launched includes a variable pointing to the Alarm ID of the matching alarm.

To link a Response Plan to an Alarm Type Modifier:

1. Open the Alarm Types interface and select the relevant Alarm Type.
2. Expand the Alarm Type and open the new **Alarm Type Modifier** wizard by one of the following ways:
 - Right-click and select **New Alarm Type Modifier**.
 - Right-click an existing **Alarm Type Modifier** and select **Edit**.

	Label	Enabled	Description	Site Name	Manual
1	Safe City - Gunshot	True	Audio analytics have identified a gunshot.	Local	True
2	ANPR White List	True		Local	False
3	VP Visit	True	A VP has arrived on site	Local	True
4	Perimeter Breach	True	Perimeter Breach Detected by PDS	Local	False
5	Video Analytic	False	Video Analytic Event	Local	False
6	Suspended Badge	True	Staff member has called in stating they have misplaced their ACS Card	Local	True
7	Fire - Fault	False	A sensor has gone into fault status	Local	True
8	Fire	True	A fire has been detected in the building	Local	True
9	Perimeter Detection	True		Local	False
10	Perimeter Analytics	True		Local	False
11	Perimeter Detection	True		Site A	False
12	Door State Change	False		Site A	False
13	Federated Site Issue	True		Local	False
13	Door Forced	True		Site A	False
14	Perimeter Analytics Alarm	True		Site A	False
15	Suspended Badge	True		Site A	False
16	Unknown Badge - High Threat	True		Local	False
17	Unknown Badge	True		Local	False
18	Correlated F			Local	False
19	Intruder Ala			Local	True
1	Active Shoo		Active Shooter Onsite	Local	False
2	Correlated Perimeter Attack	True		Local	False
3	Correlated Perimeter Alarm	True		Site A	False

3. On the **Alarm Action** step, change the Response Plan to be launched.

Alarm Action

Use this page to define actions to be performed on Alarms that match the Modifier criteria.

Alarm Action:

Alarm Alert Action:

Response Plan: ...

< Back Next > Cancel

Include Alarm Type Modifier Events in Count of Alarm Events

You can enable Alarm Type Modifier events to contribute to the count of alarm events by modifying the Rules Engine configuration file. To modify the Rules Engine configuration file:

1. Locate the Everbridge.RulesEngine.WindowsService.exe.config file in the following directory:

C:\Program Files (x86)\Everbridge\ControlCenter\ControlCenter Rules Engine

2. In the <appsettings> section of the configuration file, set to the default value to true. For example:

```
<add key="IncludeAlarmTypeModifierEventInAlarm" value="false"/>
```

to

```
<add key="IncludeAlarmTypeModifierEventInAlarm" value="true"/>
```

3. Restart the Control Center services for the changes to take effect. The Alarm Type Modifier events appear in the **Alarm Count** column of the Alarm Stack.

Managing Alert States

An alert state defines a set of visual properties that can be applied to an object. An alert state can be automatically applied to an alarm point related to an alarm.

In addition, alert states can be linked to location types so that when a device creates an alarm, the parent objects implement the alert state as well. You can define which parent location types are alerted when a device creates an alarm. For example, if a door alert is triggered, you can define for it to automatically apply the alert state to the floor, building, and site that own the door.

To create an alert state and generate it against a single object:

1. From **System Configuration**, right-click to select **New > Alert State**. A new alert state is created.
2. Provide an intuitive name for the alert state. Edit the following properties in the **Properties** pane on the right:
 - **Color** – Change the color to the desired color.
 - **Duration** – Change the duration property to the value of 30.
 - **Icon** – Change the icon property to an icon of your choice.
 - **Text** - Provide a simple text string for the Text property on the alert state.
3. Create a Location in System Explorer and add a Geographical (GIS) Scene or Schematic Scene when prompted. The location and scene are added.
4. Add one of the following objects types to the location:
 - Devices

- Placeholder
 - Sub-location (without a scene)
5. In the GIS scene, select the **GIS Layers'** property, and move the **OSM Layer** to the **Scene Layers** list.
 6. Plot the icons by dragging the object from the tree view on the left panel and drag to position on the map. Click **Save** and close the scene.
 7. Configure the System Explorer, so that the map is displayed when a location is selected in System Explorer.
 8. Ensure that the scene that was just configured is displayed in the main display area and expand the location on the system tree such that the items in the location are visible.
 9. From System Configuration, click **Alert Object**. The Control Center **Search Objects** dialog appears. Enter the object or click **Find Now** to locate the object that has already been plotted, and double-click to select it, then click **OK**.
 10. Navigate to the main display area and notice the main display area for the icon of the selected object blinking.



Modify the Alert State for an Alarm

Using the Modify Alarm shape, it is possible to update the alert that applies to an alarm.



It is also possible to clear the alert by setting the alert state property in the modify alarm shape to point to an alert state variable that is empty.

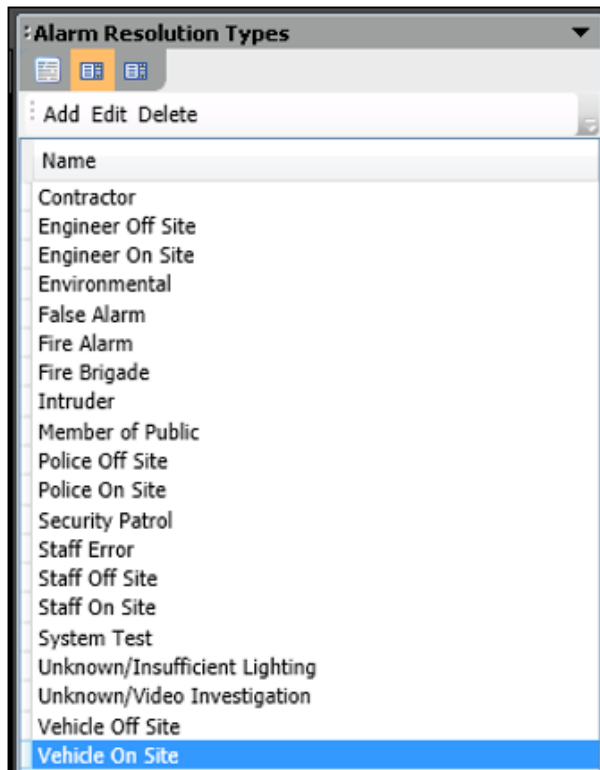
Managing Alarm Resolution Types

Resolution types are used to specify the options available when resolving an alarm, either as an end user or via logic built into the solution.

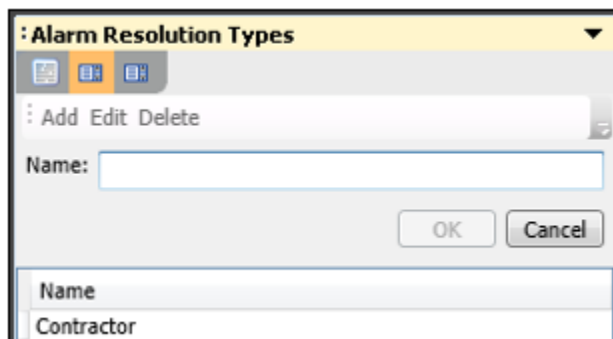
The choices available to resolve an alarm are called resolution types. Control Center has default settings called System Resolution Types. The default resolution types cannot be changed, but new types can be added that can be edited and deleted as required.

To add an Alarm Resolution type:

1. In the **Alarm Types** or **Alarm Stack Views Editor** window > **Properties** window, click **Alarm Stack View**. The default Alarm Resolution Types appear in the properties list.



2. Click **Add** to define a new Alarm Resolution Type. The **New Alarm Resolution Type** dialog opens.



3. In the **Name** field, enter a new resolution name. For example, Equipment Failure.

4. Click **OK**. The new Resolution Type appears in the list in the properties frame.

Editing Alarm Resolution Types

To edit a Resolution Type:

1. From the properties list, select the Resolution Type and click **Edit**. The Resolution Type and its description appear.
2. Edit the **Name** or **Description** and click **OK** to save the changes.

Deleting Alarm Resolution Types

To delete a Resolution Type, select the Resolution Type from the properties list and click **Delete**. The Resolution Type is removed from the list.

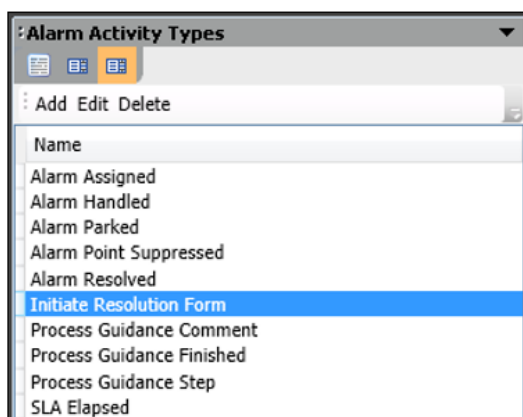
Only user-defined resolution types can be removed. System resolution types cannot be deleted.

Defining New Alarm Activity Types

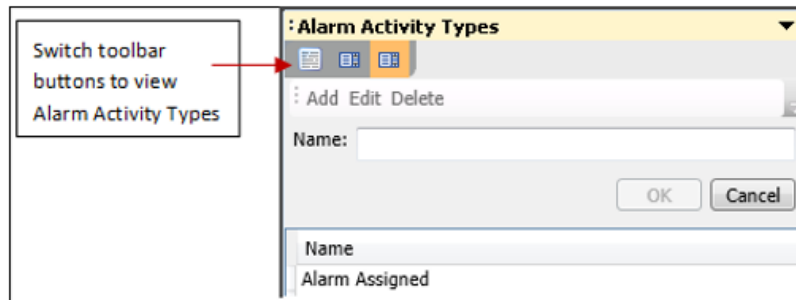
The actions available to resolve an alarm are called Alarm Actions. Control Center comes packaged with default alarm actions and shapes that cannot be edited or deleted but can be added to. However, you can edit and delete custom Alarm Activity Types.

To define a new Alarm Activity Type:

1. Go to **System Configuration** window > **System Objects** folder.
2. Locate the **Alarm Types** folder and double-click to open it.
3. In the **Properties** pane, click the last button to switch to Alarm Activity Types.
4. The Alarm Activity Types appear in the display. The items prefixed with Alarm are the default actions and the other items represent default response plan shapes.



5. Click **Add**. The **New Alarm Activity Type** dialog opens.



6. In the **Name** field, enter a new **Alarm Activity Type** name.
7. Click **OK**.

Editing an Alarm Activity Type

To edit an Alarm Activity Type:

1. In the property list, select the Alarm Activity Type and click **Edit**.
2. Edit the Name or Description and click **OK** to save the changes.

The Alarm Activity Type UI is not case sensitive, that is AbC is considered the same as abc. Therefore, if you try adding the same activity name with a different case, an error message is displayed.

Deleting an Alarm Activity Type

To delete an Alarm Activity Type, select it in the property list and click **Delete**. The Alarm Activity Type is removed from the list.

Changing the Evaluation Order of an Alarm Type

The evaluation order of Alarm Types allows the user to determine the order in which Alarm Type is checked when a new event is processed. Once an event is received, each Alarm Type in the system is checked against the event taking into consideration the location, schedule and conditions of the event. When a match is found, the evaluation of the Alarm Types is halted, and the Alarm Stack is created or updated.

The order in which Alarm Types are evaluated can be determined in the System Alarm Stack by adjusting the order in which they are shown using buttons on the toolbar. Alarm Types are evaluated top down.

This is useful where a specific Alarm Type should be checked before another general Alarm Type. Using the example below, the Alarm Type **Fire Alarm in Server Room** must be evaluated before **Fire Alarm**, otherwise any fire alarm events from the server room are categorized as **Fire Alarms** which is more of a general Alarm Type (and not prioritized appropriately).

Evaluation Order	Alarm Type	Device Type	Event	Location	Schedule
1	Fire Alarm in Server Room	Fire Panel	Fire Alarm	Server Room	Any
2	Fire Alarm	Fire Panel	Fire Alarm	Any	Any

To re-order alarms:

1. Click the Alarm in the Alarm Types Editor to select it.
2. Click the **Move Up** button in the toolbar. The alarm is promoted one level.
3. Click the **Move Down** button in the toolbar. The alarm is demoted one level – to its original position.

Define Default Service Level Agreements

Service Level Agreements set the schedule for the visible and audible reminders to bring new alarm events to an operator’s attention.

Service Levels have three stages (or levels) set with 10, 20, and 30 second response times that can be configured.

To define Service Levels Agreements for Alarm Types:

1. In the Toolbar, click **Service Levels**. The **Default Service Level Agreements** wizard appears.

2. Select the appropriate tab to set the conditions for each Service Level Agreement.
3. Specify the properties for the following fields:

- **Enable/Disabled** – Enables or disables the default service level agreements for the various levels.
- **Duration** – The up/down arrows to specify the interval (in seconds) after the alarm creation that the selected Service Level represents.
- **Override Icon** – When selected, the alarm icon that appears in the Alarm Stack View is overridden once the Service Level Agreement is initiated..
- **Fore Color** – The foreground color for the Alarm Stack row to highlight an alarm's status to users.
- **Back Color** – The background color for the Alarm Stack row to highlight an alarm's status to users.
- **Font** – The font of the text in the Alarm Stack row to highlight an alarm's status to users.
- **Response Plan** – The response plan to be executed when the service level is enacted.
- **Audio Alert** – When an alarm is enacted the Service Level Agreements can play an audio alert to all logged in users. Users will hear the highest priority alert based on their alarm stack view configuration. Audio should be in .wav or .mp3 file formats.

When audio is selected, the following additional options are displayed:

- **Loop Audio** – When selected, the audio alert will play on repeat until stopped.
- **Stop Looping** – Looping audio alerts always stop playing when the alarm is resolved. Additional stopping points can be added to stop audio when the alarm is handled or parked. See [Configuring Audio Alert Snoozing](#) for information on related functionality.

Click **Save** to save the Service Level Agreement.

Example

An alarm is raised. The alarm appears in the Alarm Stack as black text against white background with the PTZ icon to indicate the type of alarm.

After 20 seconds, the alarm in the Alarm Stack appears as black text against a yellow background with a PTZ camera icon. A beep sounds on the operator's workstation.

After 30 seconds, the alarm in the Alarm Stack appears as yellow text against a red background, a beep sounds, and an SMS message is sent to the operator's mobile phone.

If the response plan associated with the Service Level Agreement does not have the alarm variables, they are added when the dialog is closed.

Audio Alert Prioritization

If multiple active alarms have configured audio alerts Control Center will prioritize them, playing audio for the oldest, highest priority alarm visible to the user.

Once that alarm audio is silenced – either when the audio is finished in the case of non-looping alerts, or when the configured stopping point is reached for looping audio alerts – the system will automatically play audio of the next alarm based on priority.

If a new alarm is raised that is of higher priority than an existing alarm the system will switch the audio to this alarm.

Configuring Audio Alert Snoozing

A default snooze button, and an indicator of the currently audible alarm is available as part of the Alarm Stack Grid component.

✓	ID	Priority
■	111056	2
■	111059	3
■	111057	4
■	111058	4

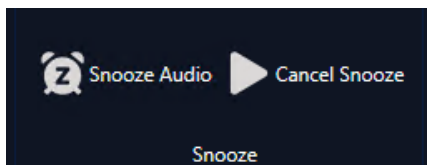
This is switched off by default but can be enabled via by a configuration option – **Show Snooze Buttons** – on the grid component in the GUI editor.

You can also configure a snooze button in the Main Menu that will temporarily mute an active audio alert via a snooze function in the Alarm Stack Grid GUI component.

```
My.SystemVariables.[Current Gui].alarmStackGrid1.SnoozeAudioAlert()
```

A separate function can be used to resume audio alerts.

```
My.SystemVariables.[Current Gui].alarmStackGrid1.ResumeAudioAlert()
```



By default, alarm audio will be snoozed for fifteen minutes before resuming; this can be changed via a new Global Setting found in the Alarm section of Enterprise Settings:

^ Alarm	
Alarm Attachment Maximum Size (MB)	10.00
Alarm Snooze Duration (In Minutes)	15
Client Side Alarm Notifications Batch Size	30

Configuring Alarm Attachments

You can use the Alarm Attachments Viewer control to add attachments to alarms.

Attachments can be media already in Control Center or external files. External files that you attach are stored in **System Configuration > Systems Objects > Alarm Media > alarm_id** where *id* is the alarm ID.

You must have type permissions to be able to add and view alarm attachments. See [Type Permissions](#) for more information.

You can configure a maximum file limit for attachments in **System Configuration > Global Settings > Enterprise Settings > Alarm Attachment Maximum Size**.

To enable operators to add attachments to alarms, you can:

- Add the Alarm Attachments Viewer control to a GUI and configure a display area for the GUI. See [Graphical User Interfaces](#) for more information.
- Configure a response plan to display the Alarm Attachments Viewer

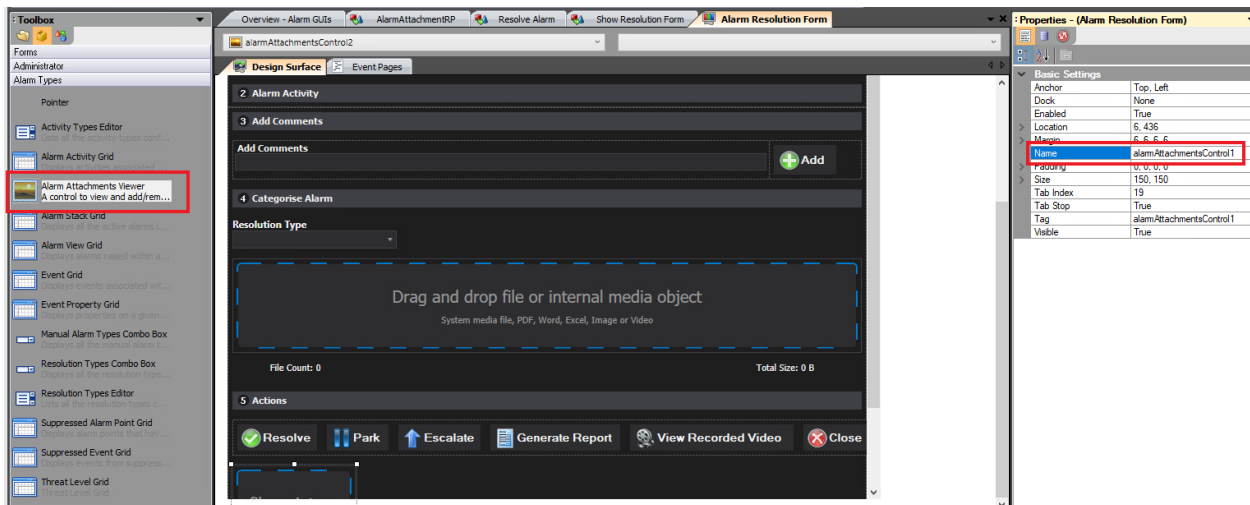
The following example describes how to add an alarm attachment display area to your **Alarm Resolution Form**.

1. Go to **System Configuration > My Organization > Modules > Alarm Processing > Alarm GUIs**.
2. In the **Response Plan** area, double-click the **Show Resolution Form** response plan to open it.
3. Double-click the **Setup the resolution form Part 1** shape.
4. Add the following line:

```
My.PageVariables.ResolutionForm.alarmAttachmentsControl1.SetFriendlyAlarmId(My.PageVariables.AlarmID)
```

where `alarmAttachmentsControl1` matches what you have in the **Name** property of your Alarm Attachment Viewer control.

5. Save and close the response plan.
6. Go to **System Configuration > My Organization > Modules > Alarm Processing > Alarm GUIs**.
7. From the **Graphical User Interface** area, double-click the **Alarm Resolution Form** GUI to open it for editing.
8. From **Toolbox**, expand **Alarm Types**.
9. Drag the **Alarm Attachments Viewer** control to the **Alarm Resolution Form**.



10. Save and close the **Alarm Resolution Form** GUI. An operator can now view and add attachments when handling an alarm. See [Adding Alarm Attachments](#).

Configuring Track Classification When Handling Alarms

When you handle an alarm from a track, the alarm defaults to the current track classification that you have configured for the track. You can use the **Track Classification** control to change the classification.

You cannot create new classifications. You can only select from your existing classifications. You can define new classifications in **System Configuration**. See [Track Display](#).

Initially, when an alarm is raised, the current track classification is displayed in the **Track Classification** control. A drop-down list displays all the classifications that are available in Control Center. An operator can decide to keep the existing classification or change the classification, depending on their requirements.

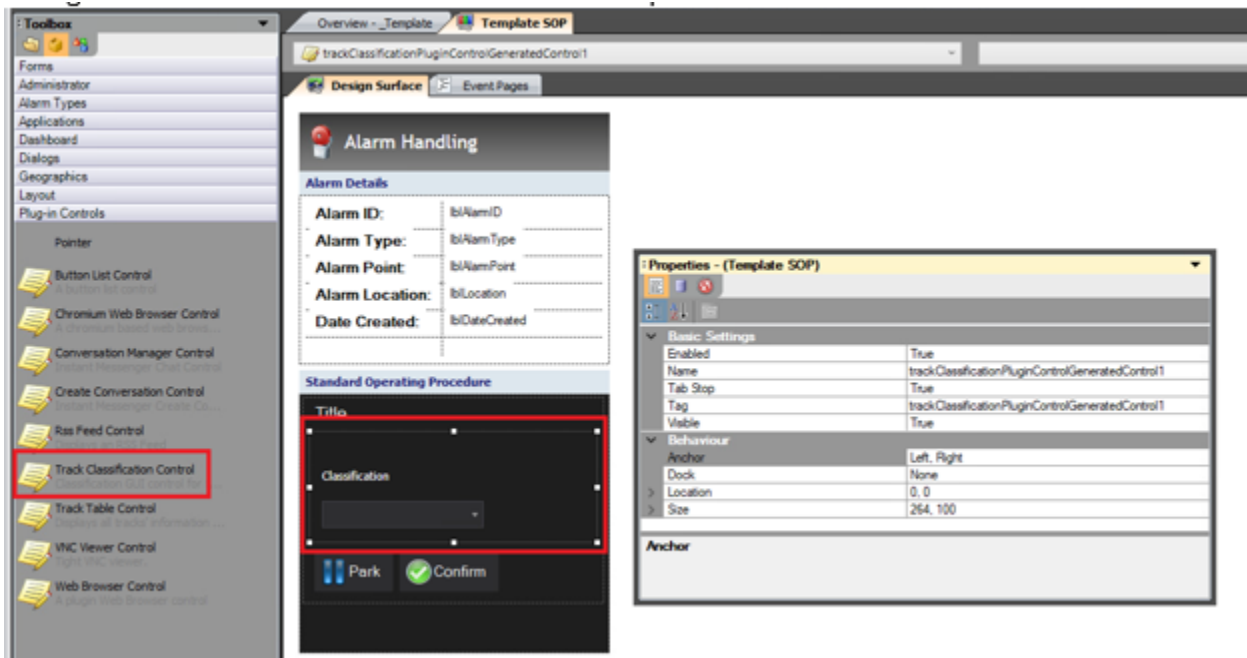
You must have type permissions to handle alarms. See [Type Permissions](#).

To enable operators to specify track classifications when handling alarms, you can configure a response plan to display the **Track Classification** control.

The following example describes how to add a Track Classification control to your Alarm Processing.

1. Go to **System Configuration > My Organization > Modules > Alarm Processing > Alarm SOP**.
2. From the **Graphical User Interface** area, double-click the **Template SOP GUI** to open it for editing.
3. From **Toolbox**, expand **Layout**.
4. Drag a **Panel** control between the control labelled **Standard Operating Procedure** and the panel below it.

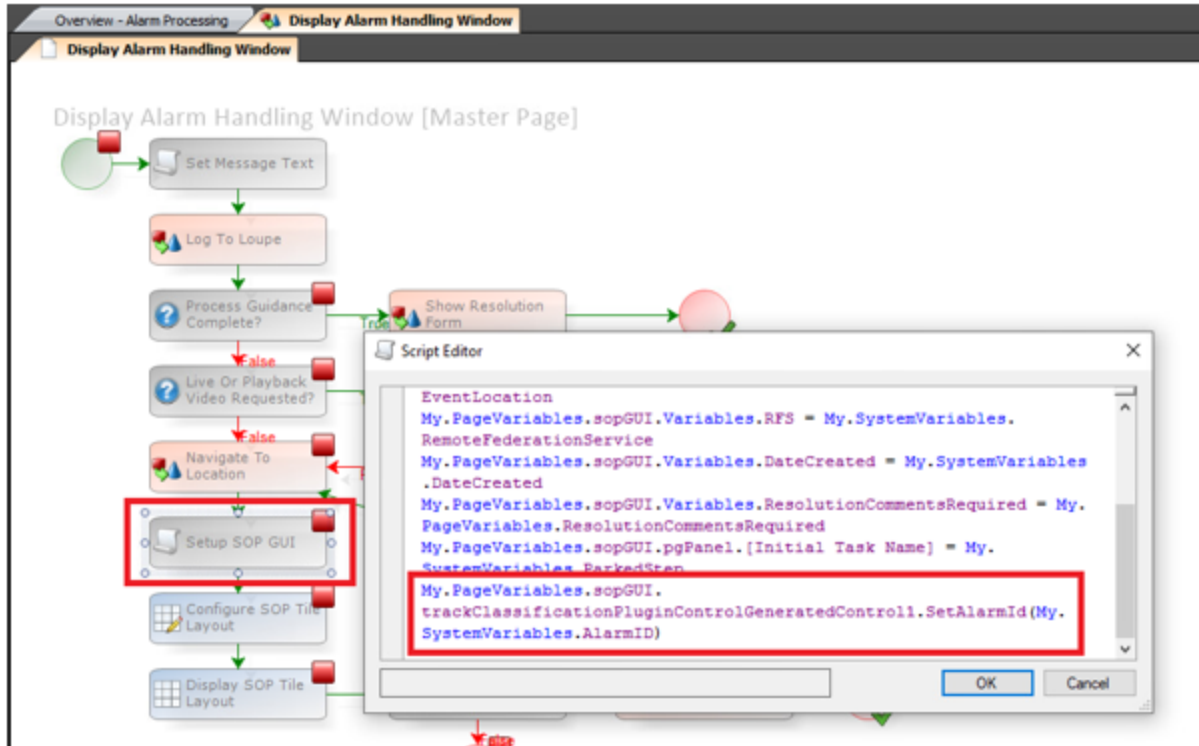
5. From **Toolbox**, expand **Plug-In Controls**.
6. Drag the **Track Classification** control to the new panel.



7. Save and close the **Template SOP GUI**.
8. Go to **System Configuration > My Organization > Modules > Alarm Processing**
9. Double-click the **Display Alarm Handling Window** response plan to open it for editing.
10. Double-click the **Setup SOP GUI** shape.
11. Add the following line:

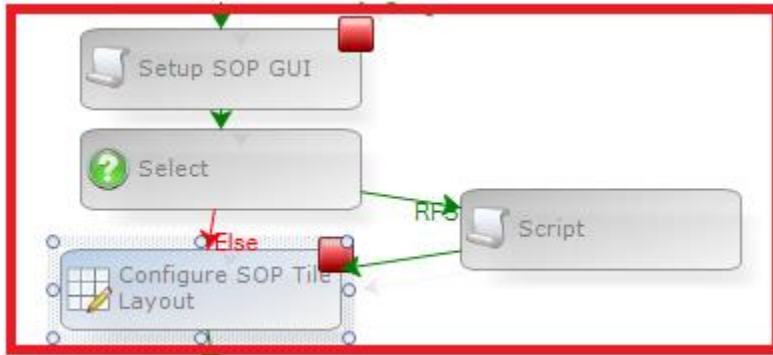
```
My.PageVariables.sopGUI.trackClassificationPluginControlGeneratedControl1.SetAlarmID(My.SystemVariables.AlarmID)
```

where `trackClassificationPluginControlGeneratedControl1` matches what you have in the **Name** property of your **Track Classification** control.



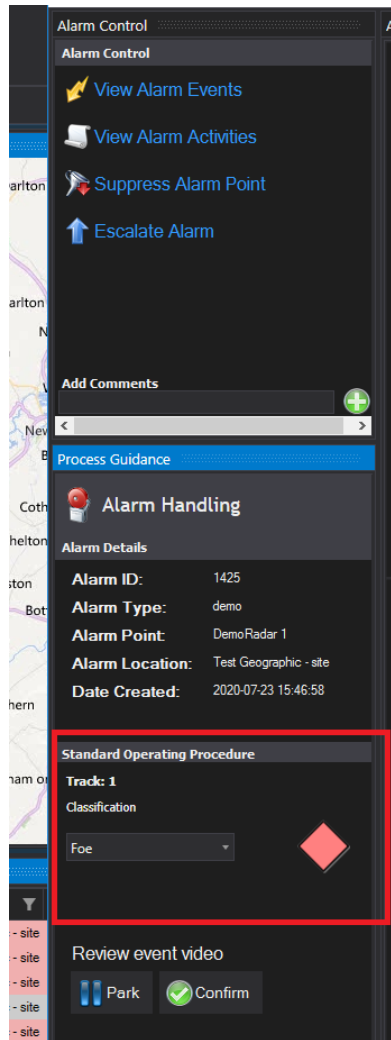
12. If you are handling an alarm from a track in a federated system, then you are not allowed to change the track classification. The following steps describe how to configure the **Display Alarm Handling** window so that the **Track Classification** control is not displayed, if the alarm is a federated alarm.

- a. From **Toolbox > Basic**, add a **Select** shape after the **Setup SOP GUI** step.
- b. Double-click the step to open it. Add a variable as follows:
 - **Label:** Type a name of your label, for example, RFS.
 - **Type:** Remote Federation Service
 - **Scope:** Page
- c. From **Toolbox > Basic**, add a **Script** shape. Connect the **Select** step to the **Script** step.
- d. Double-click the **Script** shape to edit it.
- e. Add the following line: `My.PageVariables.sopGUI.trackClassificationPluginControlGeneratedControl1.Visible=False`
- f. Connect the **Else** connector to the **Configure SOP Tile Layout** shape.



13. Save and close the response plan.

14. When an operator handles an alarm raised on a track, for example, by right-clicking an asset on your map and selecting **Handle Alarm** or by double-clicking an alarm in your Alarm Stack, when the Alarm Handling window is displayed, the **Classification** drop-down list is available.



Alarm Stack Views

Views that define filtering, grouping and sorting can be assigned to users and user groups. The System Alarm Stack Grid then shows the appropriate alarms with the specified formatting to that user based on the views available against an alarm (multiple Views will be shown in tabs across the top of the alarm stack grid).

Creating an Alarm Stack View

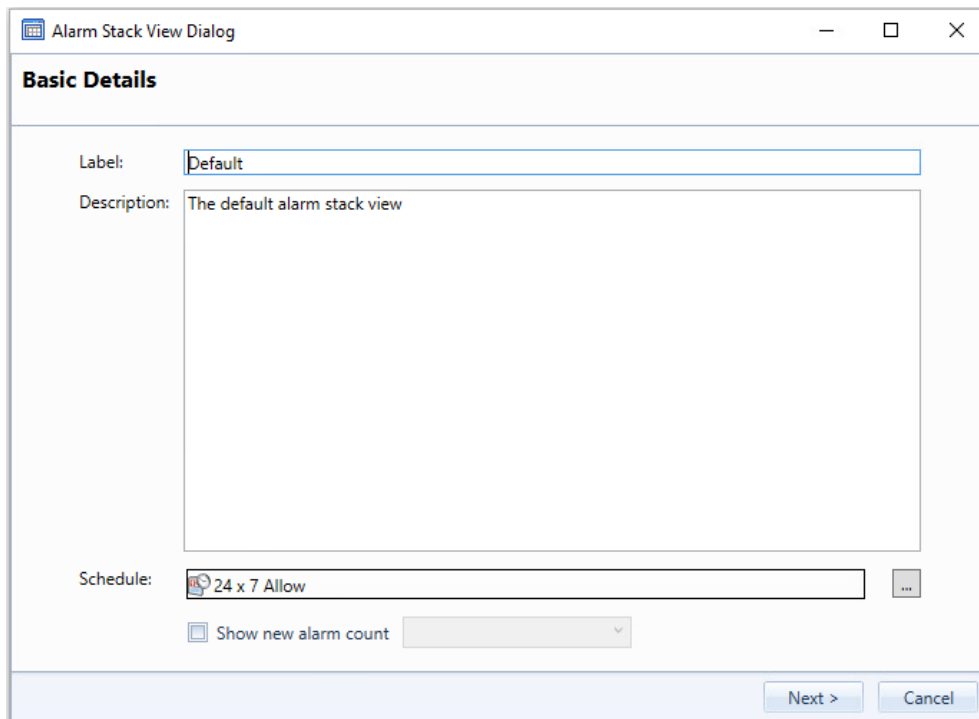
To display business-specific alarms to different users or groups, create a customized Alarm Stack View for each user or group. To create a new Alarm Stack View:

1. Open **System Configuration > System Objects**. The **Overview- System Objects** pane appears.
2. Double-click **Alarm Types** to view the **Alarm Stack Views** window. The **Alarm Types** editor appears.

- Click the **Alarm Stack Views** tab. The **Alarm Stacks Views** editor appears.



- To create a new alarm stack view, click **New** in the toolbar. Alternatively, right-click the **Alarm Stack Views** editor and select **New**. The **Alarm Stack View** wizard appears displaying the **Basic Details** page.



- Enter a label, for example **Test Alarm Stack View** and enter a description.
- Configure the alarm view to be visible at specific times by selecting a schedule. By default, the view is configured to be visible 24 x 7, therefore, you can provide a solution where an entire collection of alarms (a view) becomes hidden or available to a control room based on the time of day.



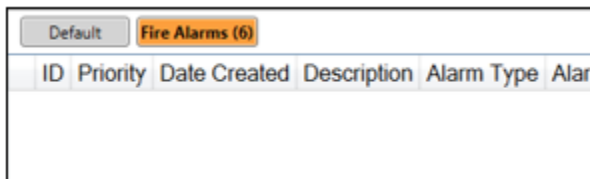
For example, when the working day ends for a satellite control room and the operators go home, then the alarms can be automatically reassigned to a central control room.

In addition to the schedule property of a view, which determines the enabled state of the view, a response plan shape is provided to set the enabled state of a view. The

schedule option can be used to commission logic to control views for operators and could be used to provide override options to the schedule. When a view is not available, any users, user groups, or clients specified in the view will be shown a message.



7. Select the **Show new alarm count** check box to show the number of active alarms in the tab and to select a color for the alarm count text. The **Alarm Stack View** tab displays the number of unique alarms to view and the specified color when there are new alarms in the view.



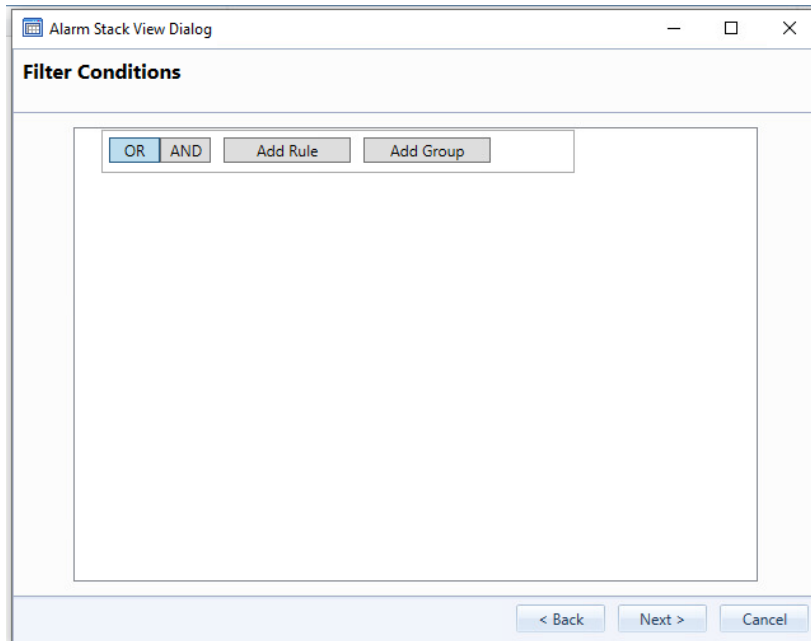
8. Click **Next**. The **Query** page appears.

Alarm Stack Views could include Supervisor View, Operator View, Maintenance View, Head of Security View, and so on.

Alarm Stack View Filter Conditions

The **Filter Conditions** page displays all the filters for the alarms to appear in the Alarm Stack View. When configuring which alarms to show in an Alarm Stack View, you can create comprehensive filters using the **Filter Conditions** dialog.

No criteria are required to filter unhandled alarms as by default, they are automatically included.



When the Filter Conditions dialog is first displayed, you can perform the following actions:

- Choose an Evaluation Operator (OR & AND)
- Add a Rule to the current Group
- Add a new Group as a Child of the current Group

Choosing an Evaluation Operator

The Filters Conditions page enables commissioning users to construct filters where each of the rules can be evaluated against the selected operator. You can add new lines for the filter using Add Rule.

For example, in the below example, the OR evaluation operator is selected, and three new rules are added. Alarms will be included in the Alarm Stack View if the following conditions are met:

- Priority less than or equal to 6, OR
- SLA Level equals 1, OR
- Alarm Point is Security Operations Center

Filter Conditions

<input type="radio"/> OR	<input type="radio"/> AND	<input type="button" value="Add Rule"/>	<input type="button" value="Add Group"/>
Priority	LessThanEqu	6	Delete
SLA Level	Equals	1	Delete
Alarm Point	Equals	Security Operations	Delete

Multiple instances of the same column can match values specified under (OR). Unique columns must match all specified values under (AND).

In the following example AND is selected as the evaluation operator. Alarms will be included in the Alarm Stack View, if the following conditions are met:

- Priority less than or equal to 6, AND
- SLA Level equals 1, AND
- Alarm Point is set to Security Operations Center

Filter Conditions

<input type="radio"/> OR	<input checked="" type="radio"/> AND	<input type="button" value="Add Rule"/>	<input type="button" value="Add Group"/>
Priority	LessThanEqu	6	Delete
SLA Level	Equals	1	Delete
Alarm Point	Equals	Security Operations	Delete

Alarm Stack Views setup this way will include fewer alarms than the previous example as the conditions are more constrained. You can also include conditions that evaluate the same property multiple times for different values. For example:

Filter Conditions

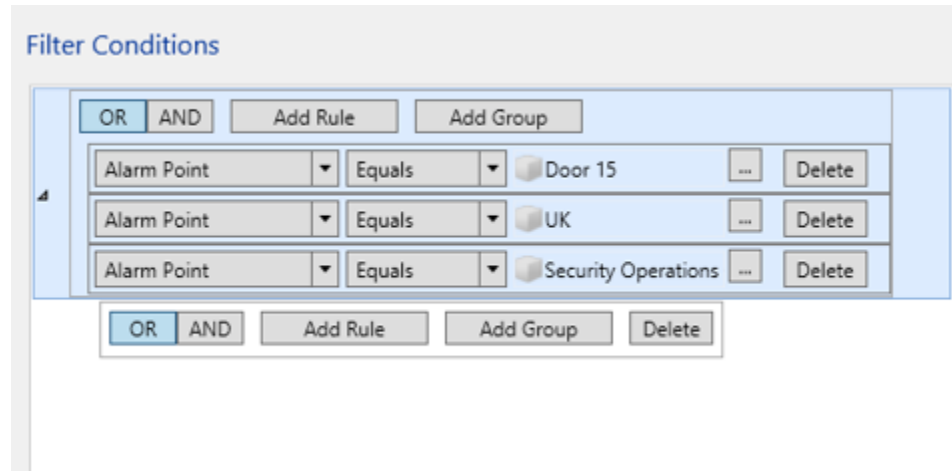
<input type="radio"/> OR	<input type="radio"/> AND	<input type="button" value="Add Rule"/>	<input type="button" value="Add Group"/>
Alarm Point	Equals	Door 15	Delete
Alarm Point	Equals	UK	Delete
Alarm Point	Equals	Security Operations	Delete

In the above figure, alarms will only be included if the Alarm Point is either Door 15, UK, or Security Operations Centre.

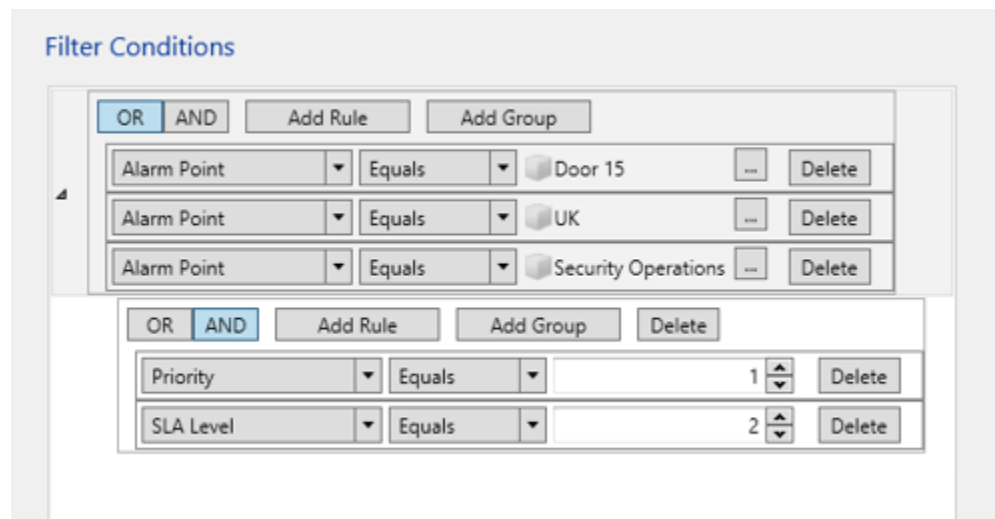
Since there is no logic present to allow Control Center to sense-check these filters, you can construct a Filter where the AND operator is applied to the conditions (similar to the above figure), which will result in no alarms being shown in the Alarm Stack View.

Using Child Groups with Filters

To allow construction of more complex Filters, the Commissioning Engineer can add Groups to the Filter Conditions by using the Add Group button.



After adding a Group, you can add an Evaluation Operator and Rules. When a Group is added, the Group of conditions are evaluated based on the Evaluation Operator chosen for the Group, then the result of the Group evaluation is added to the parent and then the parent Evaluation Operator is applied.



Group logic is always evaluated first. Therefore, for in the above figure, the logic for including an Alarm in this Alarm Stack View is as follows:

- Priority equals 1, AND
- SLA Level equals 2

You can then evaluate using the following Parent Logic:

- Alarm Point equals Door 15, OR
- Alarm Point equals UK, OR
- Alarm Point equals Security Operation

Therefore, an Alarm for any Alarm Point with the Priority set to 1 and SLA Level set to 2 will always be included. In addition, an Alarm with any Priority and any SLA Level for Alarm Points Door 15, UK, or Security Operations will be included.

Filter Conditions

OR	AND	Add Rule	Add Group
Priority	Equals	1	Delete
SLA Level	Equals	2	Delete

OR	AND	Add Rule	Add Group	Delete
Alarm Point	Equals	Door 15	...	Delete
Alarm Point	Equals	UK	...	Delete
Alarm Point	Equals	Security Operations	...	Delete

In the above figure, as the Groups are in reverse order, an alarm must now meet different conditions before being included in the Alarm Stack View.

- Alarm Point equals Door 15, OR
- Alarm Point equals UK, OR
- Alarm Point equals Security Operations
- This is then evaluated with the Parent Logic:
- Priority equals 1, AND
- SLA Level equals 2

In this example, an Alarm for any Alarm Point with the Priority set to 1 and SLA Level set 2 will only be included if the Alarm Point is Door 15, UK, or Security Operations.

You can also nest Child Groups inside each other and add any number of Child Groups to the selected parent as shown in the following example:

The screenshot shows a 'Filter Conditions' window with the following structure:

- Top level: **AND** (selected), Add Rule, Add Group.
 - Priority Equals 1 (Delete)
 - SLA Level Equals 2 (Delete)
- Second level: **OR** (selected), Add Rule, Add Group, Delete.
 - Alarm Point Equals Door 15 (Delete)
 - Alarm Point Equals UK (Delete)
 - Alarm Point Equals Security Operations (Delete)
- Third level: **AND** (selected), Add Rule, Add Group, Delete.
 - Custom Int1 Equals 2 (Delete)
 - Custom Text1 Equals Priority (Delete)

In the above figure, Alarms will be included in this Alarm Stack View only if:

Custom Int1 equals 2 AND Custom Text 1 equals Priority

AND

Alarm Point is Door 15 OR UK OR Security Operations

AND

Priority equals 1

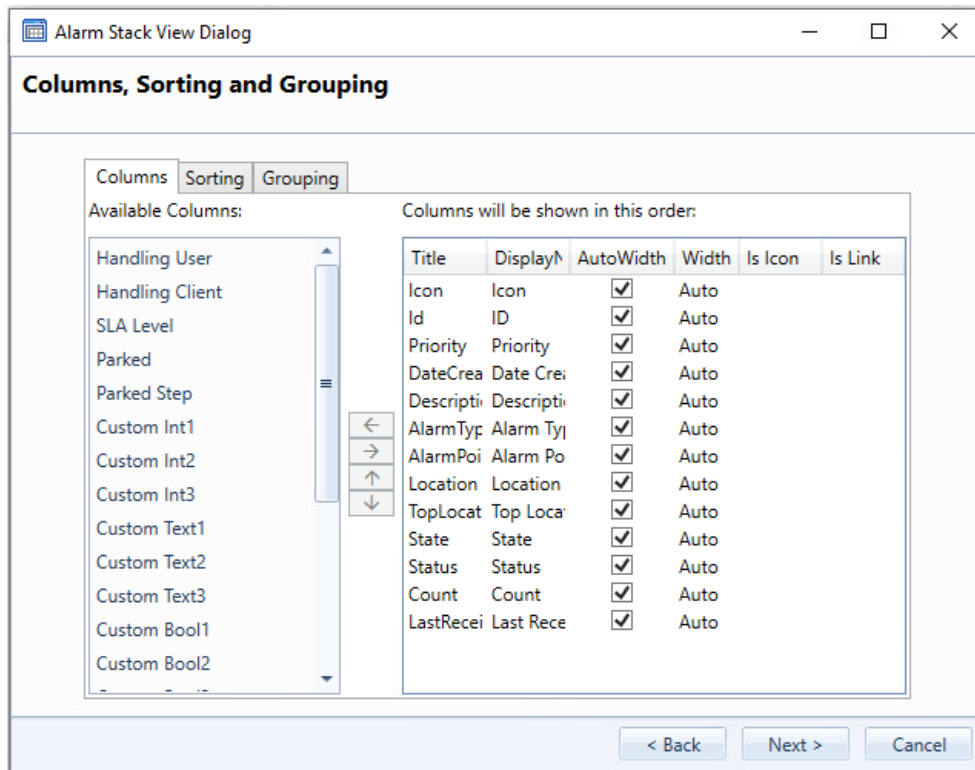
AND

SLA Level equals 2

It is necessary to restart the Client if any changes are done to the Default SLA. The changes will be saved but are not applied in the alarm stack unless the client is restarted.

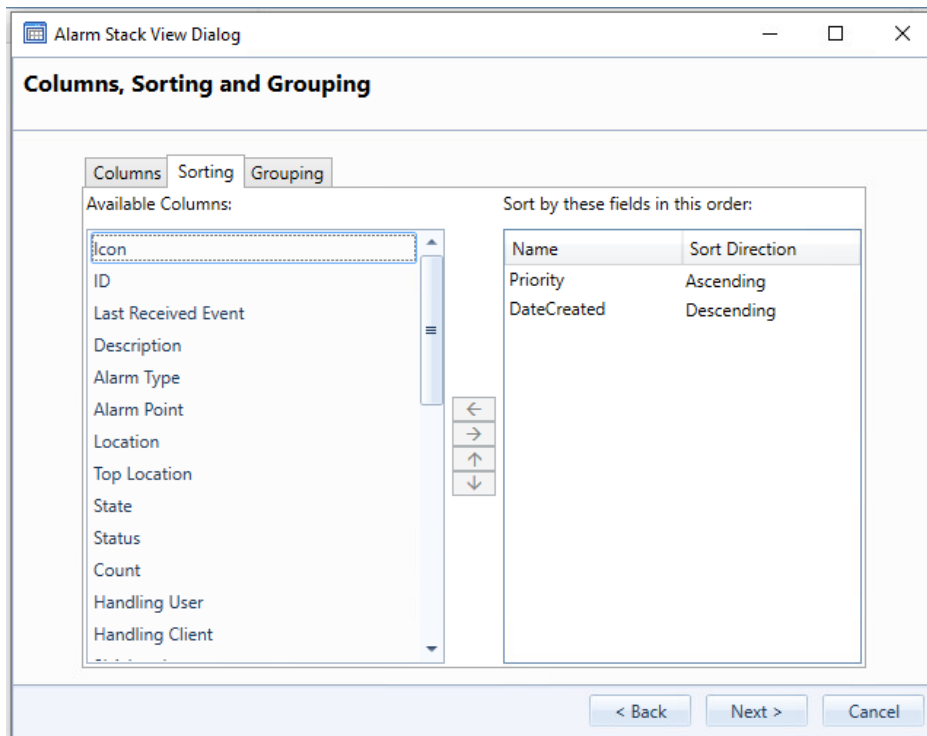
Columns, Sorting and Grouping

The default columns for the Alarm Stack View are listed in the **Columns** tab > Right Pane. Additional fields for available event data are listed on the left.



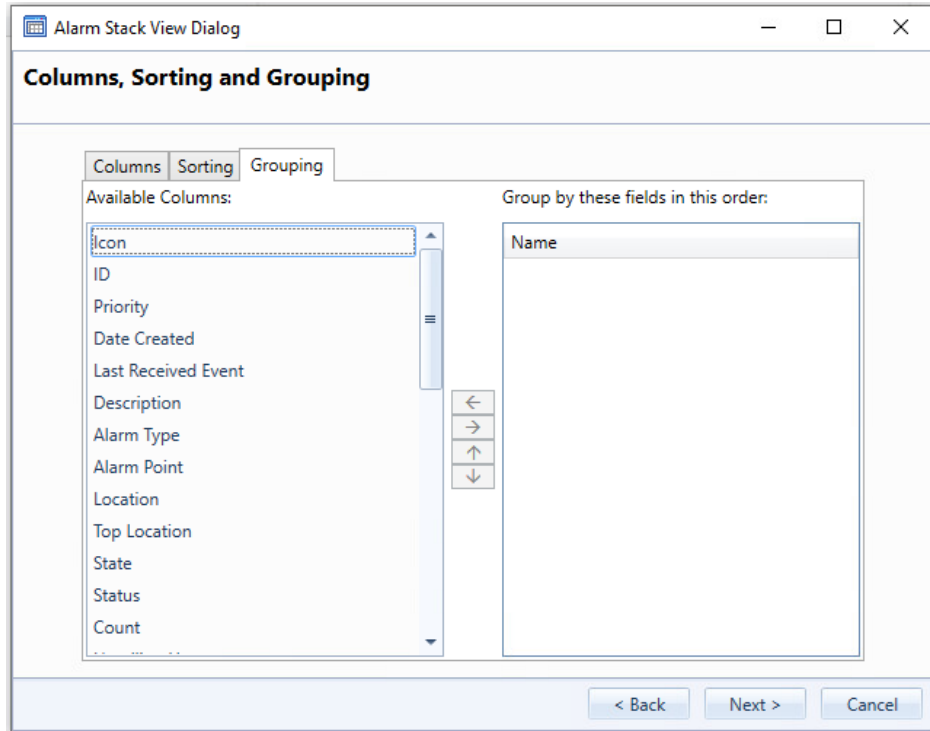
To select a new column for the Alarm Stack View:

1. Select the SLA Level from **Available Columns**. To move the available **Columns will be shown in this order** box, click the right arrow. SLA Level now appears at the bottom of the list in Columns and is available in the list on the right.
2. Use the Up and Down arrows to arrange the fields in the order you want them to appear in the Alarm Stack View. Sorting alarms in the Alarm Stack View determines the order in which they appear.
3. Click the **Sorting** tab. The **Sorting** tab appears with the **Available Columns** on the left. The current sorting is displayed on the right. By default, the sorting is based on Priority and DateCreated.



Grouping alarms allows alarms to appear in the Alarm Stack grouped together in a collapsible section. For example, alarms could be grouped by priority, location, status or date.

4. Leave the default settings for Sorting as-is and click the **Grouping** tab. The **Grouping** tab appears with the **Available Columns** on the left. The current grouping is displayed on the right.



5. Click **Priority in Available Columns** and click the right arrow to move it to the group by these field in this order field. Priority now appears in the right field. In the Alarm Stack, alarms are displayed grouped together by Priority in a collapsible section. Operators click the section to reveal all Priority 1 alarms, for example.
6. Click **Next**. The **Viewers** page appears.

Alarm Stack View Columns

The existing DateCreated and LastReceivedEvent columns within the Alarm Stack Columns continue to display the time and date that the Alarm was created and updated relative to the local user Time and Date settings.

In addition, a commissioning user can add the following columns to an Alarm Stack:

- **Date Created (UTC)** – Displays the time and date that the Alarm was created using UTC time.
- **Date Created (Origin)** – Displays the time and date that the Alarm was created at the Location where the Alarm originates from.

The **Date Created (Origin)** column converts the time recorded for the Alarm Creation within Control Center and uses the Time Zone property for the Location associated to the Alarm to adjust the time shown.

The time of the Alarm creation is the time that the Alarm was created in Control Center. This is not the time that the event triggering the Alarm was first created, unless it is

explicitly supported by the device sub-system and the Control Center connector used to communicate with the device.

The **Date Created (Origin)** column checks the Location associated to the Alarm for a Time Zone, where a location has no Time Zone configured, all parent locations will be checked and the Time Zone of the first parent that has a value configured will be used. Where no Time Zone can be established, the time will be shown as UTC.

In a Federated environment where a Hub Site receives the Alarm from a Node site, the time created is the time that the Node Server, which owns the Alarm, created the Alarm instead of the time when the Hub received the Alarm.

Location Filter

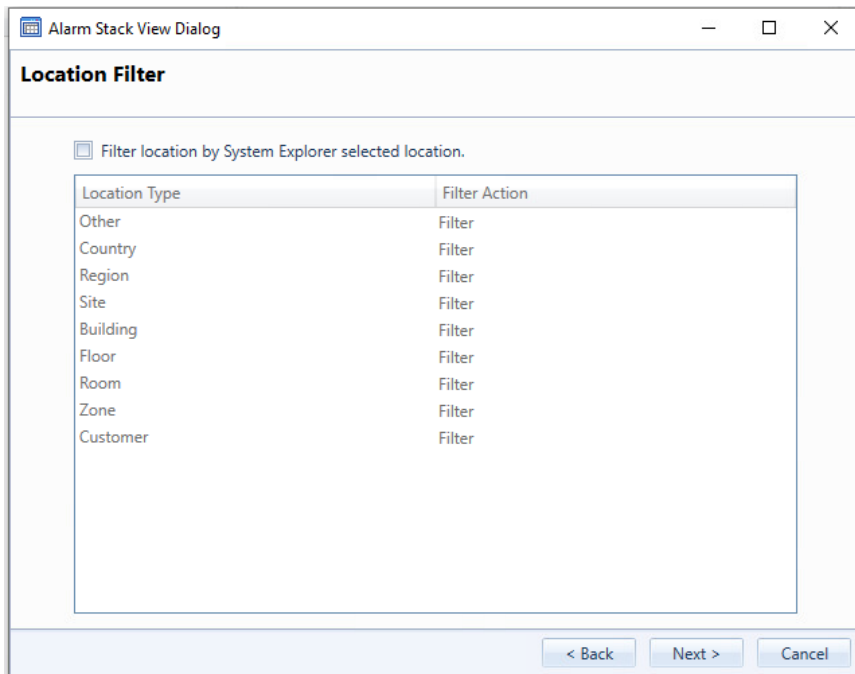
When working with many locations, it is useful to view the Alarms associated with the individual location. Filtering the Alarm Stack View on Alarm Point is currently possible however, this requires the user to enter a value to filter on.

Alarm Stack Views support Location Filtering using an Alarm Stack View that dynamically updates with alarms based on the Location currently selected in the visible System Explorer Tree. Location Filtering displays alarms in the Alarm Stack where the Location of the Alarm has been selected in the System Explorer Tree.

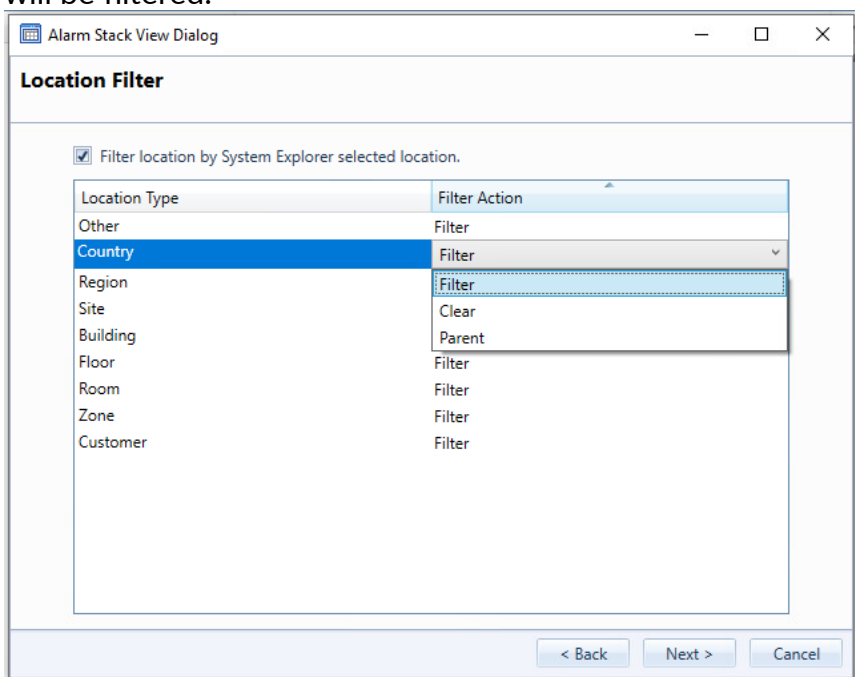
When an Alarm Stack is displayed based on location filter setting, the Alarm Alert States are normally filtered to display only those alerts that are applied to the Location selected currently. That is, the presence of a Location Filtered Alarm Stack will restrict the display of Alarms to the selected Location even if the Location Filtered Alarm Stack is currently not selected.

The System Explorer tree count of Alarms (where configured) updates accurate counts of alarms for every Location regardless of which Location is selected.

This new behavior is configured within the Alarm Stack View Dialog Location Filter Page. By default, Location Filtering is not enabled for a new Alarm Stack View.



Enable Location Filtering on this panel to configure how Alarms from the selected site will be filtered.



Alarm Stack View Location filtering is based upon Location Types and for each Location Type there are three possible Filter Actions.

Action	Description
--------	-------------

Filter	If selected, when a Location of that Type is selected in the System Explorer, all Alarms for that Location will be shown in the Alarm Stack.
Parent	If selected, when a Location of that Type is selected in the System Explorer, the Alarm Stack will find the Parent Locations for that Location until a Location is found where the Location Type is set to Filter. The Alarm Stack displays all the Alarms for that Parent location. For example, when a user selects a location within a Site (a building) the Alarm Stack will display all the alarms for that Site. Equally if a Floor within a Building is selected, the Alarm Stack can display all the alarms for that Building.
Clear	If selected, when a Location of that Type is selected in the System Explorer, a blank Alarm Stack appears.

Consider the following Site Location Structure:

System Explorer for Site

- Globe (Location Type - Other)
- Europe (location Type - Region)
- UK (Location Type - Country)
- Headquarters (Location Type - Site)
- Building 1 (Location Type - Building)
- Floor 1 (Location Type - Floor)
- Floor 2 (Location Type - Floor)
- Device 1 (A device that generates an Alarm)
- Floor 3 (Location Type - Floor)
- Device 2 (A device that generates an Alarm)
- Building 2 (Location Type - Building)

Location Filter Scenarios

Scenario 1 - Devices 1 and 2 generate alarms - Location Filtering Set to Clear

With the Location Filtering enabled in the Alarm Stack View and set to Clear for all Location Types, selecting any location in the System Explorer results in an empty Alarm Stack.

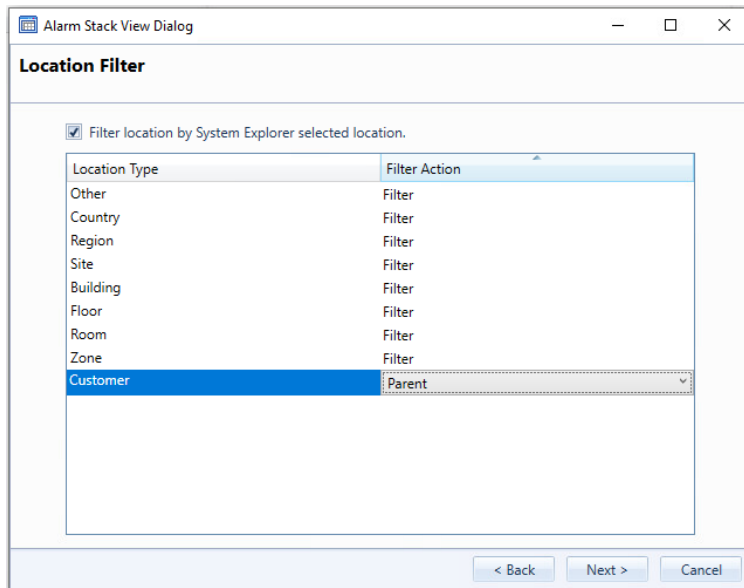
Scenario 2 - Devices 1 and 2 generate alarms - Location Filtering Set to Filter on all Types

With the Location Filtering option set to Filter for all Location Types, selecting any Location in the System Explorer results in the Alarm Stack only showing the Alarms for the selected Location. Therefore, selecting Floor 2 means that Alarms from Device 1 is shown in the Alarm Stack. Selecting Floor 3 means that Alarms from Device 2 will be

shown in the Alarm Stack. Selecting Building 1 means no alarms will be shown in the Alarm Stack as there are no devices that are direct children of Building 1.

Scenario 3 - Devices 1 and 2 generate alarms - Location Filtering Set to Parent

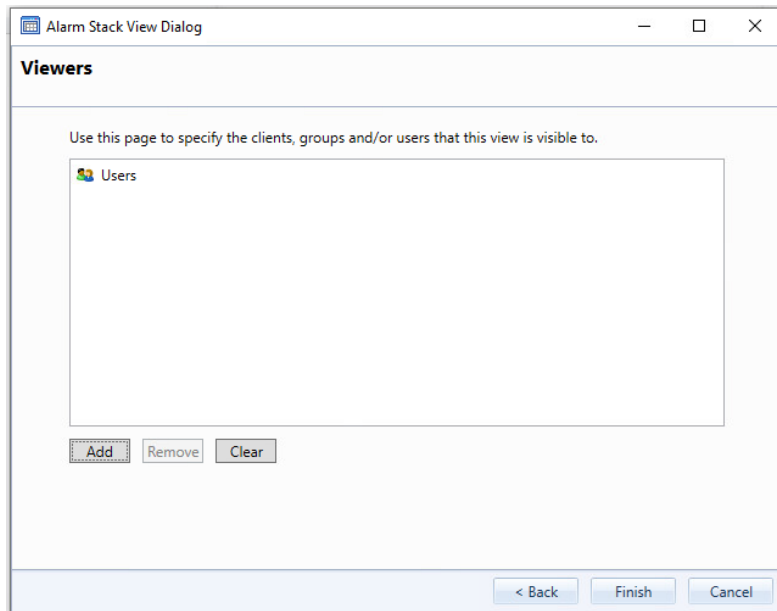
Configure Location Filtering as shown in the Location Filter example. Select Floor 1, Floor 2 or Floor 3 to show all the Alarms from Building 1 and all the sub-locations. This will also include the Alarms from both Device 1 and Device 2.



Viewers

To specify who can view this Alarm Stack View, set permissions on it. For example, create an Alarm Stack View for the Head of Security, which includes all alarms, and create another Alarm Stack View of only access control alarms for the security guards.

1. Using the **Search** dialog, select users and/or groups and click **Add**. The **Search Objects** dialog appears displaying groups, user or Windows clients.
2. Search and find the users to view this Alarm Stack View, for example, Users. Click **OK** to confirm the selection. The Users/Groups appears in the **Viewers** page.



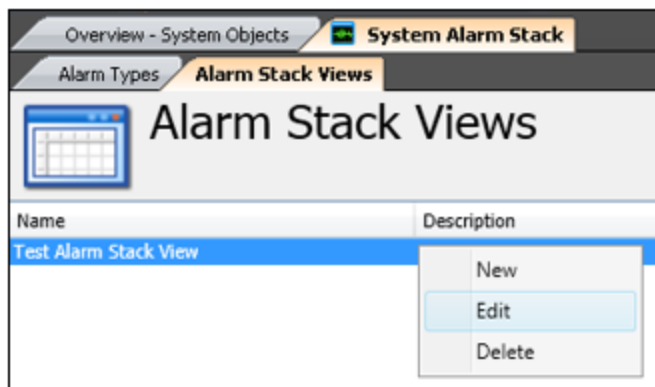
3. Click **Finish**. The Test Alarm Stack View appears in the Alarms Stack Views.

Editing an Alarm Stack View

To edit an Alarm Stack View, in the Alarm Stack View window, click the Alarm Stack and select **Edit** in the toolbar.



Alternatively, in the Alarm Stack to select it. Right-click and select **Edit**.



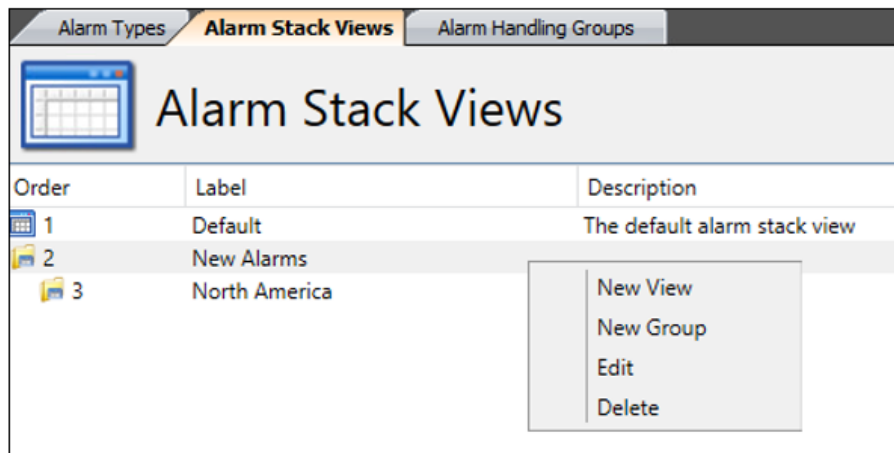
The Alarm Stack View Wizard appears with the Alarm Stack parameters populated and ready for editing.

Deleting Alarm Stack Views

To delete an Alarm Stack View, in the Alarm Stack View window, click the Alarm Stack and select **Delete** in the toolbar.



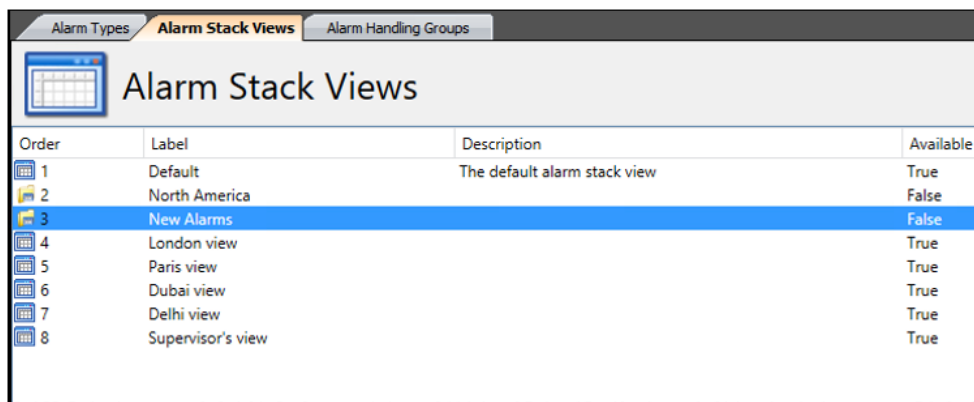
Alternatively, click the Alarm Stack to select it. Right-click and select **Delete**.



Alarm Stack View Groups

Alarm Stack View Groups enable you to access multiple Alarm Stack Views without overloading the Alarm Stack on the Alarm Stack Views configuration page. Alarm Stack View Groups are useful for creating hierarchical groups of Alarm Stack Views which contain several separate Alarm Stack Views.

When setting up the following Alarm Stack Views for display on an Alarm Stack, the display for the end-user can appear congested and may not fit the width of the screen.



The Alarm Stack View tabs wrap or occasionally display off the edge of the screen.

System Alarm Stack											
Default A View for Supervisors All Alarms for London All Alarms for Paris All Alarms for Washington All Alarms for Boston All Alarms for New York All Alarms for Munich All Alarms for Vienna All Alarms for Sar											
ID	Priority	Date Created	Description	Alarm Type	Alarm Point	Location	Top Location	State	Status	Count	Last Received Event

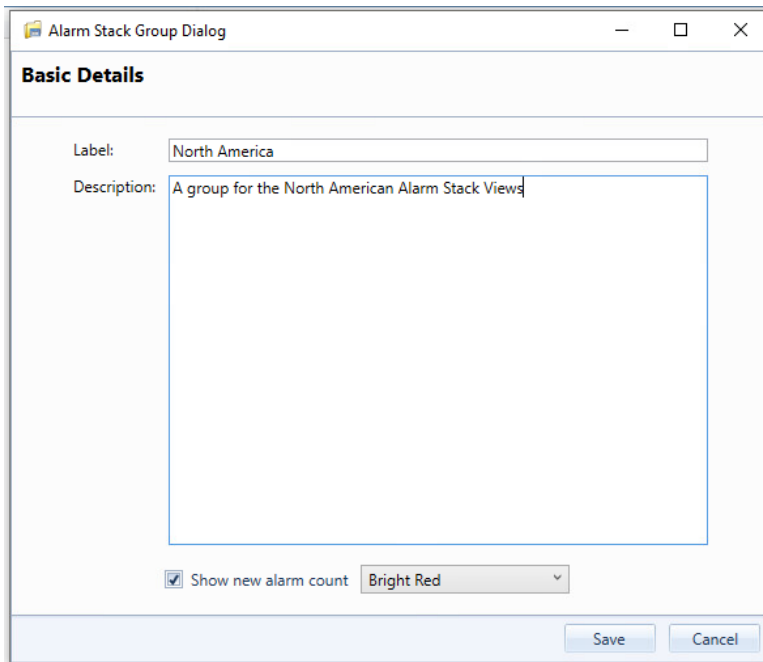
To create an Alarm Stack View Groups:

1. Right-click anywhere in the Alarm Stack Views Configuration screen and select the New Group option.

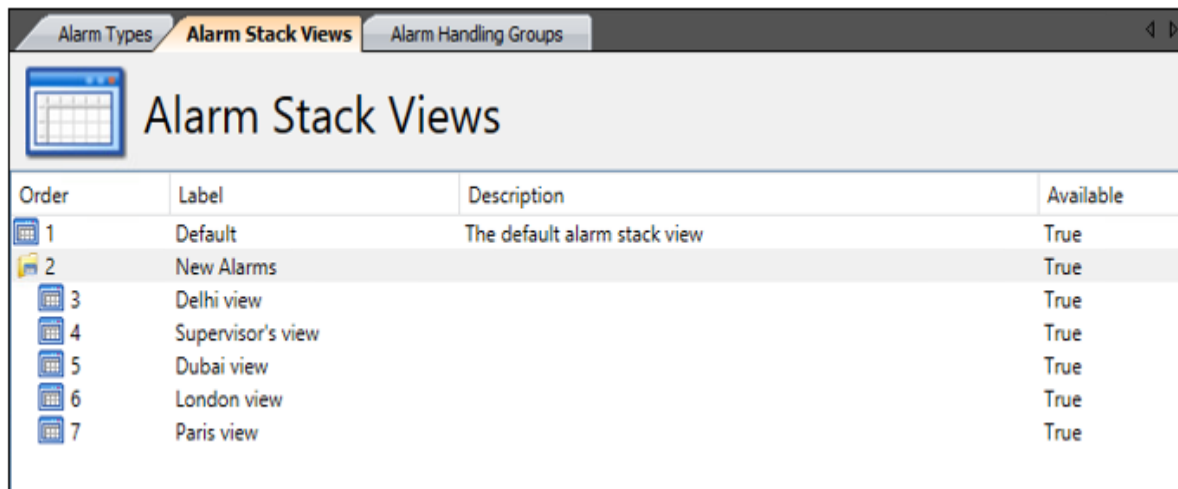
Order	Label	Description
1	Default	The default alarm stack view
2	A View for Supervisors	A supervisor View
3	All Alarms for London	
4	All Alarms for Paris	
5	All Alarms for Washington	
6	All Alarms for Boston	
7	All Alarms for New York	
8	All Alarms for Munich	
9	All Alarms for Vienna	
10	All Alarms for San Francisco	
11	All Alarms for Philadelphia	
12	All Alarms for Minneapolis	

The Alarm Stack View Group wizard opens.

2. Complete the following fields to configure the Alarm Stack View Group Wizard:
 - o **Label** - A name for the Alarm Stack Group.
 - o **Description** - A description of the Alarm Stack View.
 - o **Show New Alarm Count (Optional)** - When checked, displays the sum of the new alarms from the Alarm Stack Views within this Group.
 - o **Shown New Alarm Count Color (Optional)** - When selected, the tab background changes to the selected color to provide a visible indication that there is a new alarm in one of the Alarm Stack Views contained within



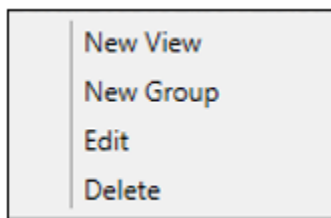
Once created, the Alarm Stack View Groups are shown in line with the Alarm Stack Views but will be shown with a different icon to distinguish between a Group and a View.



Once a Group is created, drag and drop the existing Alarm Stack Views to that group to view them grouped. When dragging a group of Alarm Stack Views, the location of the highlighted section (shown in blue) indicates where the Alarm Stack Views will be dropped. In the following case, the Alarm Stack Views for the European region will be nested inside the Europe Alarm Stack View Group.

Order	Label	Description	Available
1	Default	The default alarm stack view	True
2	Delhi view		True
3	Supervisor's view		True
4	Dubai view		True
5	Europe		True
6	London view		True
7	Paris view		True
8	Frankfurt		True
9	Amsterdam		True

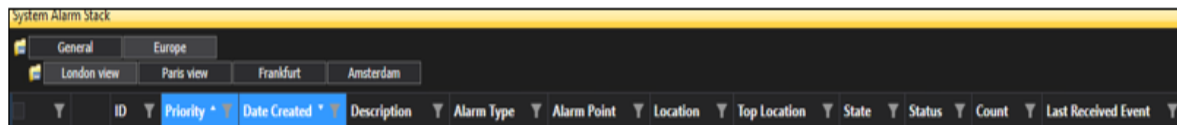
Alternatively, you can create new Alarm Stack Views directly inside a Group by selecting a Group, then right-clicking on the selected Group and selecting the New View option.



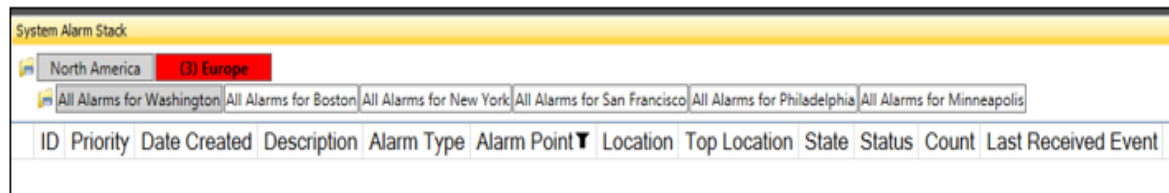
Once the Alarm Stack View Groups are configured appropriately, the Alarm Stack Views are displayed.

Order	Label	Description	Available
1	North America	A group for the North American Alarm Stack Views	True
2	All Alarms for Washington		True
3	All Alarms for Boston		True
4	All Alarms for New York		True
5	All Alarms for San Francisco		True
6	All Alarms for Philadelphia		True
7	All Alarms for Minneapolis		True
8	Charlotte		True
9	Europe	A group for the European Alarm Stack Views	True
10	All Alarms for London		True
11	All Alarms for Paris		True
12	All Alarms for Munich		True
13	All Alarms for Vienna		True
14	Frankfurt		True

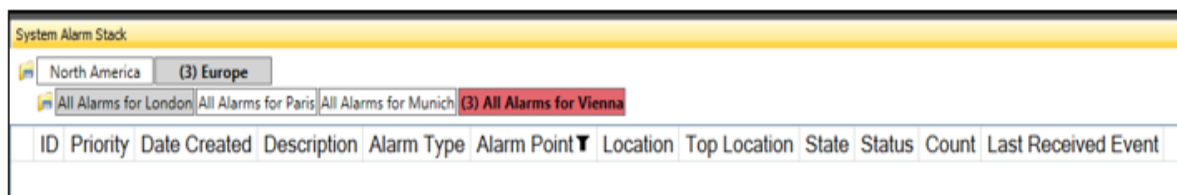
With the Alarm Stack Views configured as shown above, you can view the following Alarm Stack Views. Notice how the Alarm Stacks for the European Cities are displayed in the following figure and the general alarms are hidden from the view.



When an Alarm enters the stack for a device within London, the user is alerted to this as the Alarm Stack Group Europe is highlighted with the configured color and the number of new Alarms created since the View was last opened is also shown.

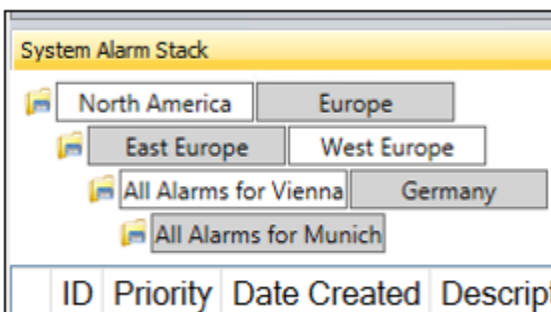


Open the Europe Alarm Stack View Group to reveal the European City Alarm Stack Views. Existing Control Center functionality allows the Alarm Stack View for Vienna to show a highlight and number for new alarms since the user last opened the View.



Nesting Alarm Stack View Groups

The Alarm Stack View Groups can be nested within other Alarm Stack View Groups. Ensure that there is enough vertical space available to display all the appropriate groups and their child Alarm Stack Views.




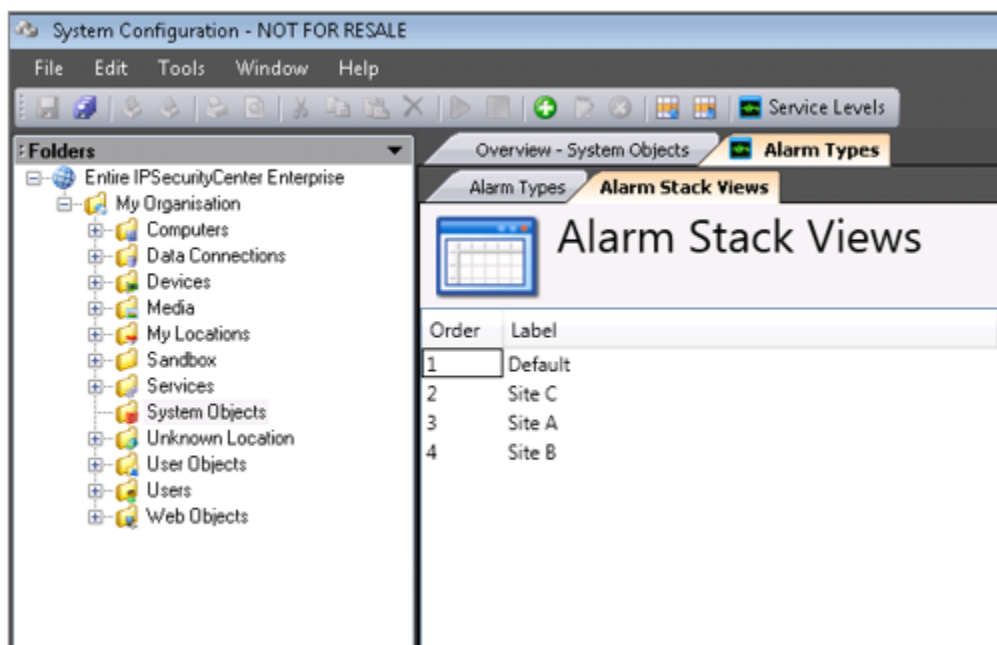
When an Alarm Stack View Group that contains children is dragged and dropped to another location, all the children for that Alarm Stack View Group will also be moved.

Alarm Stack View Index

You can specify the order of Alarm Stack Views if a user has access to more than one view.

To configure the order of views:

1. Open the Alarm Types management interface by double-clicking on the Alarm Types object in System Explorer.
2. Select the Alarm Stack Views tab.
3. Select a view and use the Increase and Decrease buttons  on the menu bar to set the index of a view. The order of the views is shown in the Order column.



4. Close the Alarm Types management interface and review the Alarm Stack in the user interface. The order of the Alarm Stack Views is changed.



Alarm Controls in Graphical User Interfaces

Control Center provides the following GUI controls to complement the underlying Alarm Types logic for end-users.

GUI Control	Description
-------------	-------------

Activity Types Editor	Provides an editor to allow for activity types to be made outside of system configuration.
Alarm Activity Grid	Shows all activities for the selected alarm.
Alarm Stack Grid	Shows all alarms in the system based on filtering options detailed in Alarm Stack Views which are managed via Alarm Types editor.
Event Grid	Shows all event for the selected alarm.
Events Property Grid	Displays properties for a given event.
Manual Alarm Types Combo Box	Shows all alarm types marked as "manual alarm" in a dropdown control for easy user selection of a manual alarm type.
Resolution Types Combo Box	Shows all resolution types configured in alarm types.
Resolution Types Editor	Provides an editor to allow for resolution types to be managed outside of system configuration.
Resolved Alarm Grid	Shows all resolve alarms in the system.
Suppressed Alarm Point Grid	Shows all suppressed alarm points in the system.

Grids

Grids are controls available within Control Center to display alarm event information to users.

The following grids are displayed:

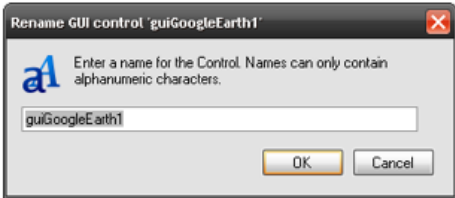
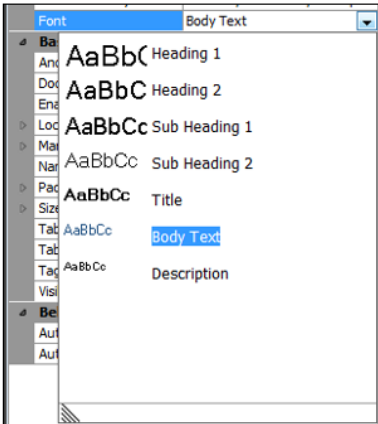
- **Alarm Stack Grid** - All unresolved alarm events
- **Event Grid** - All the events for the selected alarm
- **Alarm Activity Grid** - All the activities for the selected alarm
- **Resolved Alarm Grid** - Previously resolved alarms
- **Suppressed Event Grid** - All events that are suppressed for a group of Alarm Points

Grids are available in the GUI toolbox under the Alarm Types section.

Generic Grid Properties

Grids and objects use many of the same Basic properties and controls. The most common properties are outlined below.

Property	Description
Anchor	The anchor property defines how a control's size and position is affected by changes to the size of its parent control. It can be set to any combination of Left, Top, Right or Bottom. Anchoring a control to its parent control ensures that the anchored edges remain in the same position relative to the edges of the parent control when the parent control is resized.
Dock	The dock property defines the side of the parent control to which this control is docked. It can be set to either Left, Top, Right, Bottom, Fill or None. Docking a control to the left causes the control to align itself with the left edges of its parent control and to resize as the parent control is resized.
Enabled	The enabled property determines if the control is enabled, and therefore can be interacted with, when shown in a tile. A control can either be enabled, allowing user interaction, or disabled, which causes the controls area to be overlaid with a white background and the text "<control-name> disabled". This property can be set dynamically.
Location	The location property determines the control's top left point inside its parent control. Its x and y parameters may not be set to less than zero as this would cause the control's top left point to be outside the visible bounds of the parent control.
Margin	The margin property determines the controls Right, Left, Top and Bottom margins inside its parent control. No margin may be set to less than zero, as this would cause the control to be outside the visible bounds of the parent control.
Padding	The padding property determines the controls Right, Left, Top and Bottom padding between the control and its parent control. No padding may be set to less than zero, as this would cause the control to be outside the visible bounds of the parent control.
Size	The size property determines the height and width of the control. Neither width nor height may be a negative number. Changes to this property, if Dock property is set, to anything but "None" may be

	<p>ignored, depending on the value of the Dock Property. (If “Fill”, all changes are ignored, if “Top” or “Bottom” then changes to width are ignored, or if “Left” or “Right” changes to height are ignored).</p>
Name	<p>The name property assigns a unique identifier to the control. Each control in a GUI must have a unique name that can be referenced by other components in Control Center. To edit the Name, click the ellipsis (...) to display the standard Control Center GUI Editor Control Rename dialog. Enter a Name and click the OK button. The Name is validated against all the other controls in the GUI and if there is a conflict with another control name a red exclamation mark appears. Enter another Name and try again.</p> 
Header Font	<p>The header font property allows the user to specify which font to use for the column headers in the grid. The user must select a Control Center defined font using the standard font type editor (shown below).</p> 
Row Font	<p>The row font property allows the user to specify which font to use for the rows in the grid. The user must select a Control Center defined font using the standard font type editor (shown above).</p>
Auto Refresh	<p>The auto refresh property determines if the grid automatically refreshes its data. To enable auto refresh, select True.</p>

Auto Refresh Interval	The auto refresh interval determines the interval after which a refresh occurs, if auto refresh is enabled. The time set in this parameter is set in seconds.
Tab Index	The tab index is used to define a sequence that users follow when they use the Tab key to navigate through a page. The tab order starts at the lowest tab index value and works through in increments.
Tab Stop	The tab stop is used to define when object that should be stepped over in the tab index progression.
Tag	The tag property is a storage field for user-defined text, which may be retrieved dynamically at runtime.
Visible	The visible property determines if the control can be viewed at runtime (i.e. when shown in a tile). Changes to this property when in design-time (i.e. when editing the GUI) are ignored. This property can be set dynamically.

Alarm Stack Grid

The Alarm Stack Grid is the control used for displaying all the views associated with the current user, user groups, and current client. Control Center includes a GUI already populated with the Alarm Stack Grid, called the System Alarm Stack.

The grid loads all alarms and updates as and when new alarms occur.

More than one grid can be created to serve different purposes. However, only one grid is required in most solutions. If more than one view is available to a user, the views are displayed in separate tabs.

You can configure a grid to show only a sub-set of the Alarm Stack Views so that a grid is used for a specific purpose, for example, show all access control alarms.

To view the default Alarm Stack Grid:

1. Click **System Objects > Graphical User Interface > Alarm Stack**. The Alarm Stack Grid appears in the Design Surface.
2. Click the System Alarm Stack object. The System Alarm Stack properties appear in the right window.

Property	Description
Hide View Selection	Determines if the View

	<p>toolbar is shown that allows the user to change the view. To prevent the user from changing views, set this property to</p> <p>True</p> <p>.</p>																																										
Clickable Count Column	<p>The</p> <p>Clickable Count Column</p> <p>property determines if the</p> <p>Count</p> <p>column, when displayed to users, appears as a clickable hyperlink. If set to</p> <p>True</p> <p>, when users click the column the</p> <p>Count Column Clicked</p> <p>event is raised. The</p> <p>Event Column Click</p> <p>must be set in Events, for example:</p> <table border="1" data-bbox="561 989 1263 1247"> <thead> <tr> <th>Alarm Point</th> <th>Location</th> <th>State</th> <th>Status</th> <th>Count</th> <th>Top Location</th> </tr> </thead> <tbody> <tr> <td>Camera 2 on Vidi</td> <td></td> <td></td> <td>Unhandled</td> <td>7</td> <td></td> </tr> <tr> <td>Camera 8 on Vidi</td> <td></td> <td></td> <td>Unhandled</td> <td>7</td> <td></td> </tr> <tr> <td>Camera 5 on Vidi</td> <td></td> <td></td> <td>Unhandled</td> <td>7</td> <td></td> </tr> <tr> <td>Camera 9 on Vidi</td> <td></td> <td></td> <td>Unhandled</td> <td>7</td> <td></td> </tr> <tr> <td>Camera 6 on Vidi</td> <td></td> <td></td> <td>Unhandled</td> <td>7</td> <td></td> </tr> <tr> <td>Camera 3 on Vidi</td> <td></td> <td></td> <td>Unhandled</td> <td>7</td> <td></td> </tr> </tbody> </table>	Alarm Point	Location	State	Status	Count	Top Location	Camera 2 on Vidi			Unhandled	7		Camera 8 on Vidi			Unhandled	7		Camera 5 on Vidi			Unhandled	7		Camera 9 on Vidi			Unhandled	7		Camera 6 on Vidi			Unhandled	7		Camera 3 on Vidi			Unhandled	7	
Alarm Point	Location	State	Status	Count	Top Location																																						
Camera 2 on Vidi			Unhandled	7																																							
Camera 8 on Vidi			Unhandled	7																																							
Camera 5 on Vidi			Unhandled	7																																							
Camera 9 on Vidi			Unhandled	7																																							
Camera 6 on Vidi			Unhandled	7																																							
Camera 3 on Vidi			Unhandled	7																																							
Scriptable Elements																																											
Property	Description																																										
Enabled	The enabled property allows the control to be enabled or disabled at runtime.																																										
Visible	The visible property allows the control to be shown or hidden dynamically at runtime.																																										
Tag	The tag property provides storage for user defined text, which can be read or set dynamically at runtime.																																										

Events	
Property	Description
Count Column Click	Occurs when a user clicks the count column hyperlink. The ClickedAlarmID is passed as a variable to the event page.
Custom Column Click	Occurs when a user clicks on the custom column hyperlink. The ClickedAlarmID is passed as a variable to the event page.
Alarm Selected	Occurs when a user selects the alarm row. The Selected AlarmID is passed as a variable to the event page.
Alarm Double Clicked	Occurs when a user double-clicks on an alarm row. The DoubleClickedAlarmID is passed as a variable to the event page.
Alarm Right Clicked	Occurs when a user right-clicks on a row in the Alarm Stack. The RightClickedAlarmID is passed as a variable to the event page.

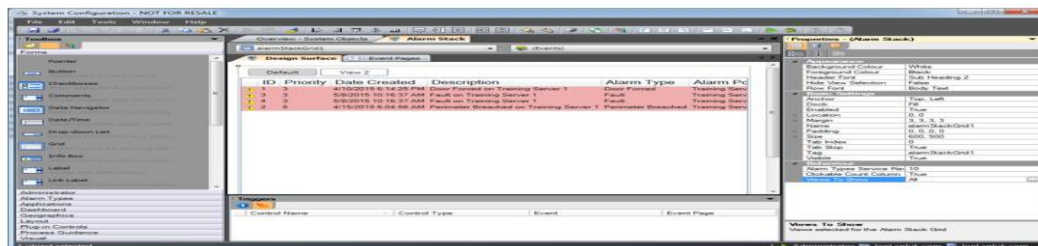
Alarm Stack View Selection in Alarm Stack Grid Control

Although a user has permissions to see multiple Alarm Stack Views, it is recommended to create a screen with one specific view or a selection of views. For instance, the user might want to see all fire alarms on a dedicated screen for better visibility.

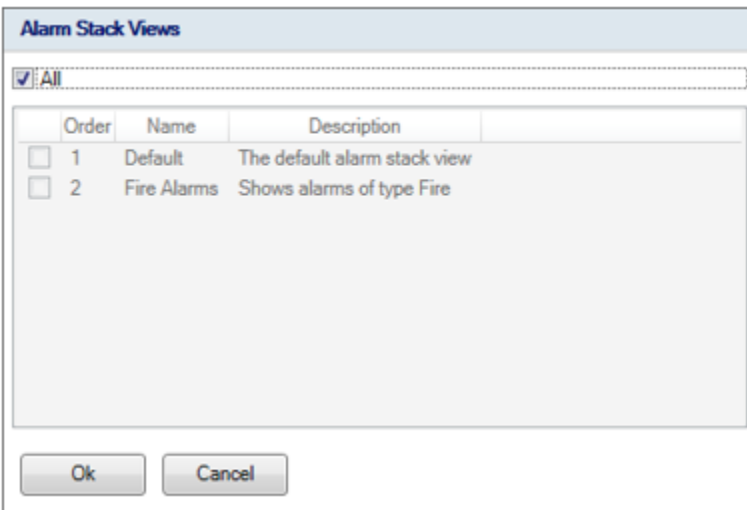
ID	Priority	Date Created	Description	Alarm Type	Alarm Point	Location	Top Location	State	Status	Count	Last Re
5	3	5/19/2015 11:37:06 AM	Fire Alarm on Training Server 1	Fire Alarm	Training Server 1	First Floor		Unhandled	2		5/19/2015 11:37:06 AM

To configure a User Interface to only show specific views:

1. Create the required Alarm Stack Views in the Alarm Types interface.
2. Create a new user interface and open it in the user interface editor.
3. Add an Alarm Stack Grid control.



4. In the properties for the Alarm Stack Grid, click **Views to Show**.
5. Select the views to show, click **OK** and save the user interface.



By default, Alarm Stack Grids are set to show all views that a user has permission to see.

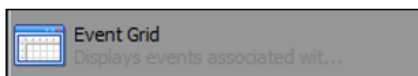
Event Grid

The Event Grid object displays all the events for a specified alarm. The user is required to specify an Alarm ID before the Event Grid displays any data. The Alarm ID can be inherited from other objects such as Grids or Response Plans.

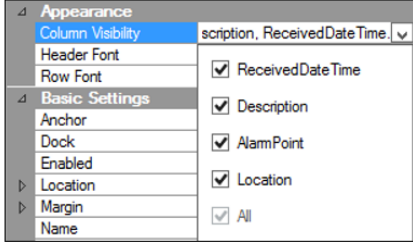
In Alarm Stack View can be created such that operators can click an alarm to see the event grid for that alarm. All the alarm's related events are included in the Event Grid.

To view the default Event Grid object:

1. In System Configuration, right-click anywhere in the middle pane and select **New > Graphical User Interface**. A new Graphical User Interface appears in the list of GUIs.
2. Specify a name for the new GUI and press **Enter**.
3. Double-click the new GUI item to open it. The new GUI appears in the Design Surface.
4. In the **Toolbox**, click **Alarm Types** to expand the menu. Find the Event Grid object and drag it to the Design Surface. The Event Grid appears in the Design Surface.



5. Click the Event Grid to select it and configure the properties that appear on the right.

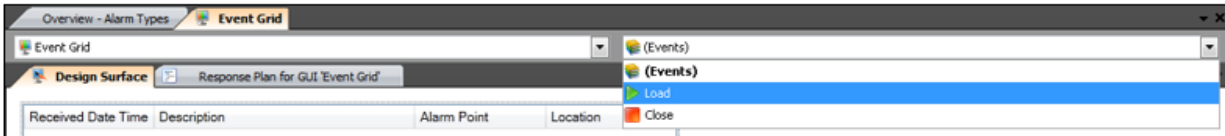
Appearance	
Column Visibility	Allows you to select the columns to be shown on the grid: 
Scriptable Elements	
Property	Purpose
SetAlarmID	The SetAlarmID method is used to set the alarms that the Event Grid displays events for. Without an Alarm ID, the Grid does not display any data.
Enabled	The enabled property allows the control to be enabled or disabled at runtime.
Visible	The visible property allows the control to be shown or hidden dynamically at runtime.
Tag	The tag property provides storage for user defined text, which can be read or set dynamically at runtime.

Adding an Events to Event Grid

The Event Grid does not define any events.

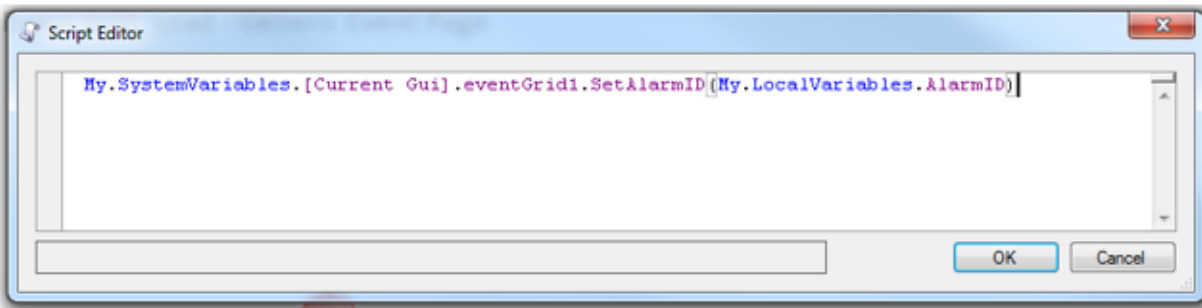
To display the Event Grid with events from a specific alarm:

1. Create a new GUI.
2. Open **Alarm Types** in the toolbox and drag-and-drop the **Event Grid** control to the Design Surface.
3. Set control properties as appropriate.
4. React to the **Load** event of the GUI.

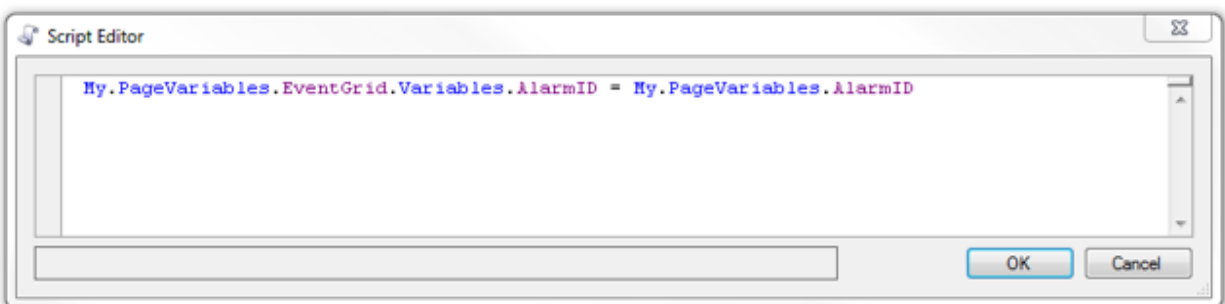


5. Create a new **Local Whole Number** variable called **AlarmID**.
6. Add a script shape and enter the following script.

`My.SystemVariables.[Current Gui].eventGrid1.SetAlarmID (My.LocalVariables.AlarmID)`



7. End the event page with a **Finish** shape.
8. Create a new Response Plan.
9. Create a new **Page** variable called **AlarmID** with **Type Whole Number**, and **Visibility** set to **Required**.
10. Create a new GUI variable called **EventGrid**.
11. Set the prototype of the variable to be the same GUI that was created in the first step of this exercise.
12. Create a new **Tile Layout** variable, called **EventTile**, and set an appropriate prototype value.
13. Add a script shape to the response plan and enter the following script.



14. Add a **Configure** tile layout shape and set the contents of a tile on the tile layout to be the GUI variable created earlier - **EventGrid**.

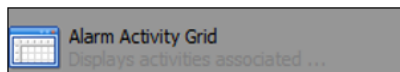
15. Add a **Display** tile layout shape and set the tile variable to **EventTile**. Set the display area and target object's properties to appropriate values.
16. Complete the response plan with a **Finish** shape.
17. Run the response plan passing the ID of the alarm to show events for.

Alarm Activity Grid

The Alarm Activity grid displays all activity for a specified alarm. An Alarm ID is required for the Activity Grid to display any data. The Alarm Activity Grid is available from the Alarm Types section of the GUI toolbox.

To view the Alarm Activity Grid object:

1. Open System Configuration and right-click anywhere to select **New > Graphical User Interface**. A new Graphical User Interface appears in the list of GUIs ready to be named.
2. Specify a name for the new GUI and press **Enter** to confirm it.
3. Double-click the new GUI item to open it. The new GUI is loaded in the Design Surface.
4. In the **Toolbox**, click **Alarm Types** to expand the menu. Find the **Alarm Activity Grid** object and drag it into the Design Surface. The **Alarm Activity Grid** appears in the Design Surface.



5. Click the **Alarm Activity Grid** to select it.
6. The Properties for the object appear in the right window. The properties in Alarm Activity Grid are defined in the Generic Grid Properties section above.

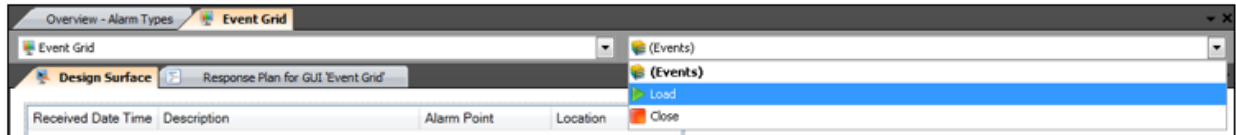
Properties - (Alarm Activity Grid)	
Appearance	
Header Font	Sub Heading 2
Row Font	Body Text
Basic Settings	
Anchor	Top, Left
Dock	None
Enabled	True
Location	13, 4
Margin	3, 3, 3, 3
Name	alarmActivityGrid1
Padding	0, 0, 0, 0
Size	572, 434
Tab Index	0
Tab Stop	True
Tag	alarmActivityGrid1
Visible	True
Behaviour	
Auto Refresh	False
Auto Refresh Interval	10

Scriptable Elements Property	Purpose
SetAlarmID	The SetAlarmID is used to set which alarm the Event Grid displays events for. An Alarm ID must be set before the grid displays any data.
Enabled	Allows the control to be enabled or disabled at runtime.
Visible	Allows the control to be shown or hidden dynamically at runtime.
Tag	Provides storage for user defined text, which can be read or set dynamically at runtime.

Alarm Activity Grid Events

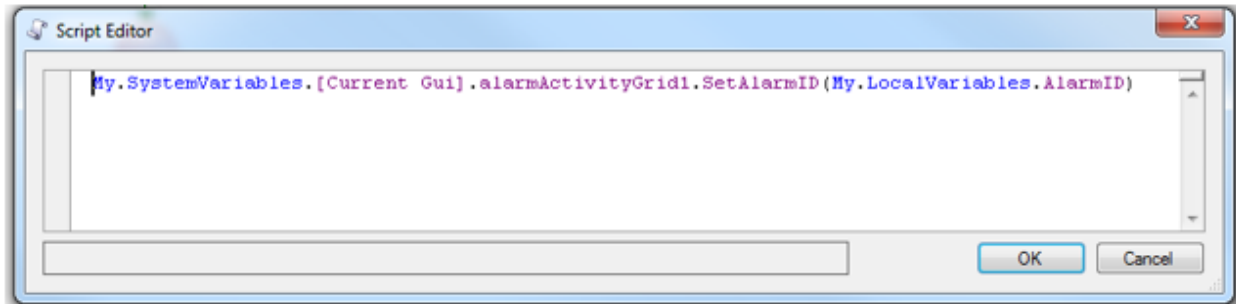
The Alarm Activity Grid does not define any events. To display the Alarm Activity Grid with activities from a specific alarm:

1. Create a new GUI, called **New Activity Grid**.
2. Add an **Alarm Activity Grid** control from the **Alarm Types** area of the toolbox.
3. Set control properties as appropriate.
4. React to the **Load** event of the GUI.



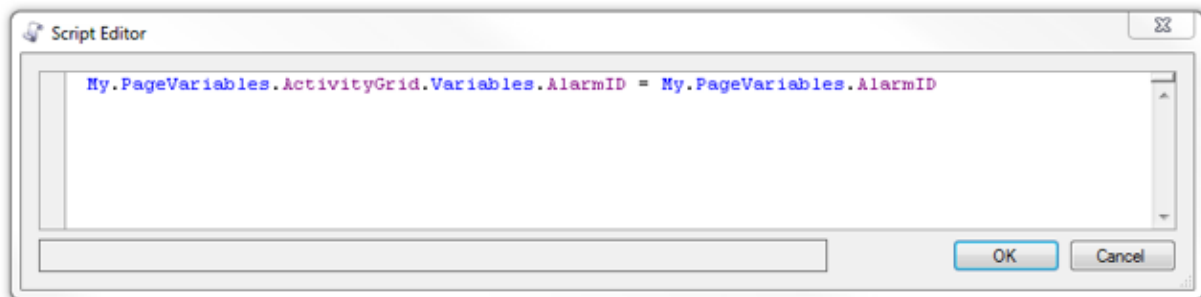
5. Create a new **Local** variable called **AlarmID** with **Type Whole Number**.
6. Add a script shape and enter the following script:

```
My.SystemVariables.[Current Gui].alarmactivityGrid1.SetAlarmID
(My.LocalVariables.AlarmID)
```



7. End the event page with a **Finish** shape.
8. Create a new Response Plan.
9. Create a new **Required, Page** scope, **Whole Number** variable called **AlarmID**.
10. Create a new GUI variable called **ActivityGrid**.
11. Set the prototype of the variable to be the “New Activity Grid” GUI.
12. Create a new **Tile** Layout variable, called “Event Tile”, setting an appropriate prototype value.
13. Add a script shape to the response plan and enter the following script:

```
My.PageVariables.ActivityGrid.Variables.AlarmID= My.LocalVariables.AlarmID)
```



14. Add a configure tile layout shape, setting the contents of a tile on the tile layout to Event Tile.

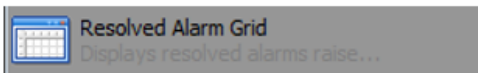
15. Add a display tile layout shape, setting the tile variable to Event Tile. Set the display area and target objects properties to appropriate values.
16. End the response plan with a **Finish** shape.
17. Run the response plan passing the ID of the alarm to show activity for.

Resolved Alarm Grid

The Resolved Alarm Grid displays previously resolved alarms.

To view the Resolved Alarm Grid object:

1. In **System Configuration**, right-click anywhere in the middle pane and select **New > Graphical User Interface**. A new GUI appears in the list of GUIs.
2. Specify a name for the new GUI and press **Enter** to confirm it.
3. Double-click the new GUI item to open it. The new GUI appears in the Design Surface.



4. In the **Toolbox**, click **Alarm Types** to expand the menu. Find the **Resolved Alarm Grid** object and drag it into the Design Surface. The Resolved Alarm Grid appears in the Design Surface.
5. Click the Resolved Alarm Grid to select it. The **Properties** for the object appear in the right window. The properties in Resolved Alarm Grid are defined in the Generic Grid Properties section above.

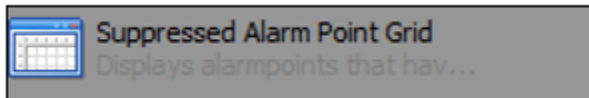
Properties - (Resolved Alarm Grid)	
Appearance	
Column Visibility	ResolutionType, ResolvingUser,
Header Font	Sub Heading 2
Row Font	Body Text
Basic Settings	
Anchor	Top, Left
Dock	None
Enabled	True
Location	20, 20
Margin	3, 3, 3, 3
Name	resolvedAlarmGrid1
Padding	0, 0, 0, 0
Size	673, 492
Tab Index	0
Tab Stop	True
Tag	resolvedAlarmGrid1
Visible	True
Behaviour	
Auto Refresh	False
Auto Refresh Interval	10

Scriptable Elements Property	Purpose
SetAlarmID	The SetAlarmID is used to set which alarm the Resolved Alarm Grid displays events for. The Alarm ID must be set before the grid displays any data.
Enabled	The enabled property allows the control to be enabled or disabled at runtime.
Visible	The visible property allows the control to be shown or hidden dynamically at runtime.
Tag	The tag property provides storage for user defined text that can be read or set dynamically at runtime.
Scriptable Elements Events	Purpose
SelectedAlarmChanged	Occurs when the user clicks one of the Resolved Alarm Grid rows. Can be used where an engineer creates a user interface containing two controls – a Resolved Alarms Grid with all the events and

	activities listed beneath it. In this case, the Grid is used to react to the operator's click event to populate the event and activities grid at the bottom of the GUI.
--	---

Suppressed Alarm Grid

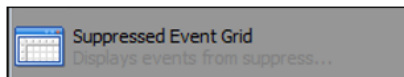
The Suppressed Alarm Point Grid displays all the alarm points that are currently suppressed. The Suppressed Alarm Point Grid is available from the Alarm Types section of the GUI toolbox.



Property	Purpose
Properties	The properties in Suppressed Alarm Point Grid are defined in the Generic Grid Properties section above.
Scriptable Elements	There are no scriptable elements in the Suppressed Alarm Point Grid.
Events Property	Purpose
Alarm Point Selected	Calls the scriptable method called Set Alarm Points and sets the AlarmPoint variable. This occurs when you click one of the Suppressed Alarm Point Grid rows.

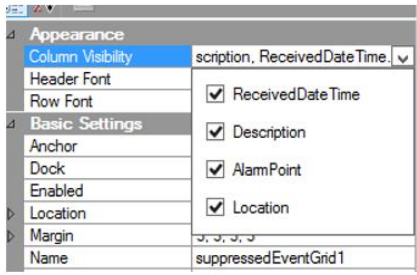
Suppressed Event Grid

The Suppressed Event Grid displays all events that have been suppressed for a specified group of alarm points. The Suppressed Event Grid is available from the Alarm Types section of the GUI toolbox.



Properties

Properties - (Suppressed Event Grid)	
Appearance	
Column Visibility	Location, AlarmPoint, Description
Header Font	Sub Heading 2
Row Font	Body Text
Basic Settings	
Anchor	Top, Left
Dock	None
Enabled	True
Location	4, 21
Margin	3, 3, 3, 3
Name	suppressedEventGrid1
Padding	0, 0, 0, 0
Size	673, 492
Tab Index	0
Tab Stop	True
Tag	suppressedEventGrid1
Visible	True
Behaviour	
Auto Refresh	False
Auto Refresh Interval	10

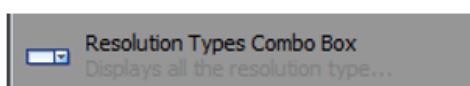
Property	Purpose
Column Visibility	<p>This property allows the user to determine which columns on the grid are shown using the type editor shown below:</p> 
Scriptable Elements	
Property	Purpose
SetAlarmPoints	Use this method to set the Alarm Points that must display suppressed events. Without an Alarm Point ID, the Grid is unable to display any data.
Enabled	Allows the control to be enabled or disabled at runtime.
Visible	Allows the control to be shown or hidden dynamically at runtime.

Tag	Provides storage for user defined text which can be read or set dynamically at runtime.
Focus	Set the focus to the control.
Events	The Suppressed Event Grid does not define any events.

Resolution Type Combo Box

The Resolution Type combo box allows selection of Resolution Types from a drop-down control. This control can be used on a Resolution Form, for example.

The Resolution Type combo box is available from the Alarm Types section of the GUI toolbox.



The properties in Resolution Types combo box are defined in the Generic Grid Properties section below.

 A screenshot of a software development environment's "Properties" window. The window title is "Properties - (Tutorial GUI)". It shows a list of properties for a widget. The "Name" property is highlighted.

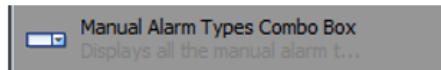
Basic Settings	
Anchor	Top, Left
Dock	None
Enabled	True
Location	272, 13
Margin	3, 3, 3, 3
Name	resolutionTypesEditor1
Padding	0, 0, 0, 0
Size	251, 364
Tab Index	1
Tab Stop	True
Tag	resolutionTypesEditor1
Visible	True

Scriptable Elements

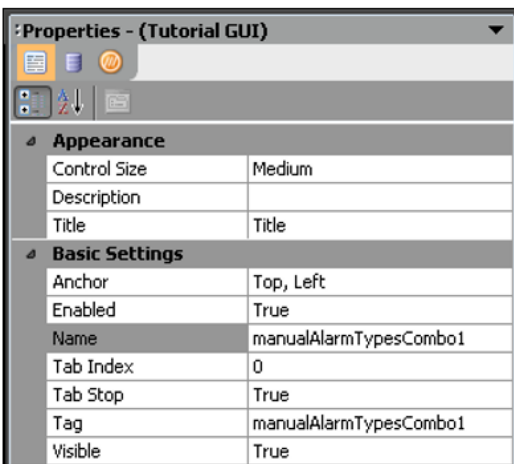
Property	Purpose
GetSelectedAlarmType	Read out the selected resolution type into a text variable for use with other shapes such as Resolve Alarm.
Events	The Resolution Type combo box does not define any events.

Manual Alarm Type Combo Box

The Manual Alarm Type combo box allows the selection of Manual Alarm Types. The list of manual alarms is generated from the Alarm Types marked as 'manual alarm'. The Manual Alarm Type combo box is available from the Alarm Types section of the GUI toolbox.



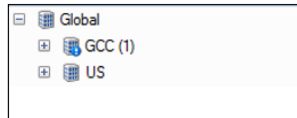
The properties in Manual Alarm Type combo box are defined in the Generic Grid Properties section below.



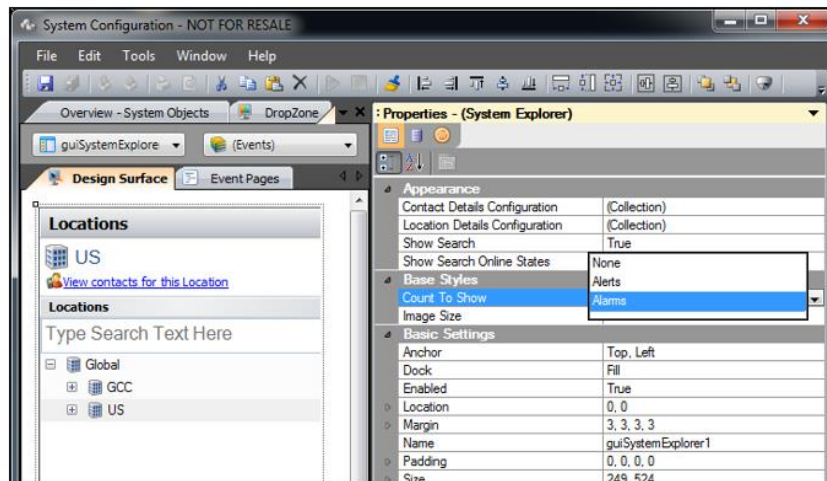
Scriptable Elements Property	Purpose
GetSelectedAlarmType	Read out the selected alarm type into a text variable for use with other shapes such as Create Alarm.
Events	The Manual Alarm Type combo box does not define any events.

Alarm and Alert Count in System Explorer

The System Explorer can show the number of alarms or alerts currently active in a location (including all child locations).



The Count to Show property in System Explorer allows you to select the type of count to show against a Location. For example, number of alerts, number of alarms, or no count.



Alarm Trails on Maps

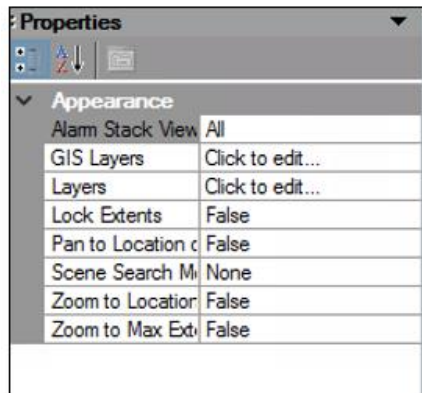
When you create alarms for a geo-aware event, the alarm trails for that event will appear on the map surface.

To view alarm trails on the map surface:

1. In **System Configuration > System Objects**, create an alarm by clicking the **Add** (plus sign) icon. The **Alarm Types Wizard** appears.
2. In the **Basic Information** page, enter the required information such as label, icon, and click **Next**.
3. In the **Evaluation Alarm Creation Event** page, configure the appropriate information for the device being configured. For this example, using the DemoRadar device, provide the following information and click **Next**:
 - **DeviceType** – DemoRadar \ 2D Track Simulator connector
 - **Device(s)** – DemoRadar Device \ Geo-aware device
 - **Event** – TraceUpdated \ Position Changed event
4. In the **Collation and Actions** page, select **Collate by TrackID**.
5. Confirm the **Alarm Type** details and click **Finish**. The **Alarm Type** appears in the **Alarm Types Overview** window.

The Alarm Trails appear on the end-user map surface and the trail object icon is replaced with the **Alarm Trails** icon.

6. From **Locations**, open the scene editor for the scene that you want to display alarm trails on. The scene editor opens.
7. In the **Appearance Properties** section, set the **Alarm Stack View** option to **All**.



The Alarm Trails should now appear on the end-user map surface replacing the Trail Object icon with the Alarm Trails icon.

Once Alarm Trails are displayed, right clicking on the tracking object displays the Handle Alarm (Alarm ID) – When selected, the alarm is handled for the Alarm Id shown.

Applying Alert States to Alarm Trail Paths

When a trail is associated with an active alarm by its track id then the icon and trail color will change to reflect any alert state configured for the alarm.

To apply an alert to a Trail Path:

1. In **System Configuration > System Objects**, create an **Alert State** object and configure the following properties:
 - **Color** - The color for the Alert path. Set a different color from Trail Path Color.
 - **Duration** - The time required to display the alert, for example, 60 seconds.
 - **Icon** - The icon for the alert. Set a different icon from the Trail icon.
 - **Parents to alert** - Location Type property of your parent location, for example, Country, site or region.
 - **Text** – Text for displaying on the duration of the alerted state.
2. From **System Objects**, open the Alarm Type created for the geo event related to the associated connector (demo radar, 2d track simulator and so on) and navigate to the **Collation & Alarm Actions** page. The **Collation & Alarm Actions** page appears.

3. In the **Alarm Actions > Created - Alert State** section, click **Alert Alarm Point** and select the newly created Alert State object. The Alert State Object is assigned to the Alert State property on the Alarm Type Wizard for the Alarm Created action.
4. On the display area, verify if the alert has been applied to the object on the Scene.
5. The Trail icon or Alarm icon (depending on what was being displayed previously) should now be replaced with the Alert icon on the end-user map surface. However, if you did not configure an icon for the Alert object when applying it via the alarm on Trail Path, then the Alarm Trail paths will be displayed with the Alarm icon.

Configuring Alarm Handling Groups

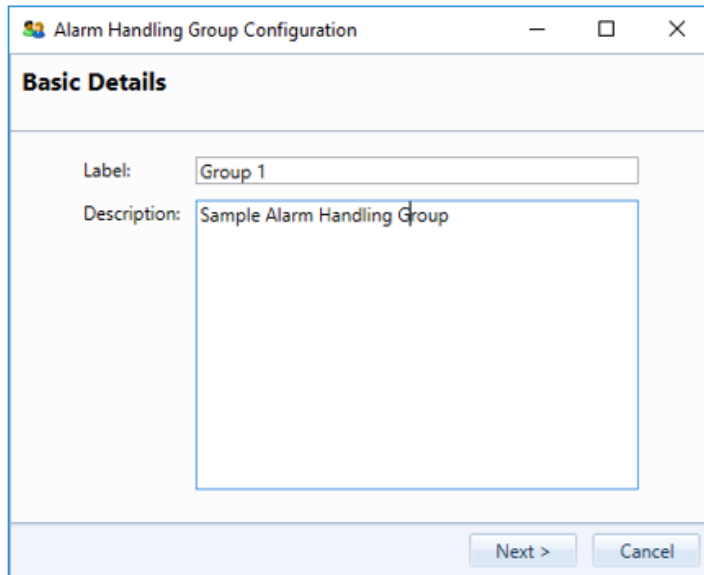
You can create Alarm Handling Groups to define which users can handle and/or resolve alarms based on the specified conditions. When no handling groups are defined for an Alarm Type or a Correlated Alarm Type, all users who have permission to view alarms from this alarm type can handle and resolve alarms.

You can configure Alarm Handling Groups to restrict users from handling and resolving certain alarms. To do this:

- At least one Alarm type is configured in the system.
- Create users or user groups for configuring permissions to handle alarms.

To configure Alarm Handling Groups:

1. From **System Configuration > System Objects** > double-click on **Alarm Type** object. The **Alarm Types** page editor appears
2. Click the **Alarm Handling Groups** tab to create an Alarm handling group
3. Right-click on the empty space and choose **New Handling Group**. The **Alarm Handling Group Configuration Wizard** opens.
4. Enter the label and description and click **Next**.



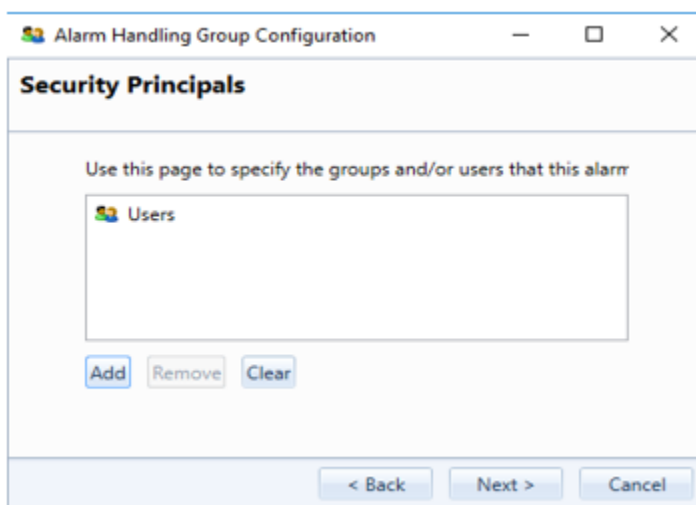
Alarm Handling Group Configuration

Basic Details

Label:

Description:

- On the **Security Principals** page, click **Add** to add the user group you want to apply the handling group permissions to. For instance, **Users** and then click **Next**. The **Handle Conditions** dialog appears.



Alarm Handling Group Configuration

Security Principals

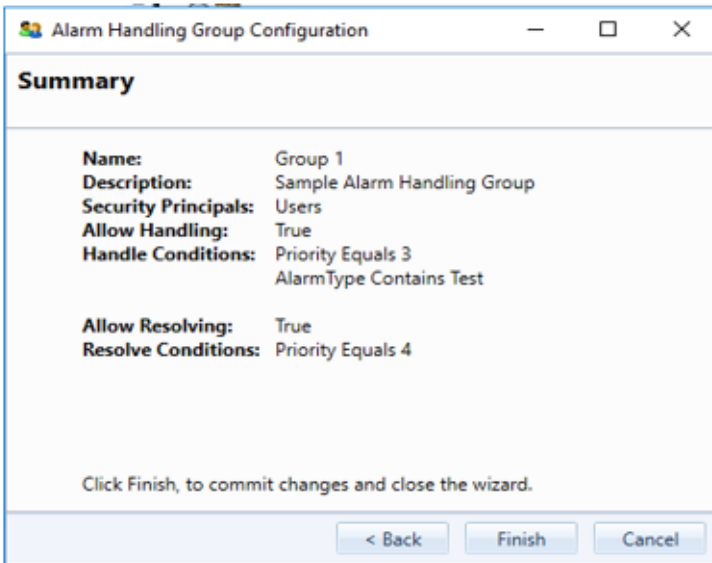
Use this page to specify the groups and/or users that this alarm

- This dialog is used to state the condition/conditions under which the user group can handle/resolve the alarms. You could specify as many conditions as required and choose the operator [AND/OR] to concatenate the conditions. You are allowed to define several nested condition groups here to meet the criteria for the user groups. It is perfectly acceptable not to specify any conditions. This will allow the users of the group to handle all alarms. Click Next to proceed.

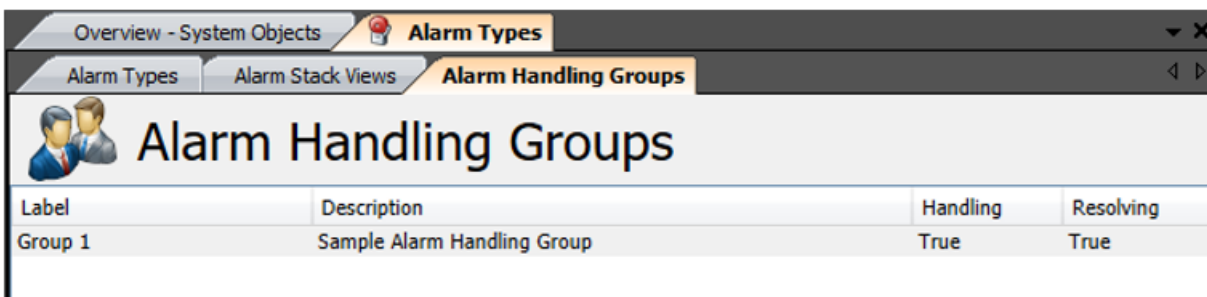
If the check box is left unselected, then no users can handle an alarm for the selected handling group.

7. Configure the Resolve Conditions page similarly to the Handle conditions page by selecting the Allow Resolving option and specifying the conditions for the users and then click Next.

8. Check the configuration on the summary page and click on Finish.



The alarm handling group created can be viewed under Alarm Handling Group tab in Alarm Types



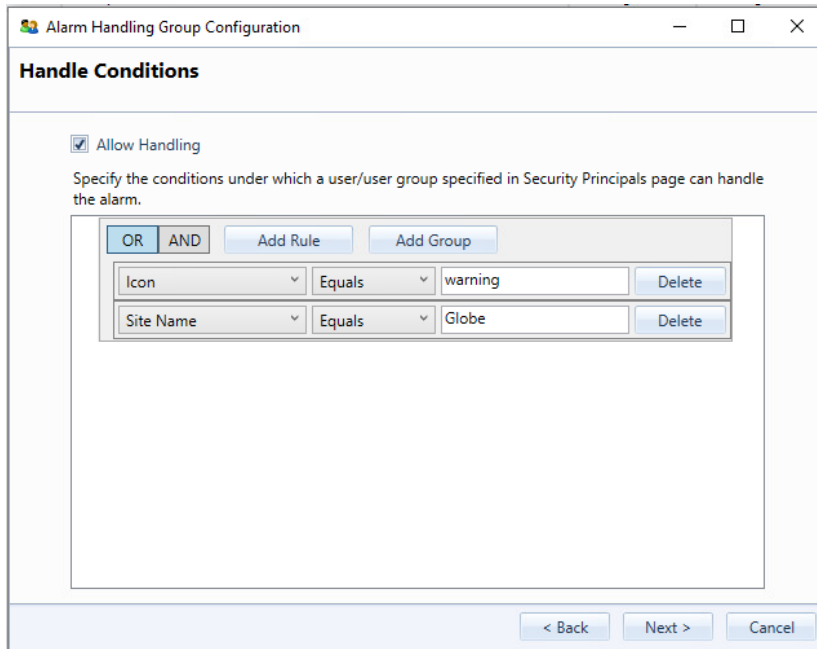
To configure filter conditions, when the Filter Conditions dialog is first displayed, select Allow Handling and then specify one or either of the following conditions:

- Choose an Evaluation Operator (OR & AND)
- Add a Rule to the current Group
- Add a new Group as a Child of the current Group

The Filters Conditions page enables you to construct comprehensive filters where each of the rules can be evaluated against the selected operator. You can add new lines for the filter using Add Rule.

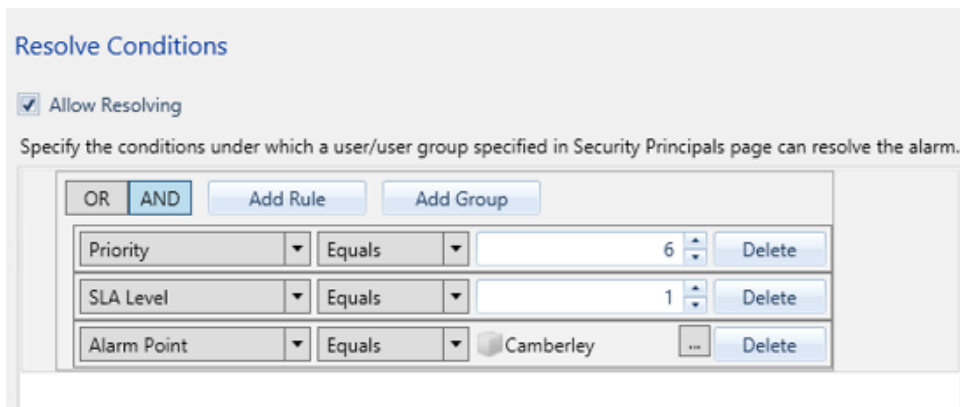
In the below example, the OR evaluation operator is selected, and three new rules are added. Alarms will be included in the Alarm Stack View if the following conditions are met:

- Icon Equals to warning, OR
- Site Name Equals Globe



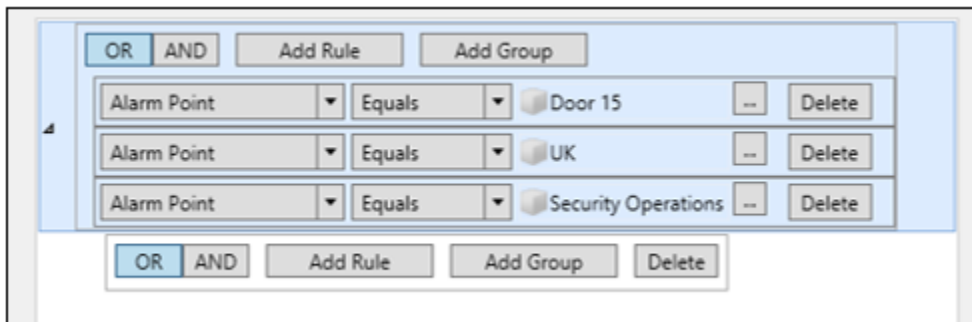
Multiple instances of the same column can match values specified under (OR). Unique columns must match all specified values under (AND).

9. Configure the Resolve Conditions for the Alarm Handling group in the same manner. In the following example, Alarm Groups are included in the Alarm Stack View only if the following conditions are met:
 - o Priority less than or equal to 6, AND
 - o SLA Level equals 1, AND
 - o Alarm Point is set to Security Operations Center



The above configuration will include fewer alarms than the previous example as the conditions are more constrained. You can also include conditions that evaluate the same property multiple times for different values.

For example, in the below figure, the filters for a handling group are set such that alarm handling groups will only appear if the Alarm Point is either Door 15, UK, or Security Operations Centre.



Since there is no logic present to allow Control Center to sense-check these filters, you can construct a Filter where the AND operator is applied to the conditions (similar to the above figure), which will result in no alarms being shown in the Alarm Stack View.

For more complex Filters, you can add Groups to the Filter Conditions by using the Add Group button.



After adding a Group, you can add an Evaluation Operator and Rules. When a Group is added, the Group of conditions are evaluated based on the Evaluation Operator chosen for the Group, then the result of the Group evaluation is added to the parent and then the parent Evaluation Operator is applied.

For more information on how the alarms are evaluated, see [Alarm Stack View Filter Conditions](#).

10. Click **Finish** to complete the filter setup.

Handling Alarms Configured with Alarm Handling Groups

Typically, alarms are handled in one of the following four ways in Control Center:

- Alarm Stack View
- Map (when a trail point layer is configured)
- Response Plans
- Time bar

As alarm handling groups can affect the way you handle alarms, it is recommended to understand the impact it has on the modules that are associated with handling alarms. For example, in the Alarm Stack View, the Alarms with unhandled status will appear as a link only if you are part of the Alarm Handling group associated with the Alarm Type and the handling conditions defined in the Alarm Handling Group are met.

Handling Alarms From the Alarm Stack View

The status **Unhandled** does not appear as a link in the Alarm stack if:

- no users are specified in the Alarm Handling Groups, or Resolving Groups page, or
- if the conditions specified in the Alarm Handling Group are not met.

Similarly, the Resolve checkbox is no longer visible in the Alarm Stack, if the Handling Group conditions are not met:

Handling Alarms From the Time bar

You can handle alarms from the Time bar when viewing playback video on camera. However, when the necessary filter conditions assigned to the alarm type are not met, the following **Can't Handle Alarm** error message displays:

The selected alarm doesn't meet the alarm handling groups' conditions assigned to the alarm type.

Handling Alarms From a Map

You can handle alarms from a map like before, except that you can only handle alarms that can be handled as part of the handling group settings. An error message appears if there are no handling groups assigned to handle the alarm or if the handling conditions are not met. As handling alarms from a map requires setting up trail paths, refer to the Adding a Trail Point Layer section.

Handling Alarms From a Response Plan

When handling alarms via the Alarm Type shapes, Handle Alarm and Resolve Alarm defined in a response plan, the same alarm restrictions apply as the rest of the Alarm Handling functionality.

Take Over of Alarm

You can allow any authorized end-user to take over the handling of an alarm currently being handled by another user. To enable other users to take over the handling of alarms, you must first define which users are permitted to takeover handling of alarms in Control Center using the Takeover handling of an alarm policy. Any authorized user can handle an alarm which is either currently unhandled or parked. Only one alarm can be handled at a time and by one user only.

Configuring Users to Take Over Handling of Alarms

To configure users to take over handling of alarms:

1. From **System Configuration** window, right-click on the topmost folder where the policy should apply, for example, **My Organization** and select **Security Policy...> Allow Alarm Handling Takeover**.
2. Double-click the **Allow Alarm Handling Take over** policy and then define the users in the **Users and Groups** dialog box like the other user-security policies.
3. In the **Alarm Stack view**, click the **Status** of an alarm currently being handled by another user. When an alarm is taken over by a new user, the alarm stack updates the status message to reflect the name of the new user that is handling the alarm.

ID	Priority	Date Created	Description	Alarm Type	Alarm Point	Location	Top Location	State	Status
7	3	2/12/2018 9:23:58 AM	Loop on Training Server 1	Intruder Alarm	Training Server 1	Devices			Handled by Administrator
10	3	2/14/2018 9:51:41 AM	2d on Trackable Device 1	2d	Trackable Device 1	Devices			Handled by Operator
11	3	2/14/2018 12:09:26 PM	Loop on Training Server 1	Loop	Training Server 1	Devices			Unhandled

When a user takes over the handling of an alarm which is currently being handled by another user, any response plan associated with the Alarm Handled Alarm Action of the corresponding Alarm Type will be run. For more information, see [Using Alarm Handled VRP to React to an Alarm Take Over](#). In addition, the Audit trail for an alarm will include details of when alarm handling is taken over by another user.

An alarm can only be taken over if the alarm is in the process of being handled and the user taking over the alarm has the security privilege to do so. In a Federated environment, you can take over the handling of any alarm that you have permissions to handle directly. This includes alarms raised and being handled at a remote site.

Configuring Assign Alarm Handled VRP

To assign Alarm Handled VRP:

1. In the **System Configuration** window, create a new response plan. Rename it to **Alarm Handled**.
2. From **System Objects**, create a new Alarm Type for an actual device such as an access control device, and navigate to the **Collation & Alarm Action** dialog.
3. Click **Browse** and select the Alarm Handled VRP, and then complete the wizard.

4. Open the Alarm Handled VRP. The VRP opens in the VRP editor.
5. Notice the variables available in the response plan configured for handling an alarm. The variables relevant to configuring alarm handling are added to the plan automatically. The following variables specific to alarm take-over are newly available:
 - **PreviousHandlingClient**
 - **PreviousHandlingUser**
 - **PreviousHandlingClientRfs**
6. In the VRP editor, drag and drop a script shape and enter the following information:

```
My.PageVariables.Output = "Alarm ID"+
My.SystemVariables.AlarmID.ToString +",Alarm Point:" +
My.SystemVariables.AlarmType +", Event Location:" +
My.SystemVariables.EventLocation.Label +", Priority:" +
My.SystemVariables.Priority.ToString
```

7. Right-click on the Alarm Handled VRP header and save it.

Using Alarm Handled VRP to React to an Alarm Take Over

To use Alarm Handled VRP to react alarms takeover:

1. Open the Alarm Handled VRP for editing.
2. Select all shapes, and right-click to select Toggle Breakpoint or press F9 to toggle the break points on the shapes. Then, save and close the response plan.
3. Right-click on the Alarm Handled VRP and select Enable Debugging.
4. From the Alarm Stack view, take over an alarm that has already been handled by another user or remote site in the system. Alternatively, raise an alarm by disabling the device that is configured in the Alarm Types Wizard to simulate an alarm. The Alarm Handled VRP opens in the VRP editor.
5. Use the toolbar to step through the logic and check the values of the response plan variables in the Watch window at the lower part of the response plan editor. Notice the values for the following variables:
 - **PreviousHandlingClient** – Displays the name of the Control Center Client that was previously handling the Alarm if the alarm handling was taken over by another user. Is null if not applicable.
 - **PreviousHandlingUser** – Displays the name of the Control Center User that was previously handling the Alarm if the alarm handling was taken over by that user. Is null if not applicable.

- **PreviousHandlingClientRfs** – Displays the name of the Control Center Client of the Remote Federation Site for the original handling user. Is null if it is a local site. For example:

PreviousHandlingClient	User 1 (test18)	Generic Client
PreviousHandlingClientRfs	Remote Federated Service	Remote Federated Service
PreviousHandlingUser	Administrator	User

6. In the Alarm Stack view, click the Status of an alarm currently being handled by another user. When an alarm is taken over by a new user, the alarm stack updates the status message to reflect the name of the new user that is handling the alarm.

Notes:

- To populate the PreviousHandlingClientRfs property with a value in the Watch window of the Alarm Handled VRP, you must take over handling of Alarm raised at the remote site.
- To populate the PreviousHandlingClient and PreviousHandlingUser properties with values Watch window of the Alarm Handled VRP, you must take over handling of alarm at a different Client and as a different user.

Configuring Bulk Resolution of Alarms

The Alarm Type Bulk resolve option enables authorized end-users to quickly and easily resolve multiple alarms that appear in the alarm stack. The users can select any number of qualifying alarms of an alarm type category in the Alarm Stack to resolve, as long as they are added to the Allow Bulk Resolution of Alarms Properties security policy. This section is divided into the following three parts to help understand the process of resolving bulk alarms:

- Add Users and Groups to the Bulk Resolution of Alarms policy
- Enable the Allow Bulk Resolution of Alarms in the Alarm Types wizard
- Resolve bulk alarms with a resolution

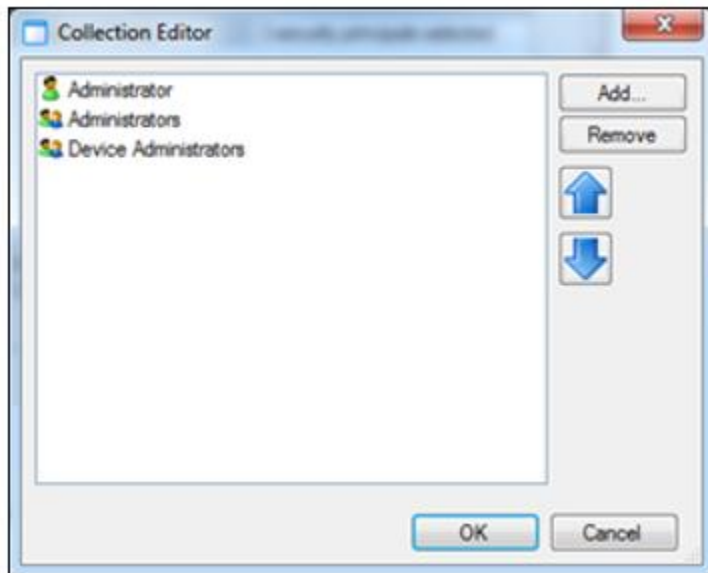
Adding Users and Groups to the Bulk Resolution of Alarms Policy

Using the Allow Bulk Resolution of Alarms security policy, you can determine which users are able to bulk resolve alarms. For example, you can create a list of users and groups who are able to bulk resolve alarms. By default, this new security policy will not be enabled, and there shall be 0 users or groups added to the Bulk Resolve policy.

To add users and groups to the Bulk Resolution of Alarms Policy:

1. In the **System Configuration** window, right-click on the topmost folder where the policy should apply, for example, **My Organization** and select **Security Policy...**
2. Select **User Policies** and double-click on **Allow Bulk Resolution of Alarms**. The **Allow Bulk Resolution of Alarm Properties** dialog appears.

3. Select the **Define Policy** check box and then click **Users and Groups** to define the priorities.



4. Add users and groups. Click **OK**.

Alarm Stack Permissions for Alarm Points

You can prevent a user from seeing alarms from assets that the user does not have permission to see. If the user does not have permission to see the asset, the alarm will not be visible in the alarm stack.

To enable this feature:

1. Open Global Settings and select the Alarms tab.
2. Select the Don't allow users to see alarms if they lack read access to the associated alarm point checkbox.

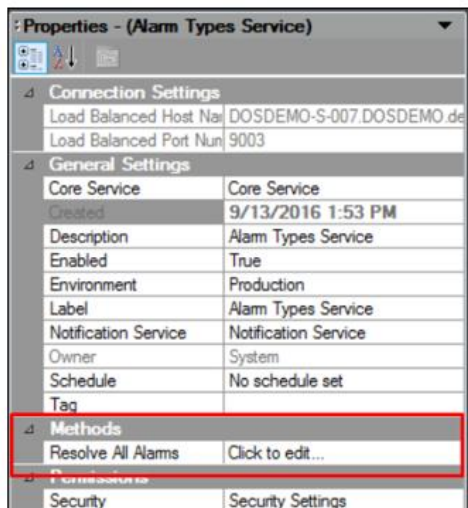
Location Aware Alarm Stack

Control Center will restrict the visibility of Alarms and Alarm Alert States if a Location Aware Alarm Stack is being displayed. Depending on the configuration of the Location Filtering for the Alarm Stack View, the scene may not display the Alert States associated to an Alarm unless an appropriate Location has been selected in the System Explorer tree.

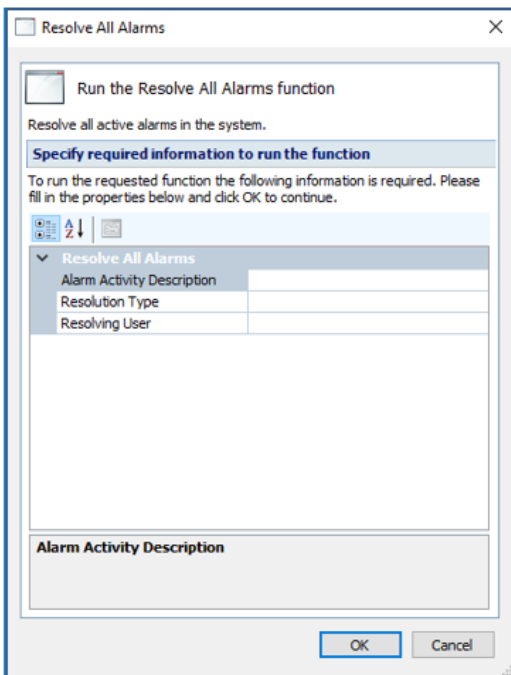
Manually applied Alert States are not affected by Location Filtering for the Alarm Stack View as the Alert State is not considered to be linked to an Alarm.

Resolve All Alarms Method on Alarm Types Service

Using the **Resolve All Alarms** option in the Alarm Types Service object, you can force resolve all Alarms that exist on the current server.



When executed, you will be prompted to update several required fields before the current Alarms are resolved.



In the **Resolve All Alarms** dialog, enter the appropriate Alarm Activity Description, Resolution Type, and Resolving User and click **OK** to resolve all the current alarms. Alternatively, use the Bulk Resolve Alarms method to resolve all alarms, which is also the recommended method to resolve all alarms.

In addition, you can use the Dynamic Action shape to automate the process of mass Alarm Resolution by targeting the Alarm Types Service and calling the Resolve All Alarms method.

Alarm Indicators on Video Playback Time bar

The Time bar that is displayed when a Video Player is in Playback mode shows alarm indicators for alarms that are in the Alarm Stack. The Alarm indicators enable you to track the actual time when a specific alarm was raised. The alarm indicators will appear on any video camera configured within Control Center that is in playback mode at the time. The alarm icons that are displayed match the icons that appear in the Alarm Stack View.

Handling Alarms on Video Playback Time bar

To handle alarms on the video playback time bar:

1. Click on an alarm on the Camera playback time bar mode. An alarm is selected.
2. Right-click on the alarm and view the shortcut option. The ID of the selected alarm is displayed next to the Handle Alarm menu option, for example, Handle Alarm 1.
3. Click Handle Alarm 1.
4. Check the status of the alarm in the System Alarm Stack view area. It should now be changed to Handled by Administrator.
5. This works in the same way as the standard Handle Alarm option on Alarm Stack View, that is, you can see the status of the Alarm once it has been handled.

Notes:

- If you park an alarm using the Park Response Plan, the status in the System Alarm Stack view area changes to Parked by Administrator. Once parked, the alarm becomes available again on the Time bar.
- The alarm icons get updated when an SLA is updated, therefore, the existing Alarm indicator icon will reflect the changes made to the SLA.

Removing an Alarm From the Playback Time bar

To remove alarms from the video playback time bar:

1. Create a response plan to resolve a single alarm.
2. Run the response plan by providing the Handled alarm ID (for example, 1).
3. In the Alarm Stack View, verify if the alarm is resolved.
4. In the display area, view the video playback time bar. Alarm 1 is removed from the Playback Time bar.

5. Re-display the camera and check if alarm 1 is being displayed on the Playback time bar.

Displaying Alarm Indicators Generated by Correlated Alarms

To display correlated alarms on playback time bar:

1. Create a Correlated Alarm Type. For detailed steps, see [Correlated Alarms](#). Correlated alarms provide the ability to define alarms that should only occur if one or more events occur/do not occur/ based on the conditions specified on the object within a defined time.

When an event comes into the rules engine, it is evaluated against the list of correlated alarm types defined within the system. During this process, previous events can be referenced and added into evaluation. Once the Rule Engine has decided that a new alarm needs to be created, any existing alarms based on these events can optionally be resolved or reset.

	Evaluation Order	Priority	Label	Description	Site Name	Enabled	Manual
⊕ ⚠	1	6	test Alarm		Local	False	False
⊕ 📱	2	3	TEST_ACS		Local	False	False
⊕ +	3	3	New alarm gro		Local	True	False
⊕ 🚪	1	2	Test Door	An example of the Correlated /	Local	True	False

Correlated alarm types are listed along with other classic alarm types. You might want to describe them appropriately to distinguish between them in the list.

Alarm types cannot be deleted if there are any alarms in the system of their type. This includes alarms that have been resolved. Alarms should be archived and removed from the live Pacific database if their alarm types need to be deleted. This applies to both classic and correlated alarm types.

With classic alarm types, the order that alarm types appear in the list affects the way alarms are created. Each event can only create a single alarm from a classic alarm type and they are evaluated in the order shown in the list. A single event can result in multiple correlated alarm types, so the order shown here is unimportant.

2. Create a Correlated Alarm Type.
3. Add the following 2 events:
 - Door forced

- Device State Changed
- 4. Display a Camera on the display area.
- 5. Set the live camera to playback mode.
- 6. Display the Alarm Stack on the display area.
- 7. Generate the correlated alarm and view the alarm in the Alarm Stack view.
- 8. View the playback camera on the display area. The alarm icon should appear on the playback time bar.

Suppressing Alarms

You can temporarily suppress an alarm, for example, if you need to perform some maintenance on a device. You can suppress, extend and cancel suppression on alarms:

- From objects
- From response plans

Suppressing Alarms Permissions

You can only suppress alarms if you have, both:

- Execute permission of General Settings of the object whose alarm you want to suppress.
- The Alarm Point Suppression type permission. See [Type Permissions](#) for more information.

Suppressing Alarms From Objects

To do this:

1. You can suppress alarms by right clicking an object:
 - on a map
 - in System Explorer

and selecting **Suppress**. The **Suppression** dialog displays.

2. Select and enter the time duration that you want the alarm to be suppressed for. Once you have entered the time, the **Suppression** dialog displays the time that the alarm suppression ends. If you do not specify a time for the alarm suppression to end, then the alarm is suppressed indefinitely or until you manually cancel suppression of the alarm from the **Suppression** dialog.
3. Optionally, enter the reason for suppressing the alarm. For example, engineer testing on site.
4. Select **Suppress**. The Alarm Point is suppressed.

5. You can extend the time for which an alarm is suppressed by right-clicking a suppressed object
 - on a map
 - in System Explorer

and selecting **Suppression Options > Extend Suppression**. The **Suppression** dialog displays.

6. Select and enter the duration that you want the alarm suppression to be extended by.
7. Select **Extend Suppression**.

Viewing Currently Suppressed Alarms

You can view the alarms that are currently suppressed by using the:

- Suppressed Alarm Point Grid
- Rules Event Viewer

Viewing Suppressed Alarms in Event Viewer

The Rule Engine Event Viewer lists all events processed at machine service level. From the Is suppressed column, you can see which alarms are currently suppressed. To open the Rules Engine Event Viewer:

1. Go to **System Configuration > Computers**. The **Overview** tab displays.
2. Double-click your Rules Engine Server. The events for your machine are displayed.

Viewing Suppressed Alarm Point Grid

Using the Suppressed Alarm Point grid shows your currently suppressed alarms.

Column	Description
Alarm point	The alarm point, for example, the door or camera whose alarm you wanted to suppress.
Suppressed User	The user that initiated the alarm suppression.
Suppressed Since	The date and time the suppression began.
Suppressed Until	The date and time the suppression ended.
Events	The number of events logged while the alarm was suppressed. Note

	: Even though an alarm may be suppressed, any events that are triggered during the time the alarm is suppressed are still logged.
Reason	The reason for the alarm suppression, if given.

The Suppressed Alarm Point grid is available in the GUI Toolbox under Alarm Types.

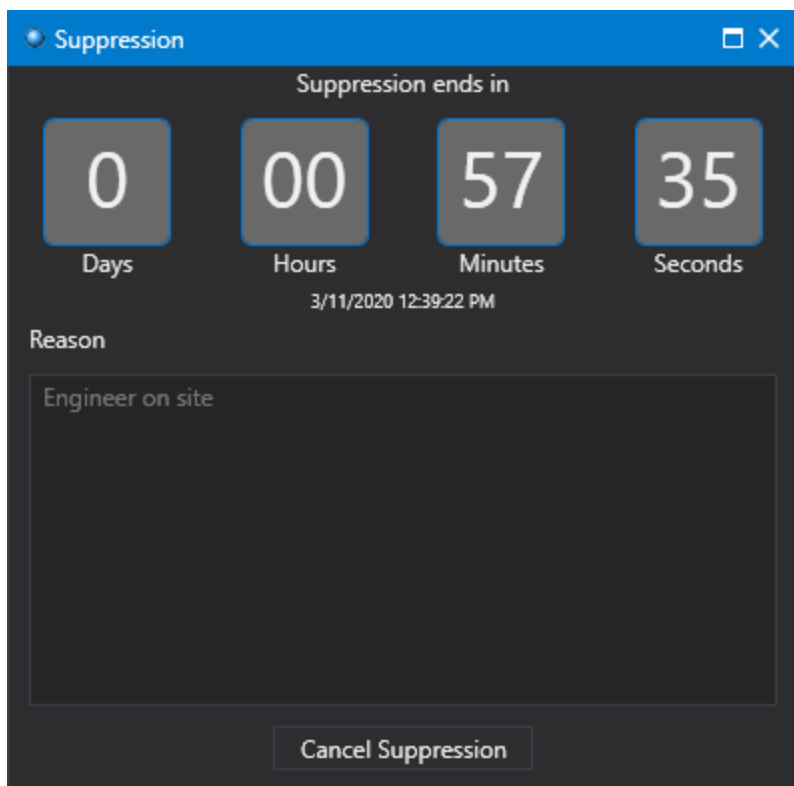
Canceling Suppression on Alarms from Objects

You can manually cancel suppression on an alarm from the Suppression dialog or, if you have specified an end time for the alarm suppression, you can allow the suppression of the alarm to be cancelled automatically by allowing the alarm suppression time you specified to elapse.

To cancel suppression of an alarm manually:

1. You can cancel suppression on alarms by right clicking a suppressed object:
 - on a map
 - in System Explorer

and selecting **Suppression Options > Cancel Suppression**. The **Suppression** dialog displays.

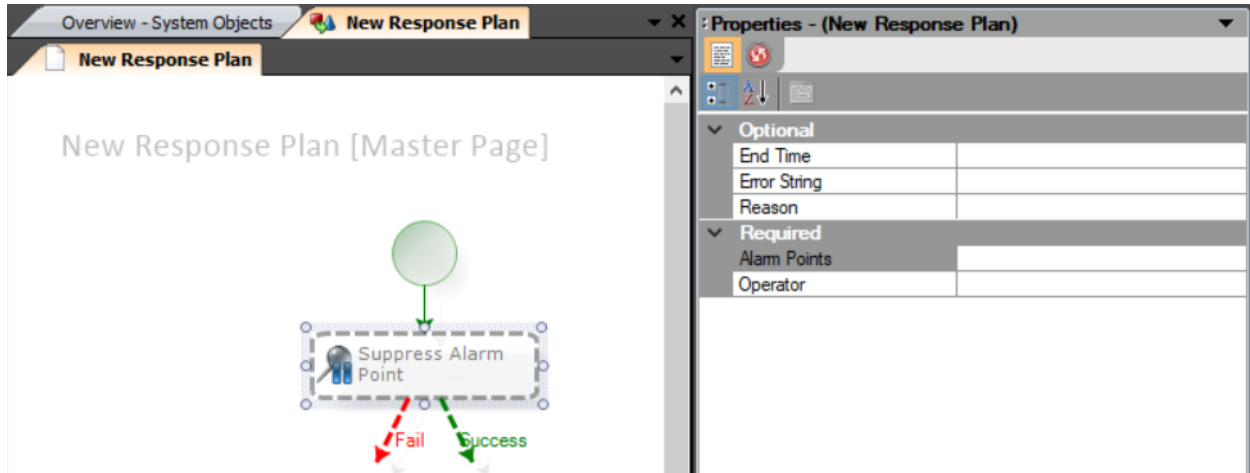


2. Select **Cancel Suppression**. The Alarm Point is unsuppressed.



Suppressing Alarms Using Response Plans

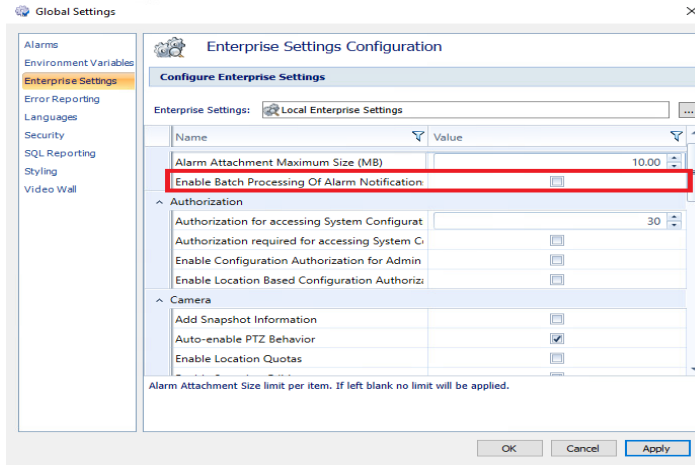
You can suppress alarms in response plans using Suppress Alarm Point and Unsuppress Alarm Point shapes. Using Suppress Alarm Point shape, enter the time you want your alarm suppressed until. If you do not enter a suppression end time, the alarm is suppressed indefinitely.



See [Response Plan Shapes](#) for more information.

Batch Processing of Alarm Notifications

Clients have to orderly and repetitively fetch notifications and other information related to alarms for all the alarms in the alarm stack. This will result in the client reaching out to the server, back and forth several times, doing the exact same process steps increasing the network traffic. This might cause a lot of overhead on the already loaded network. In order to reduce this traffic and increase efficiency of processing the alarms, this release of Control Center has incorporated an option in the Enterprise settings to reduce the network traffic by grouping the notifications to the server every 3 secs. This option is disabled by default. The user needs to enable it, if batching of alarm notification has to take place.



Alarm Data Management

Control Center stores data about received events and the alarms that these generate in its database. This data can be automatically cleaned up regularly based on a configurable schedule. The following two options are available:

- **Cleanup Alarms and Events** – This deletes alarm and event data that are older than the specified time from the database
- **Cleanup Events that are not Alarms** – This deletes event data that is not linked to any alarm if older than the specified time

Everbridge recommends enabling this feature and setting it to a period appropriate to the customer implementation.

For upgraded solutions, the options to clean up the data are turned off.

For upgraded solutions, this feature is disabled by default. If enabled, alarm and event data is deleted. Check the solution requirements before this feature is enabled.

To configure the Alarm Data Management options:

1. Open the **Global Settings** interface.
2. Click **Enterprise Settings** and navigate to **Alarm Data Management**.

The screenshot shows the 'Enterprise Settings Configuration' dialog box with the following settings visible:

Name	Value
Alarm	
Alarm Attachment Maximum Size (MB)	10.00
Client Side Alarm Notifications Batch Size	30
Client Side Alarm Notifications Buffer Time (seconds)	3
Don't allow users to see alarms if they lack read access to the associated alarm point	<input type="checkbox"/>
Enable Batch Processing Of Alarm Notifications	<input type="checkbox"/>
Hide alarm stack tabs that are not currently in schedule	<input type="checkbox"/>
Alarm Data Management	
Alarms - Clean Up Alarms And Events	<input checked="" type="checkbox"/>
Alarms Retention Period	6
Alarms Retention Period Type	Months
Events - Clean Up Events That Are Not In Alarms	<input checked="" type="checkbox"/>
Events Retention Period	1
Events Retention Period Type	Months
Retention Period For Trails That Are Not Alarms (hours)	1
Retention Period For Trails That Are Resolved Alarms (hours)	7
Schedule to Run	Alarm Maintenance
Authorization	
Highlight color of object when selected in a tile.	

3. Specify the following properties:

- **Cleanup Alarms and Events** check box – If selected, Alarm and Event data is continuously deleted.

This option operates against entries in the PacificArchive database instead of the pacific database.

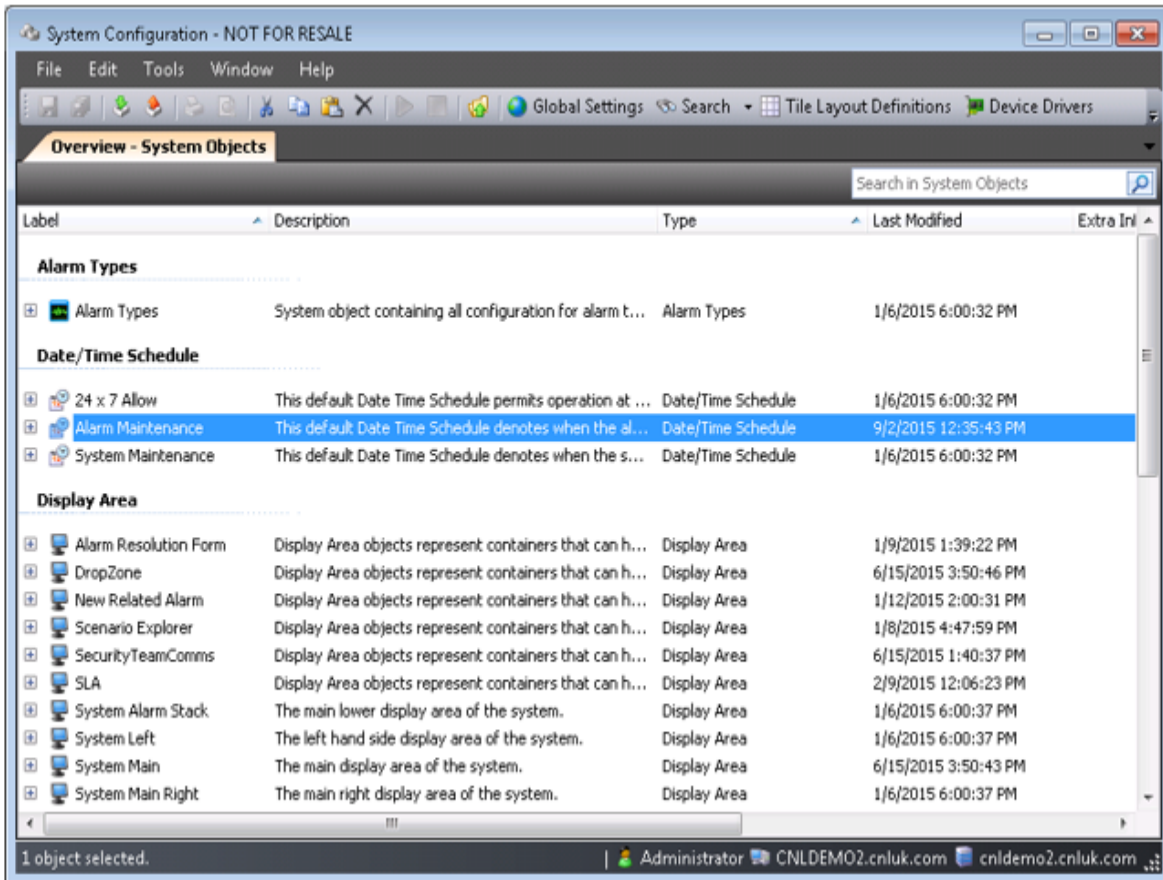
- **Alarm Retention Period** - The retention period to keep alarms in months and days.
- **Events - Cleanup Events That Are Not in Alarms** check box - When selected, Event data that is not related to alarms is continuously deleted.
- **Events Retention Period** - The retention period to keep events in months and days.

4. From **Alarm**, select the following options, if required.

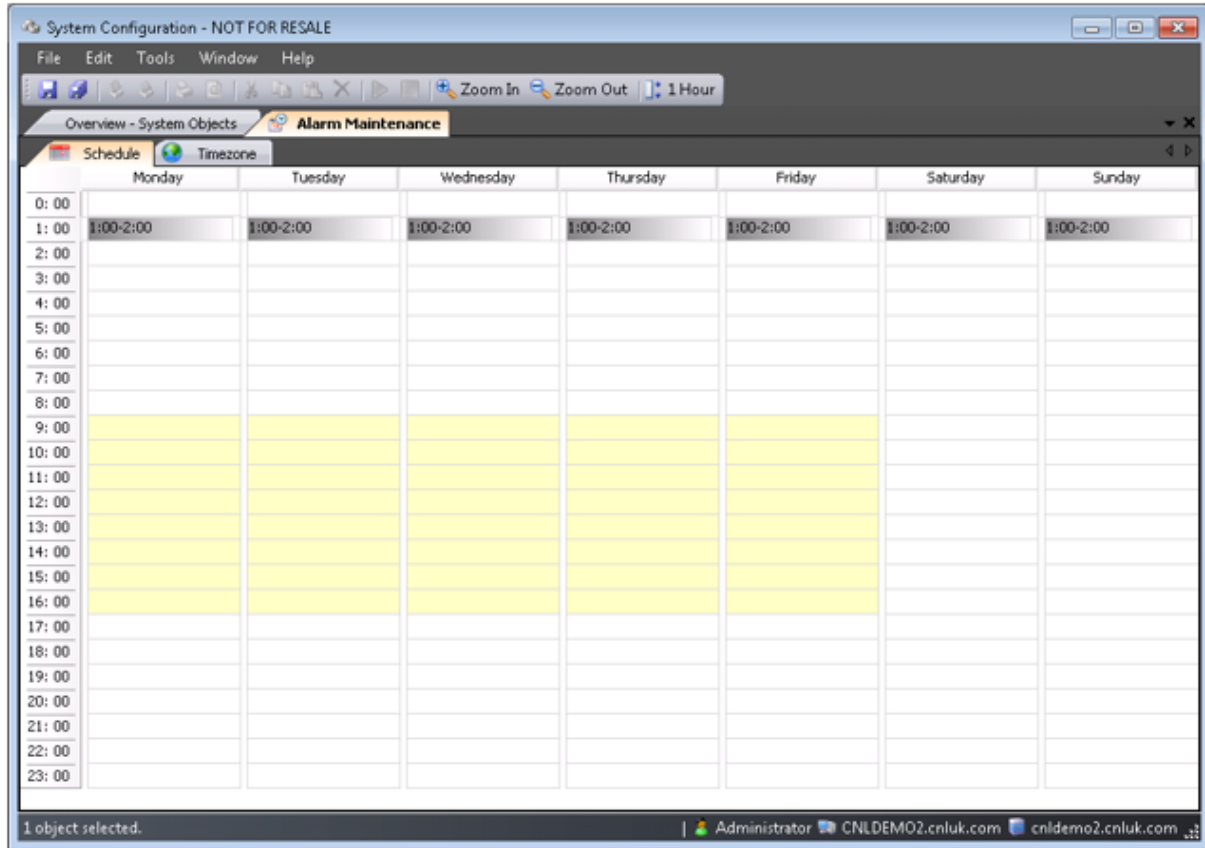
- **Hide Alarm Stack tabs that are not currently in the schedule.**
- **Do not allow users to see alarms if they lack read access to the associated alarm point.**

The process of deleting old data can initially take significant time (many hours). This process will run in the background until the new retention requirements are met.

The process of deleting old data is executed in accordance with the Alarm Maintenance schedule. To change the schedule, double-click **Alarm Maintenance** in **System Explorer**.



The default schedule is configured to execute between 1-2 am every day.

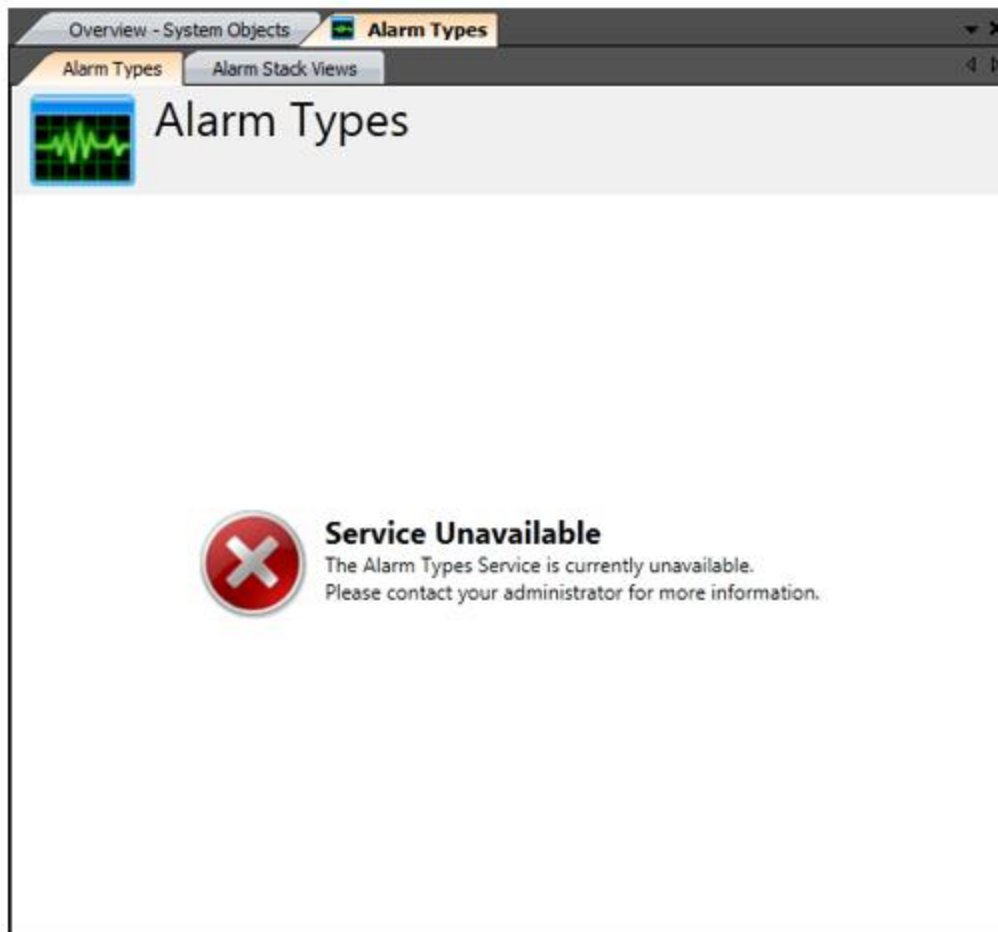


Troubleshooting

The sections below describe some troubleshooting scenarios.

Service Unavailable in Alarm Type Filter

When opening the Alarm Types editor in System Configuration, an error message appears stating that the Alarms Types Service is currently unavailable.



This usually happens when Alarm Types Windows Service is not running or if the Alarms Types Service URL in Global Settings is incorrect. Ensure that the Control Center Alarm Types Event Service is running.

Services (Local)					
	Name	Description	Status	Startup Type	Log On As
Control Center AlarmTypes Service Stop the service Restart the service Description:	ConsentUX_b622f	Allows Con...		Manual	Local Syste...
	Contact Data_b622f	Indexes con...		Manual	Local Syste...
	Control Center AlarmTypes Service	Notifies clie...	Running	Automatic	cnluk\int_a...
	Control Center Audit Server	Control Cen...	Running	Automatic	cnluk\int_a...
	Control Center Connection Mana...	Control Cen...	Running	Automatic	cnluk\int_a...

Caching Large Number of Open Alarms

If a customer has a requirement to keep large numbers of unresolved alarms (more than 10,000), you can increase the alarm cache by editing the following configuration file found in the **Alarm Types Service** application directory:

Everbridge.ControlCenter.AlarmTypes.WindowsService.exe.config

Change the value of the following key as required:

```
<add key="ReadAlarmsCacheSize" value="1000"/>
```

Viewing Recent Alarms and Alarm Events

You can check the latest events and alarms sent from your devices using **Recent Events** and **Recent Alarms**. These viewers are available from within System Explorer and maps.

You can view an event history for:

- Individual devices
- Device shortcuts
- Locations, and all devices within the selected location
- Asset groups, and all the assets within the selected asset group
- A group of devices, locations, or asset groups that you have selected.

To do this:

1. Go to **System Explorer** on the **Main** screen.
2. Find the device whose alarms or events you want to view. You can either:
 - navigate to the device you want from **Locations**
 - find the device on your map.
3. Right-click on the individual device, location, asset group or group of devices and select, either:
 - **View Recent Events**, or,
 - **View Recent Alarms**,
4. Select the time period whose events you want to display.
5. Optionally, you can configure a more specific time using **From date** and **To Date** in the **Recent Events** or **Recent Alarms** window, depending on what you selected in step 2.

Received Date Time	Description	Alarm Point	Location	Event Count
11/21/2019 11:49:20 AM	Device State Changed	UK-CAM-03-Building Lobby	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	UK-CAM-06-Lift Lobby	Building 11	1
11/21/2019 11:49:20 AM	Custom State Changed	CNL-DOOR-02	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-02	Building 11	1
11/21/2019 11:49:20 AM	Custom State Changed	CNL-DOOR-06	Building 11	1
11/21/2019 11:49:20 AM	Custom State Changed	CNL-DOOR-05	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-06	Building 11	1
11/21/2019 11:49:20 AM	Custom State Changed	CNL-DOOR-04	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-04	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-05	Building 11	1
11/21/2019 11:49:20 AM	Custom State Changed	CNL-DOOR-03	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	UK-CAM-02-Building Entran	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-03	Building 11	1
11/21/2019 11:49:20 AM	Custom State Changed	CNL-DOOR-01	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-01	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	UK-CAM-04-Sales Corridor	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	UK-CAM-05-Front Door	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-03	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-02	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-04	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-06	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-01	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-05	Building 11	1
11/21/2019 11:49:20 AM	Device State Changed	CNL-DOOR-03	Building 11	1
11/21/2019 11:49:19 AM	Device State Changed	CNL-DOOR-04	Building 11	1
11/21/2019 11:49:19 AM	Device State Changed	CNL-DOOR-02	Building 11	1

Response Plans

A Response Plan, also called Visual Response Plan (VRP), is a collection of shapes representing program instructions that are executed in accordance with the structure of the shapes when the VRP is run.

Response Plan Shapes

You can use shapes in response plans to design the logic to affect in Control Center. For example, the data shapes allow for a response plan to interact with a database via a data connection, the alarm type shapes allow you to interact with your alarm management functionality, such as process guidance and alarm resolution and geographical shapes allow you to interact with assets in a geographic map.

Basic Shapes

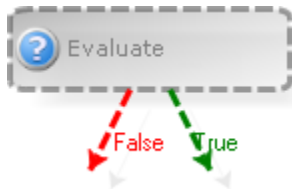
Evaluate

The Evaluate shape provides a True and False route where the chosen path is determined by the specified code. The code to evaluate is added using the script shape editor. The script must therefore result in either a true or false outcome.

For example, to check if a whole number variable is greater than 10, you can add the following script:

“My.PageVariables.varWholeNum > 10”

If that statement is true, then the true route will apply otherwise the false route will apply.



Finish

The Finish shape denotes the end of the response plan. The response plan will cease execution at this point and return control of execution to the point at which the response plan was called, typically, from a Link shape.

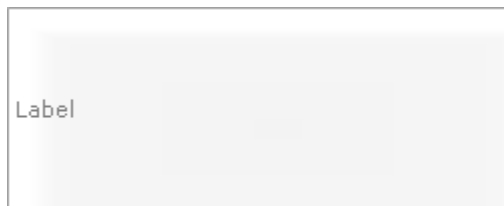
The success state of the Finish shape can be determined which will indicate if the response plan completed successfully or not. This can then be used in the calling logic to take appropriate action; for example, show a message to the user if the response plan failed in some way.

The success state of the Finish shape is denoted by a tick or a cross. The default is a tick which denotes success.



Label

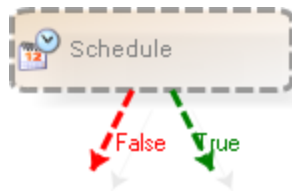
The Label shape provides for annotation of a response plan. It cannot be connected into any other logic and is not executed. Typically, this would be used to further describe the purpose and configuration of a response plan.



Schedule

The Schedule shape provides two paths of execution which are determined based on the status of a specified date time schedule: this date time schedule identifies active and inactive times of day.

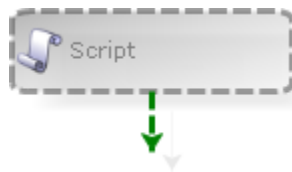
Typically, this is used to determine if the response plan is being executed inside or outside of working hours.



Script

The Script shape can be used to perform multi-lined complex calculations using a combination of Response Plan variables and static data. Typically, this is used to set GUI control values or for functions such as getting the current date and time.

The Script shape editor provides IntelliSense to assist with writing the script. The editor also provides full validation of script to identify any errors or warnings.

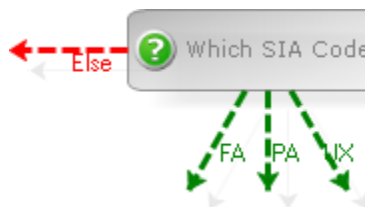


Select

The Select shape provides multiple routes where the route taken at execution is determined by the value of a response plan variable. An editor at design time provides multiple routes to be specified, typically using static values.



For example, a Select shape could be used against a text variable which could contain one of several different values at run-time. The Select shape would therefore be configured with all possible options.



Start

The Start shape denotes the beginning of a response plan. It is present on all response plans and event pages, and can only exist once per page. This shape is added automatically and therefore does not exist in the shapes palette.

Special rules have been included in the designer to prevent the shape from being deleted and preventing routes from any other shape from entering.



Wait

The Wait shape provides the ability to pause the execution of the response plan for a specified number of seconds. This is typically used to slow the execution of the response plan to allow for other processes or actions to be performed before continuing.

The wait interval is set at design time using a whole number or may be specified using a whole number variable allowing for a dynamic value to be specified at run-time.

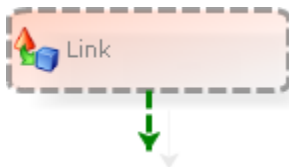


Link

The Link shape allows for a response plan to be executed from within another response plan. The Link shape requires the response plan to execute and then allows for variables within the target response plan to be executed.

This is typically used to create individual, reusable response plans which can be called throughout the system.

For example, a response plan, which may contain several shapes, could be created to send an email. This response plan can then be called from anywhere else in the system by using a single shape and then passing the necessary values to any variables, such as message or recipients.



Remove from List

Use the Remove from List shape to remove a specific item from a list variable. This can be useful when wanting to filter an existing list variable to remove certain items before using the list elsewhere in the solution.

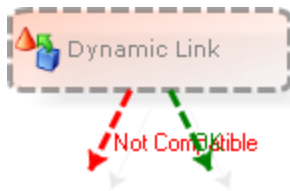
For example, you can use it to remove test cameras from a list that displays all cameras.



Dynamic Link

The Dynamic Link shape allows for the execution of a response plan where the target response plan is not known at design time but is specified using a response plan variable. The variable is then populated at run-time and executed using this shape. VRP inheritance is used to allow for data to be passed into the target response plan and specified at design time. A parent response plan must be created and specified to provide the response plan mappings on the shape.

This shape is typically used when multiple response plans with the same set of variables are required. The response plan to execute would then typically be held in a database and accessed via a data connection and the data select shape.



Go Sub

The Go Sub shape executes a sub-page within a response plan. Sub-pages can be used when logic is required in multiple places within the response plan and therefore reduces any duplication of logic.



Dynamic Action

The Dynamic Action shape executes methods, functions and property changes on both system objects and response plan variables. The values set against the specified targets can also be specified using variables.

A typical use of this shape would be to show a message box to a client where the target client is specified using a variable and the message to show to the client is also specified using a variable. Other typical applications of the shape include running methods on devices, such as opening a door on an access control device or sending an SMS message using a GSM modem.

The shape provides an easy to use wizard to specify the target objects and the actions to run.



Alarm Type Shapes

Alarm Types support several Response Plan shapes that can be used to link commissioned functionality with the Alarm Types feature so that product and toolkit logic interact seamlessly. For example, Process Guidance GUIs, the resolution form and so on. The following Alarm Type Shapes are available in the Response Plan Shapes palette:

Add Threat

The Add Threat shape allows for manual threats to be added into the stack for consideration in the system threat level. The manual threat specified can range from 1 through to 5. A key must also be specified which is then used to subsequently remove the threat.

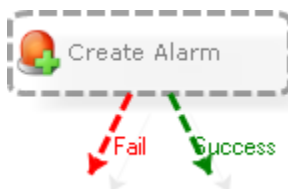
The threat specified will be the minimum value for the system threat level. The system threat will be based on any other manual threats (with differing keys) and any alarms which specify a threat level.

Manually logged threats can be viewed using the Threat Level Grid GUI control.



Create Alarm

The Create Alarm shape is used to create manual alarm types via a response plan. The Create Alarm shape allows for the selection of any alarm types marked as 'manual alarm'. A device and location can also be specified to capture alarm related information.

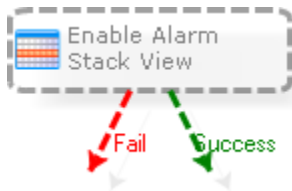


Enable Alarm Stack View

The Enable Alarm Stack View shape will set the availability of the selected view. When disabled, the alarm stack view will not be available to any viewers of the view. The Alarms Stack tab will still show; however, a message will be shown to the user in place of

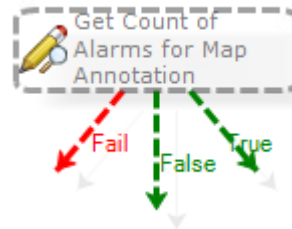
the alarms. However, when the view is enabled, the alarms will start showing back to the user.

Note that the view also includes a schedule property, which can be set to periodically enable and disable a view. This shape, therefore can be used to provide an override mechanism to compliment the schedule option of a view.



Get Count of Alarms for Map Annotation

When a map annotation is provided, this shape will return the number of alarms linked to the annotation. This is typically used to determine whether a map annotation can be removed from the system when a linked alarm has been resolved.



Get Map Annotations

When an alarm ID is provided, this shape will find map annotations linked to the alarm and populate a list variable.

This is typically used together with the Get Count of Alarms for Map Annotation shape in order to remove map annotations from the system once all linked alarms are resolved.



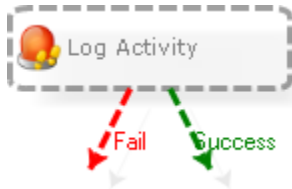
Get Threat Level

The Get Threat Level shape provides a mechanism to retrieve the current threat level in a response plan. The shape will populate a whole number variable.



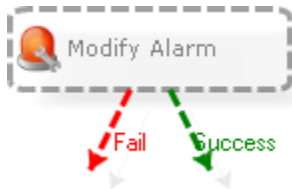
Log Activity

The Log Activity shape adds custom activity to an active alarm together with text comments for a particular user. Most activities are logged automatically by alarm types, such as alarm created, handled or resolved. Custom activities can be logged against any alarm, this is typically used to audit operator activities during the alarm handling process, for example process guidance step complete, which cannot be logged automatically.



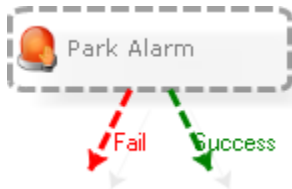
Modify Alarm

The Modify Alarm shape updates the column values for a specific alarm based on the Alarm ID property. The values to update are specified using the Property Mappings property. Alarm types maintain the alarm automatically in most cases; however manual updates might be necessary. For example, running a response plan after an alarm has been created to populate some of the custom columns with data after using data shapes to extract this from a HR database.



Park Alarm

Parks an unresolved handled alarm and marks the alarm as Parked by ... in the alarm stack. This can be incorporated into the alarm handling logic to enable the user to park an alarm for handling by another user or at another time.



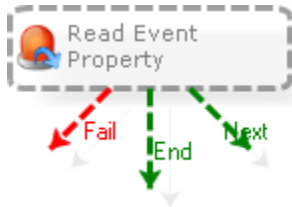
Read Alarm

When an alarm ID is provided, this shape reads properties associated with an alarm into response plan variables. This shape is useful in determining additional information of an alarm, when you only have the alarm ID.



Read Event Property

All events are logged in the Pacific database and then evaluated against Alarm Types. Some of the event data may be required during the alarm handling process. Instead of including logic in a solution to hold any required event data in the Alarm Stack (Card ID or Analytic Zone), you can extract this data in a VRP (Response Plan) using the Read Event Property shape. This shape iterates through all events for an alarm similar to a Data Select shape. You can also specify the order in which to iterate through the events for an alarm to find a specific event. In addition, you must specify a device type and event type so that the shape knows which events to pull from the alarm as an alarm could include different types of events. This helps to pull out the panel reset event for an alarm which contains many fire alarm events.



Remove Threat

The Remove Threat shape will remove a manual threat from the system threat level stack with a key for which a threat exists.



Resolve Alarm

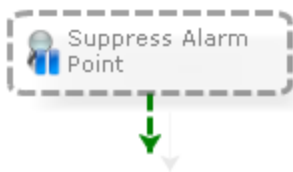
This shape resolves an active alarm based on any of the available resolution types. The status of the alarm must be handled, and the operator specified must match with the operator currently handling the alarm.

This would typically be used in conjunction with the Resolution Types combo box which would provide the operator the ability to select an appropriate resolution type from a drop-down list.



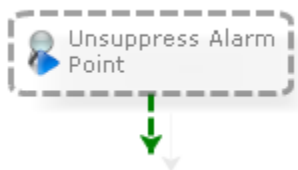
Suppress Alarm Point

Use this shape to suppress one or more alarm points. Suppressed alarm points do not participate in alarm categorization, however events are logged regardless and can be displayed using the Suppressed Event grid. Suppressed alarm points can be shown in the user interface using the Suppressed Alarm Point grid.



Unsuppress Alarm Point

Use this shape to unsuppress one or more alarm points. Unsuppressed alarm points can now participate in alarm categorization.



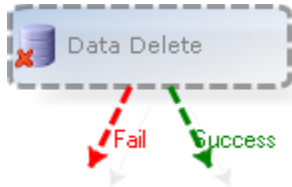
Data Shapes

The data shapes allow for a response plan to interact with a database via a data connection. A data connection is an object in Control Center which details the database instance, database name and any connection credentials. The data connection will then replicate the schema which can then be used within response plan shapes.

All data shapes include a fail route and an Error Text property. The fail route will be taken if the shape is unable to perform the request command. If the fail route is taken, then the Error Text property can be used to populate a text variable for reporting and debugging purposes.

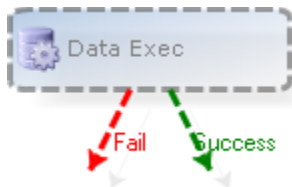
Data Delete

The Data Delete shape will delete all records in a specified table based on the WHERE Clause property. If no WHERE Clause is specified, then all records in the table will be deleted.



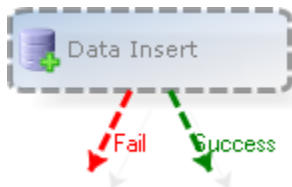
Data Exec

The Data Exec shape can be used to run any stored procedure via a Data Connection. It supports passing parameters in and out of the stored procedure using response plan variables. It can also return the number of rows that have been affected by the stored procedure.



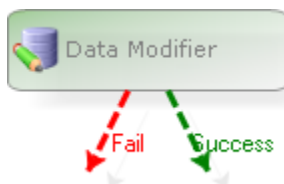
Data Insert

The Data Insert shape will insert a record into a specified table in a database. The shape includes a column mappings property which is used to specify the values for each column. The values can be either statically defined or specified using variables.



Data Modifier

The Data Modifier shape runs complex SQL scripts against a database via a data connection. This can be useful when wanting to execute a script which is not easily managed by some of the other data shapes which break down the common activities into easy to understand shapes.

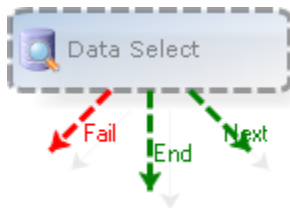


Data Select

The Data Select shape retrieves data from an external data source using a data connection. This shape will iterate through each record returned every time the shape is executed. The first pass of the shape will select the data from the table, for example 4 records are returned, and will take the Next route. Each subsequent execution of the shape will move to the next record and again take the Next route. If no records are available or every record has already been iterated, then the End route will be taken.

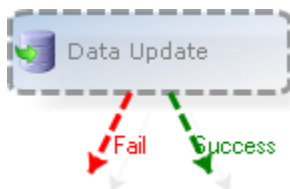
The shape provides a column mappings property to map columns in the table to variables in the response plan, which is used to extract data from each record in the data set.

The shape also includes a WHERE Clause property which can be used to filter the records returned from the database. The script editor is used to specify the WHERE Clause to provide prompts as to the available columns and variables.



Data Update

The Data Update shape will update records in a specified table based on the column mappings specified for the shape. A WHERE Clause property is available to determine which records in the table are updated otherwise all records will be updated by default.



Device Shapes

Display Tile Layout on Video Wall Device

The Display Tile Layout on Video Wall Device shape enables tile layouts to be shown when they are on a Video wall instead of the Client.



Get Connected Devices

The Get Connected Devices shape enables you to determine the list of connected devices for a specified device. For example, you can determine the Parent Object of the camera or any other object the device belongs to.



Get Idle Preset

The Get Idle Preset shape will accept a camera and return the specified idle preset based on the visible object mapping feature in Control Center, where active and idle presets can be specified for each mapping.



Get Preset

Similar to the Get Idle Preset shape, the Get Preset shape will return a preset position based on a specified camera and a specified viewed object. Typically, this shape is used along with the Get Visible Objects shape by populating a list with the visible objects, iterating through the list, and using the Get Preset shape to retrieve the preset for the pair of devices.



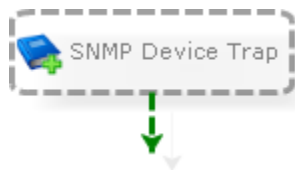
Set Tile Contents on Video Wall Device

Use the Set Tile Contents on Video Wall Device shape to display tile layouts and custom layouts on a video wall device.



SNMP Device Trap

Use the SNMP Device Trap shape to broadcast an SNMP message sent to a device, message string, timestamp, and event type. Use the SNMP Device Trap shape to compliment the online state messages which are broadcasted by the connection manager service.



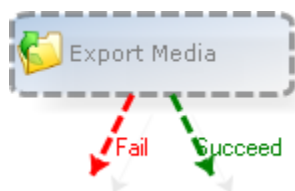
This shape is not available in GUI event pages.

Evidence Bank Shapes

The evidence bank shapes provide functionality to support creating evidential packs on a network drive which contain exported video and reports.

Export Media

Use the Export Media shape to export a media object from the system to a local or network drive. This could for example be used to save a generated PDF report to a network drive as a backup measure.



Submit Video Export Job

The Submit Video Export Job shape creates a new job in the video export service based on a specified set of cameras, folders, or locations. The export destination, footage start time and footage end time must be specified.

Once executed, the shape registers the new job with the video export service and return details of the job back into the response plan using different properties which can be set against variables. These include the estimated job size, export duration, completion time and a unique identifier which can be stored for reference and later used for reporting purposes.

Optionally, you can configure Email addresses, subject and message, if you want to email your video export. For example, if the video needs to be made available for forensic review.



Geographical Shapes

Get Assets Within Radius

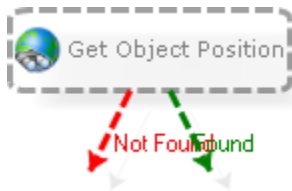
The Get Assets Within Radius shape will search for different types of objects in the system based on a specified latitude, longitude and scene. The shape will populate a list variable with the returned objects which can be determined using the Types to Include property.

The shape includes additional properties to further contain the search. These include the maximum search distance, the maximum search distance unit (default kilometers), and the maximum number of results to return (default 10).



Get Object Position

The Get Object Position returns the geographical position of a specified object. The shape also requires a geographical scene to be specified to determine the object position. The position is returned as latitude and longitude which can be stored in variables of type decimal number.

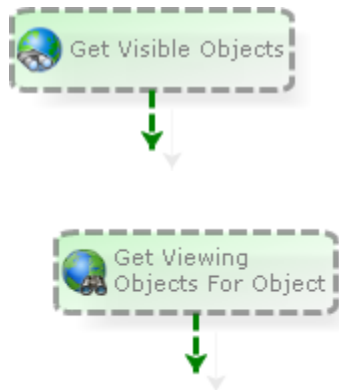


Get Viewing Objects for Object

Much like the Get Visible Objects shape, the Get Viewing Objects for object shape will populate a list variable with objects, except that this shape could also include a PTZ variable with objects visible to a device specified as configured using the visible object mapping feature in Control Center. Additionally, you can specify the types of objects to return and a PTZ Preset value.

Get Visible Objects

The Get Visible Objects shape will populate a list variable with objects visible to a specified object as configured using the visible object mapping feature in Control Center. Additionally, the types of objects to return must also be specified.



List Shapes

Use list shapes to manage list variables in a response plan. For example, when configuring logic in the solution to send a message to several clients, a client list variable must be created, then populated with the Add to List shape and then iterated through using the Iterate Collection shape. This can be useful to quickly retrieve contents for a folder or location.

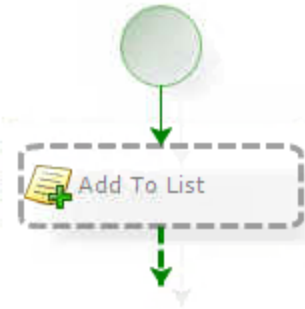
Other response plan shapes also support list variables directly. For example, the Generate Tile Shape will accept a device list variable and then generate a tile layout based on the contents of the list.

List variables can be either basic or referenced. A basic list will simply contain multiple values of the same type. However, each item in a referenced list will be keyed by a unique value. An example of a referenced list would be a list of response plans each referenced by a number or a list of clients each referenced by some unique text/key.

Add to List

The Add to List shape adds objects to a list variable, enabling Control Center to iterate through a list of items and perform a function on each item, in a loop, until the list is completed. A typical use of this shape is to populate a device list variable from a location or to populate a client list variable from a folder.

1. Add items to a list variable. A list variable can have either statically defined objects, variables or objects from a folder or location.



Add New Variable ✕

Add Variable

Basic Properties

Label

Type

Scope

Visibility

List Properties

Do not make a list

Make as a basic list

Ensure contents are unique

Make as a referenced list

Reference each item in the list using the following type:

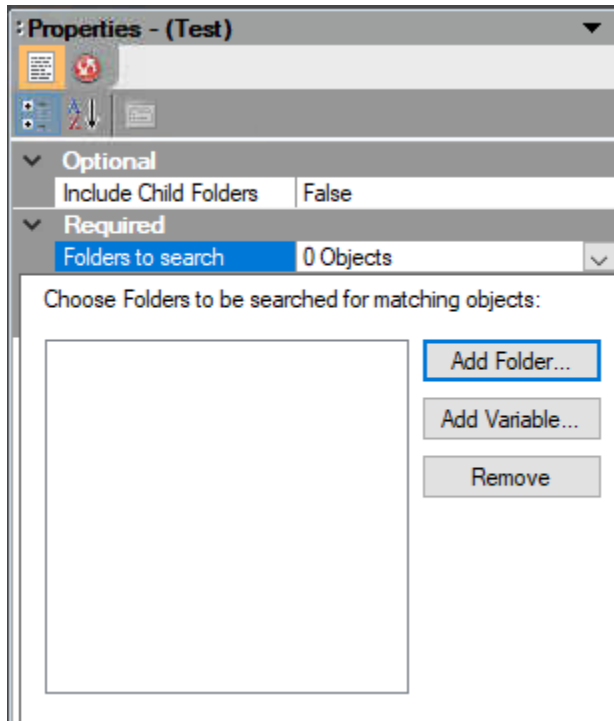
Comments

2. The Add to List shape has 3 properties.

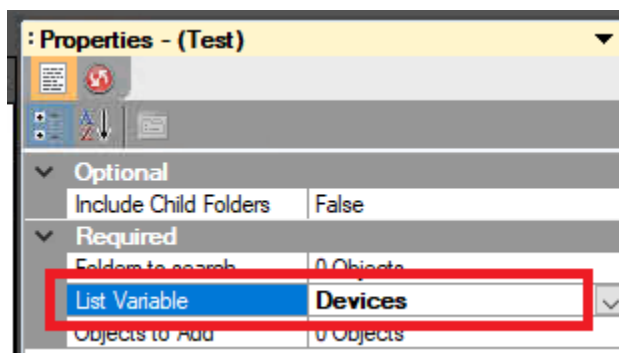
Properties - (Test)	
<div style="display: flex; align-items: center; gap: 5px;"> ⌵ ⌵ ⌵ ⌵ </div>	
Optional	
Include Child Folders	False
Required	
Folders to search	0 Objects
List Variable	
Objects to Add	0 Objects

The **Properties** dialog displays that all 3 properties are **Required**. In fact, you should select either **Folders to search** or **Objects to Add**, depending on your requirements.

- (Optional) **Folders to Search** – select this if you want the Add to List shape to search a folder or location (including child folders and locations) for matching object types.
 - Select **Add Folder...** for a static defined folder or location.
 - Select **Add Variable...** for an existing, populated variable for either location or folder in the current response plan.

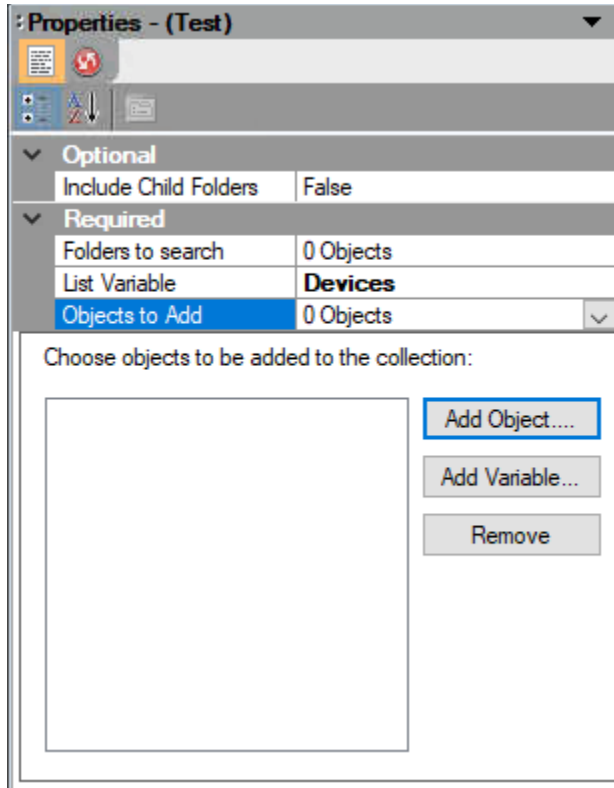


- (Required) **List Variable** – the list variable you defined in step 1.



- (Optional) **Object to Add** – select this if you to add specific objects (either a variable or a system object) for the Add to List shape to search for.

- Select **Add Object...** if you want to search for, and add, static system objects.
- Select **Add Variable...** if you want to use an existing, populated object variable of the matching type to the list.



The method that you choose depends on how you want your objects to be added to your list.

- If you know the populated object variable (accessible to the same response plan as the Add to List shape) and you want to add it to a list, select **Objects to Add > Add Variable...** to define the object variable to add.
- If you want to add some static system object items to a list, select **Objects to Add > Add Object...** to open the **Search** dialog to select the objects to add to the list.
- If you want Control Center to dynamically populate the list with objects in a folder or location, select **Folders to search**, with either a static (search for a system folder/location) or a dynamic folder or location (in other words, a populated variable accessible by the response plan), depending on your requirements. In either situation, the **Include Child Folders** setting can be used to define if child folders within the search folder should also be searched and any objects also added to the list.

Clear Collection

The Clear Collection shape will simply clear the contents for a specified list variable.



Iterate Collection

The Iterate Collection shape will loop through the contents of a list variable taking the Next route for each item in the list. The value of the current item in the list can be referenced using a response plan variable.

An example of this shape would be to iterate through a list of clients. Each pass of the shape would result in the current value property populating a specified variable. The updated variable can then be used in other logic such as a Dynamic Action shape to show a message box to each client.



Multi Processing Shapes

Join

Use the Join shape after a split shape to continue execution once all paths into this shape have completed. The shape will wait for all incoming paths to complete before continuing.

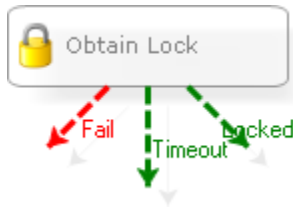


Obtain Lock

The Obtain Lock shape is used to create a lock in the system based on a specified lock name. This can be used when logic must be executed sequentially and not in parallel to avoid race conditions. The use of a specified lock name means that the response plan can run multiple times in parallel however no two instances of the same lock name will ever run at the same time.

A timeout property is provided to determine the maximum duration to wait to obtain a lock. The timeout route will be taken if the shape is unable to obtain the lock in the specified duration due to an existing lock for the specified lock name.

The Release Lock shape must then be used after the required logic to release the lock for the next pass.



Release Lock

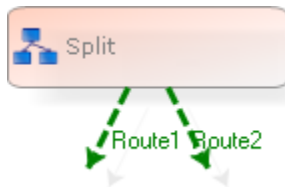
The Release Lock shape will remove any active lock based on a specified lock name so that subsequent executions of the logic using the same lock name can execute.

Locks will also be cleared when the server starts to ensure that deadlocks are not possible.



Split

The Split Shape provides multiple paths of execution for running logic in parallel. Several Splits properties are available to determine the number of routes out of the shape. Use a Join shape to collect all the different routes back into a single path of execution.

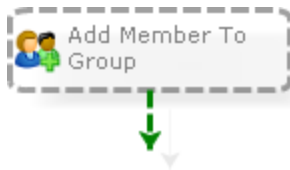


System Shapes

The system shapes contain various shapes used to interact with system objects. This includes assigning, moving and deleting objects, managing user/group membership, and various forms of searching for objects.

Add Member to Group

The Add Member to Group shape can be used to add a user/group into a group or add a contact/contact group into a contact group.



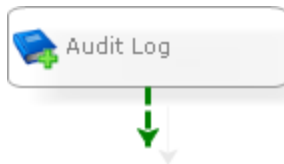
Assign Variable

The Assign Variable shape will assign the value of a specified variable to reference an object in the system. Typically, this shape would be used prior to executing other shapes which utilize the variable; for example, the shape could be used to assign a device variable to a camera in the solution before showing the camera to a user.



Audit Log

Use the Audit Log shape to insert an entry into the Windows event log. This shape allows for the message and event ID to be specified using either static values or variables. This can be useful for collecting system diagnostics in the background to help report on usage, warning, exceptions, etc.



Authenticate Client

The Authenticate Client shape forces the specified client to re-authenticate. This can be useful when wanting to verify that the currently logged in user is permitted to perform a mission critical action. This helps to avoid such issues as an unauthorized operator using a workstation that has been left logged in and unattended.



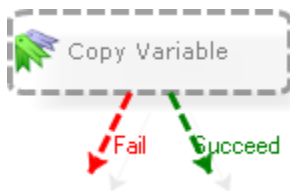
Copy Object

The Copy Object shape duplicates an object referenced by a response plan variable.



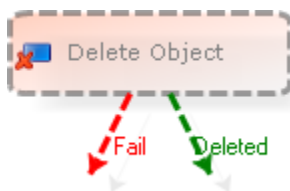
Copy Variable

The Copy Variable shape is used to copy the value of one variable into another. The shape has two required properties: a source variable to copy from and a target variable to copy into. If the shape can populate the value of the target with the value of the source variable then the success route will be taken, otherwise the fail route will be taken indicating a mismatch.



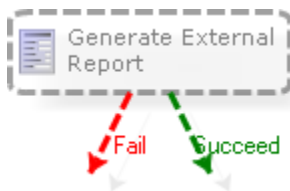
Delete Object

The Delete shape will delete an object in the system based on the value of a response plan variable. Deletion will fail if the object is referenced by another object.



Generate External Report

The Generate External Report shape can be used to generate a report based on an external report service such as SQL Server Reporting Services. The shape allows for the selection of the report template, format, label and folder. Parameters in the report can also be specified from variables in the response plan.



Get Environment Variable

The Get Environment Variable shape can be used to populate information related to Control Center in response plans as variables. It returns the required value into a String variable. The shape can also interpret the name of the Environment Variable as case sensitive or case insensitive.

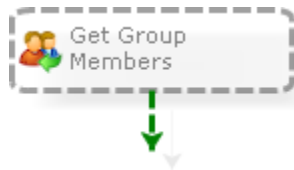


For Federated Sites, the environment variables can only be accessed on a local site. When a Response Plan is being published to a remote site, both sites must be running a version of software that includes the new shape otherwise the Publish operation will fail.

Get Group Members

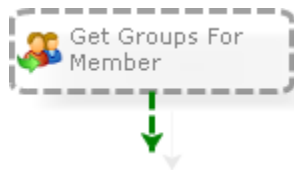
The Get Group Members shape can be used to populate a list variable with members of a specified group. The type of the list variable will determine which members of the group will be retrieved. For example, a user group can include members of type user and user group. Therefore, specifying a user list variable will extract all users from the group. A second shape must then be used to extract any groups that are members.

An Iterate Collection shape must then be used to extract each value in the list.



Get Groups for Member

The Get Groups for Member shape will return a list of groups or contact groups based on a specified member. The specified member could be a user, contact, group or contact group.



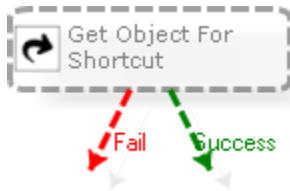
Get Location

The Get Location shape is used to find a location for a specified object, for example a camera. The shape will search through the system for all locations and populate a location variable based on the specified object. The type of location can also be specified which can be useful when iterating up through a tree of locations where a specific level must be returned, for example return the 'building' location rather than the room or the floor.



Get Object for Shortcut

The Get Object for Shortcut shape can be used to get an object in the system based on a specified shortcut. This can be useful to determine the parent object when only the shortcut is available in the response plan.



Get Placeholder

The Get Placeholder shape searches through the system for a placeholder with the parent device and the device data. The shape will then populate a placeholder variable if one is found. The shape can also be configured to automatically create a placeholder if one is not found based on the specified search criteria. This option can then be used to configure a solution to automatically grow and maintain itself over time. Care must be taken to not exceed the allocated license count for placeholders.



Get Shortcuts

The Get Shortcuts shape will return a list of shortcuts for a specified object. The list of shortcuts can then be expanded using the iterate collection shape.



Import Media

The Import Media shape will import a media file from the local drive into the system. For example, you can use this shape to import PDF files or image files which can be used elsewhere in the solution.



Log to Audit Database

You must have configured your Auditing Server in Control Center before you can use the **Log to Audit Database** shape. See [About Auditing in IPSecurityCenter](#).

Using a Log to Audit Database shape in your response plan allows you to audit interaction with any of your response plans, including reacting to an event from a connector and auditing any important information. For example, you may want to see which user paused a video, resolved an alarm and deleted a user from the Users group on your system at a specific time.

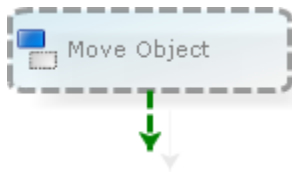
The Log to Audit Database shape has the following properties:

Name	Required ?	Description
Event Type	Y	The event type you want to audit. For example, a camera. The event type can be a static value or a variable.
Object 1	Y	Any Control Center object. For example, a Sequence
User	Y	The user who performed the interaction.
Operation	Y	The operation that has been performed. For example, pause, step forward or step back.
Client	N	The Control Center Client where the action has taken place.
Object 2	N	Allows you to specify another Control Center object.
Extra Information	N	Any extra text you want to provide for information.

The audit data are written to the Audit database schema. See [About Auditing in IPSecurityCenter](#).

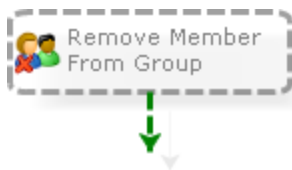
Move Object

The Move Object shape can be used to move an object into a specified folder. This can be useful when configuring the solution to dynamically maintain its configuration. For example, this shape can be used to move automatically created placeholders into different locations.



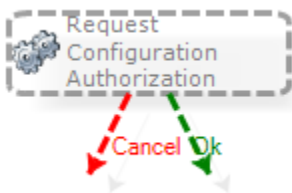
Remove Member from Group

The Remove Member from Group shape can be used to remove a member from a group or contact group.



Request Configuration Authorization

The Request Configuration Authorization shape is used to prompt the current user to request authorization.



The shape displays the request dialog and if the user submits a request, will go down the OK route. If the user cancels the request, it will go down the Cancel route.

When a user submits a request, the request will appear in the Authorization Request grid for approvers to approve. See *Secondary Authorization* for more information.

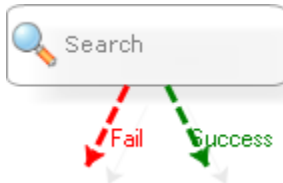
Search

The Search shape will populate a target variable (regular or list) with objects in the system based on specified search criteria. The type of object to search for will be based on the type of the target variable. In addition to the target variable to populate with the results, the shape also requires a search value by which to search, an operator, and the property to search.

The operator provides a multiple choice of different operators which includes (not exhaustive) 'equals', 'less than', 'greater than', 'starts with', 'contains', etc.

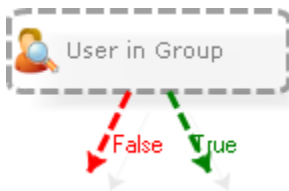
The property to search will be based on the target variable. The available properties to select from will be determined by the type of the target variable. For example, specifying a location variable as the target variable will result in the property to search including items such as 'label', 'address 1', 'address 2', 'location ID', etc.

If multiple results are returned by the search and a list variable has not been specified as the target, then the first item in the set of results will be used to populate the target variable.



User in Group

The User in Group shape is used to check if a user/contact is a member of a specified group/contact group. This shape can be useful when validating user membership within a response plan.

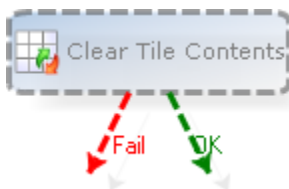


User Interface Shapes

The user interface shapes in a response plan allow for the logic to affect the user interface, typically of the current client. Most shapes utilize tile layout variables to contain the user interface contents which are then shown to the user.

Clear Tile Contents

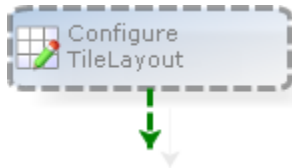
The Clear Tile Layout shape will clear the contents of a specified tile of a tile layout variable. The tile layout must then be displayed to the client to apply the changes.



Configure Tile Layout

The Configure Tile shape allows for individual tiles of a tile layout variable to be populated with GUIs, including Addons, or devices. An editor is provided to specify which content should be placed into which tiles.

A Display Tile Layout shape must then be used to show the tile layout variable to the user.

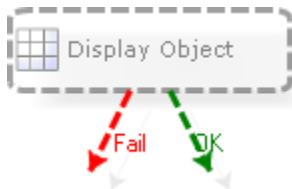


Display Object

The Display Object shape can be used to display one or more cameras or GUIs (including Addons) to the user. Unlike the Display Tile Layout shape which requires a Tile Layout variable, this shape can directly show a GUIs or cameras and dynamically create a containing tile layout when displayed.

This shape should be the primary option for displaying content to end users.

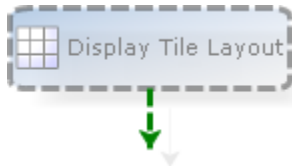
The one limitation with this shape is that it cannot update the contents of a currently displayed GUI, for example changing the current location on a Google Earth GUI. In this instance, the Configure Tile Layout and Display Tile Layout shapes should be used where the Update property on the Display Tile Layout shape can be used to persist and update any currently shown content.



Display Tile Layout

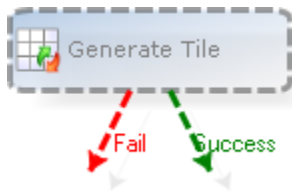
The Display Tile Layout shape displays a tile layout variable to one or more specified clients or users. The tile layout variable must be populated prior to this shape using some of the other user interface shapes. Alternatively, no changes can be made to the variable in which case the default contents of the specified tile layout will be shown.

The shape requires a tile layout variable to be specified, as well as a target display area and one or more target users/clients.



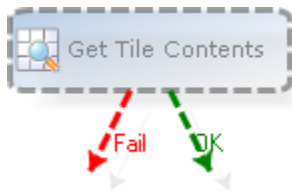
Generate Tile

The Generate Tile Layout shape can be used to build up a tile layout variable based on one or more GUIs, devices or sequences. The layout used will be dynamically determined based on the number of items specified. For example, specifying a list of 4 cameras will result in a 2x2 layout being used.



Get Tile Contents

The Get Tile Contents shape populates the value of a specified variable with the contents of a specified tile. This is useful for extracting the contents of a tile layout into a variable for further analysis however the Get Tile Contents from Client shape is more useful as this can retrieve the contents directly from the client rather than from the tile layout variable which may not reflect that shown on the client.



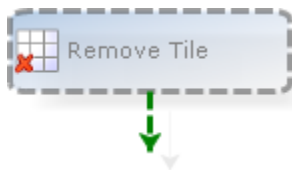
Get Tile Contents from Client

The Get Tile Contents from Client shape can be used to populate the value of a response plan variable (GUI, device or sequence) with the contents of a specified tile from a specified client. This could be used for example to send the contents of the local spot monitor to the video wall when clicking a button on the main menu.



Remove Tile

The Remove Tile shape removes a tile layout from a specified group of users, clients and display areas. However, the Close UI shape is more effective as this only has one property.



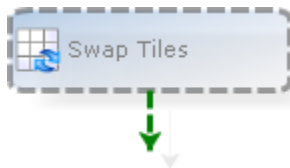
Set Tile Contents

The Set Tile Contents shape sets the content of a specified tile to the value of a specified variable. This is similar to the Configure Tile Layout shape; however, a whole number variable can be used for the target tile.



Swap Tiles

The Swap Tile shape will swap two specified tiles within a layout. This can be useful when needing to move a smaller tile into a larger tile for improved viewing.



Tile Action

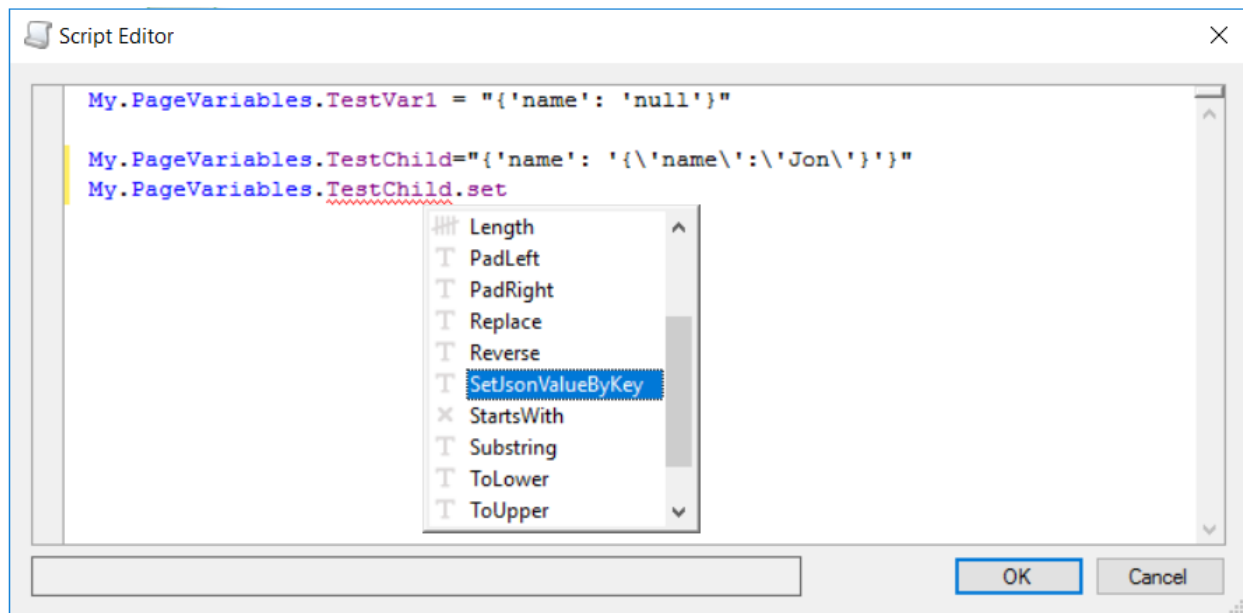
Use the Tile Action shape to perform an action against a specified tile in a tile layout. For example, the shape can be used to automatically take a snapshot, switch to playback, move to a preset, and so on.

To use the shape, you must specify the target client, tile layout, and tile number to perform the action. Where applicable, the shape also supports parameters to be specified when executing the command, for example the preset position to move to.



Using JSON in Response Plans

JSON Object Creation

It is possible to both read and write JSON data structures and store in text variables that can be used in Response Plans, using the `SetJSONValueByKey(string key, string value)` method.



An example of where this could be used is if form data has to be stored while handling an alarm. For instance, if a visitor management form has to be completed as part of a gate-entry process, where an operator handles a gate-intercom call and there is a new visitor. As part of process guidance, the operator enters the visitor information which is then saved as a JSON object and stored in the custom text property of the alarm. This data can then be passed on to the visitor management system at a later stage in the alarm handling process.

 Visitor Management
 ✕

Date: 26/02/2019

Name	From	To	Responsible
Luke Jones	1/1/2020 12:00:00 ...	1/1/2021 12:00:00 ...	Aimen Nicolson
Lisa Lake	1/1/2020 12:00:00 ...	1/1/2020 12:00:00 ...	Dave Fenchurc
John Smith	1/1/2020 12:00:00 ...	1/1/2020 12:00:00 ...	William Handle

Visitor Name:

Authorized Date:


Purpose:

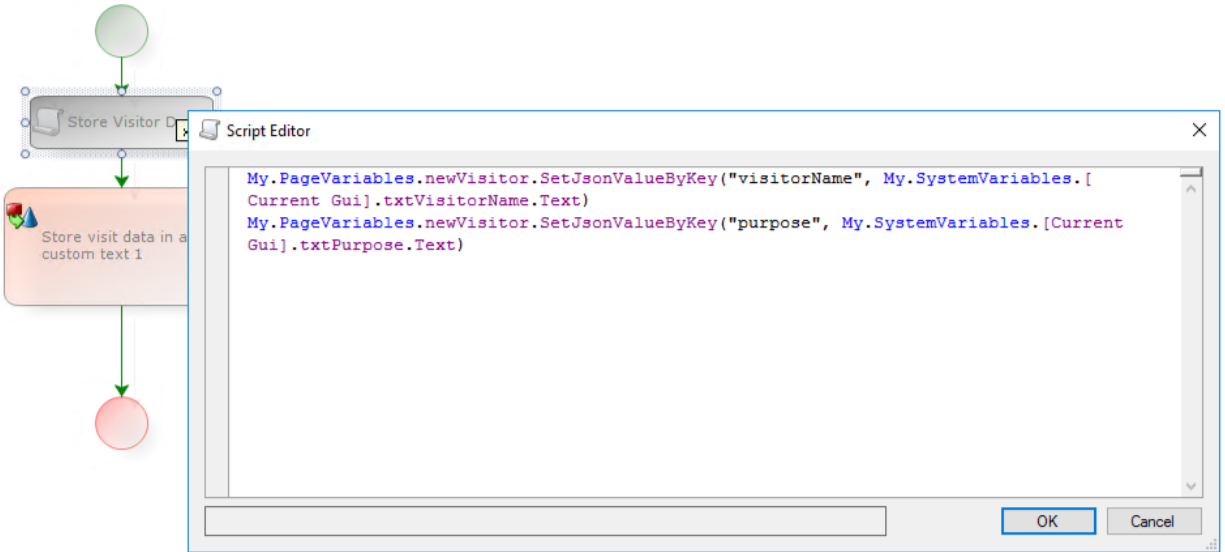
Supervisor:

Vehicle Plate:

Phone No:

ID Number:


Submit Request

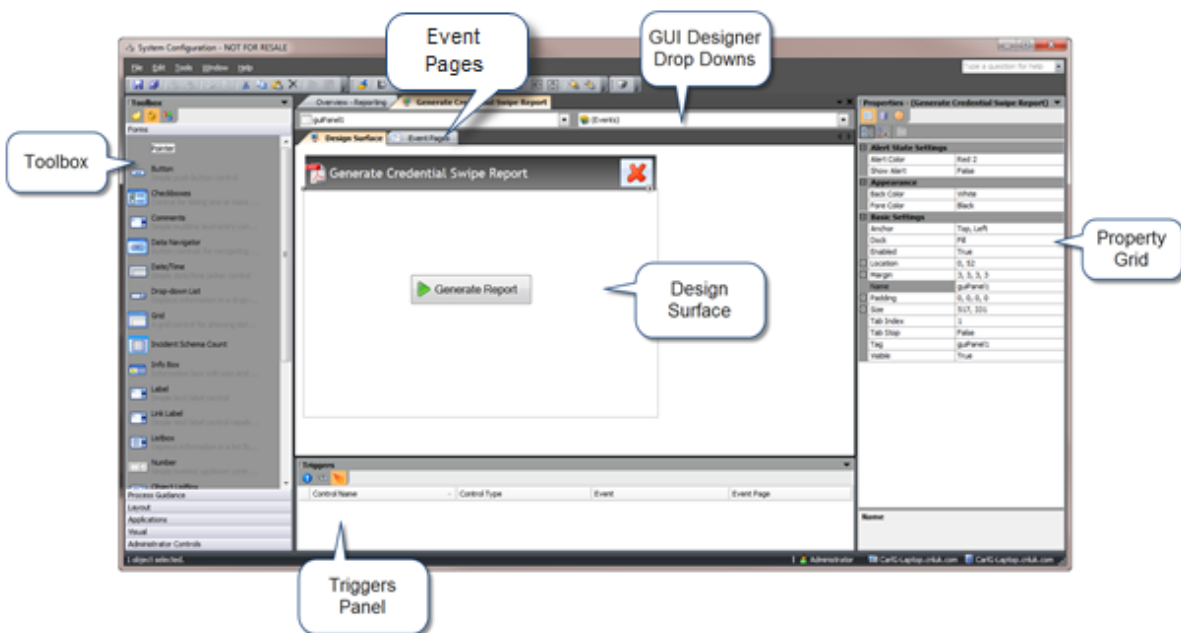


Graphical User Interfaces

The Graphical User Interface (GUI) object provides a platform to design and manipulate GUIs. The GUI Designer allows you to select from a list of GUI controls and place them on the design surface in the order you like.

You can also create triggers from events that may occur within the GUI, for example, when the user clicks a button. Event Pages can be defined to specify when to react to events, such as running actions, initiating Response Plans, and so on.

In addition, you can also control GUIs from a Response Plan to create advanced dynamic interfaces that react and change depending on the status of the system.



The GUI Editor has the following controls:

- **Toolbox** - Contains a palette of user interface controls. You create a GUI by dragging and dropping controls from the Toolbox to the Design Surface. The controls are grouped together into blocks based on their usage. For example, Windows Controls and Cluster Controls.
- **GUI Designer drop-downs** - The following drop-down lists are available in the GUI Designer:
 - **First drop-down** - Lists all user interface controls placed on the GUI. Choosing a control from this list selects that control on the Design Surface.

- Second drop-down - Lists the events that can be raised by the currently selected control. Selecting an event enables you to specify how to react to that event by defining or selecting an Event Page to run behind the GUI.
- Properties grid - Displays the associated properties of the User Interface control that can be configured. There is a group of common properties to aid in design layout and arrangement.
- Design Surface - The main area of the GUI Designer. It is where you create a Graphical User Interface by placing the user interface controls from the Toolbox on the left to render visual elements on a GUI.
- Event Pages - Provides a mechanism for reacting to GUI control events. This is where you see the events raised by GUI and react to events generated from controls on your GUI. The GUI Designer has a built-in Event Page editor to provide a mechanism for reacting to GUI control events via Event Pages. When the Event Pages tab behind the Design Surface is selected, the built-in Event Page Editor opens.

Creating a Simple New GUI

To create a new GUI for generating a Credential Swiped report.

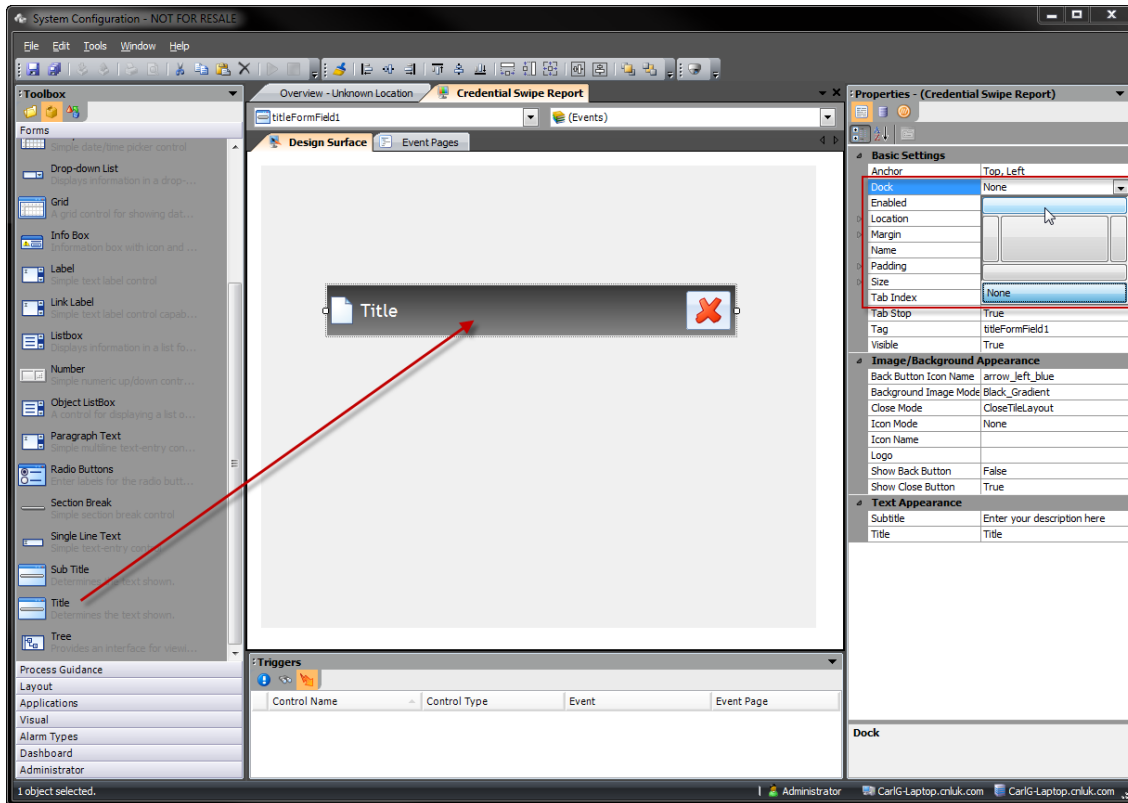
To create a new GUI:

1. Right-click anywhere within the **Reporting** folder and select **New > Graphical User Interface**.
2. Rename it to **Credential Swipe Report**.
3. Right-click the GUI and select **Generate Tile Layout**. This will create a one-way tile layout with the GUI stored in the first tile. To display a GUI, you must use a tile layout. Tile layouts specify the number and layout of the individual tiles shown within the designated display area. For example, a 1-way tile layout would fill the entire display area with the GUI being displayed, whereas a 4-way tile layout will display a grid with four tiles that can be laid out in multiple ways. For more information, see [Tile Layouts](#).

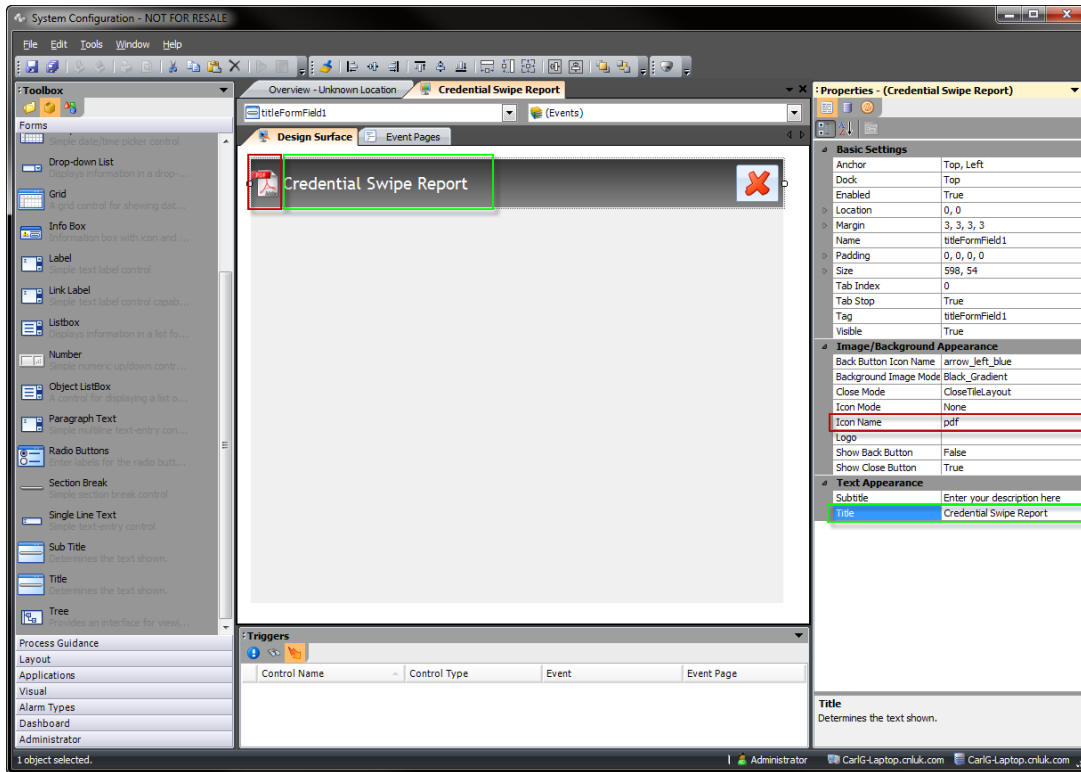
Similar to the Report Designer, controls can be added to the Design surface by dragging them from the toolbox on the left panel.

To add a GUI control:

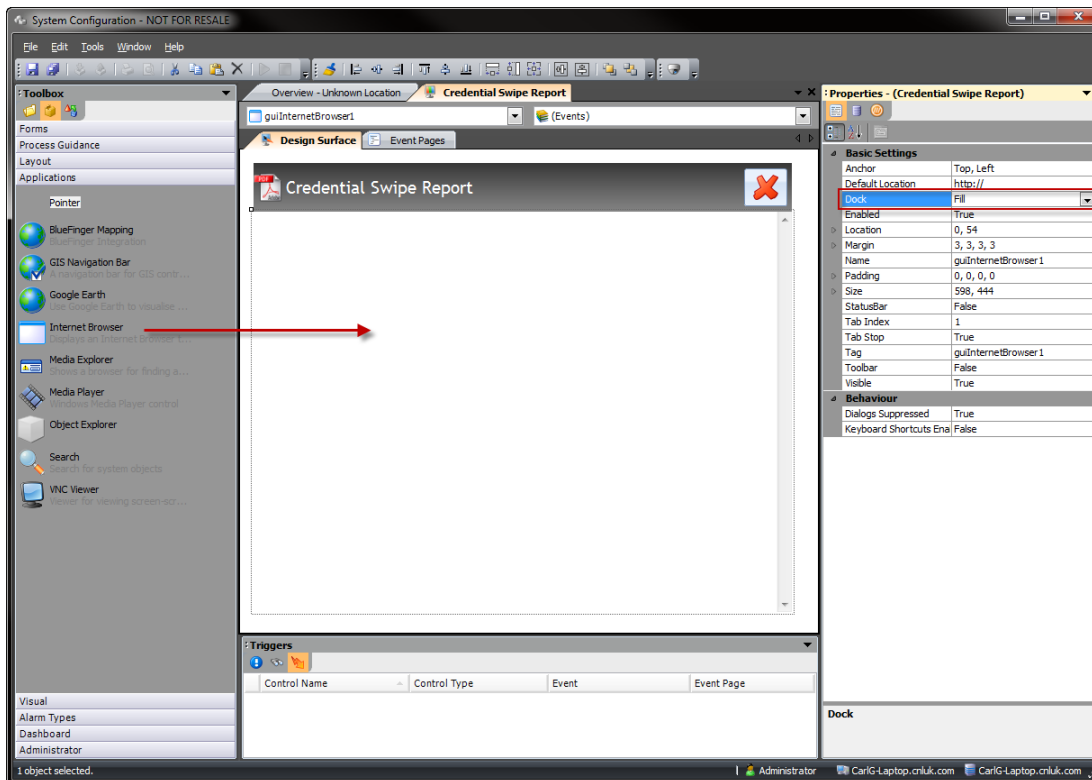
1. Drag the **Title** control and drop it to the design surface.
2. Set the **Dock** property to the top position.



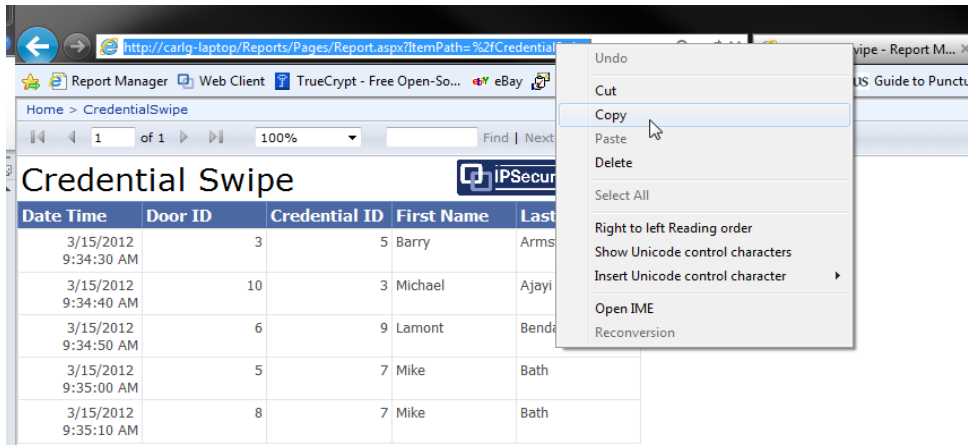
3. In **Properties**, rename the title to **Credential Swipe Report**.
4. Set the icon name to **pdf**.



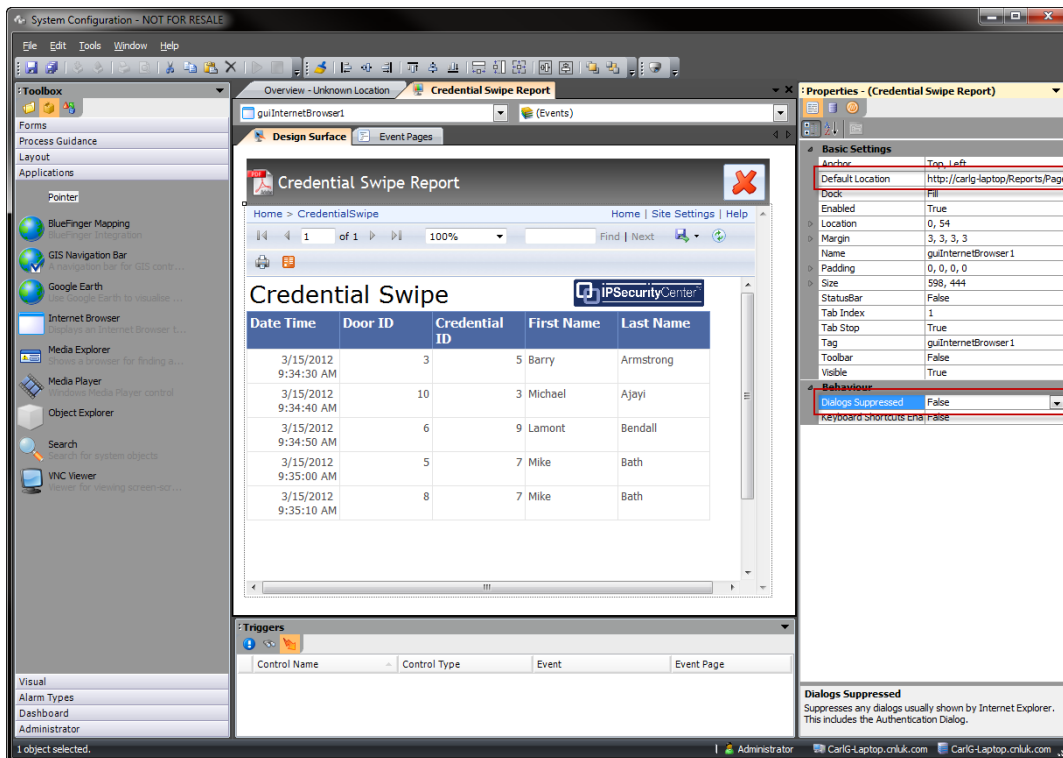
5. From Toolbox > Applications, drag the Internet Browser control.



- Open Internet Explorer and copy the Credential Swipe Report URL into the clipboard.



- Go back to the GUI designer in System Configuration and select the Internet Explorer control.
- Set the following properties:
 - Default Location** - path copied from Internet Explorer
 - Dock** - Fill
 - Dialogs Suppressed** - False



The GUI will show all controls available in the Report Manager. To restrict the controls available to the end user, the report can be loaded with fewer controls. Use the following URL in the Default Location property while making sure that the report name is correct.

<http://localhost/ReportServer/Pages/ReportViewer.aspx?/CredentialSwipe&rs:Command=Render>

Where *localhost* is your machine name. <http://localhost/ReportServer/Pages/ReportViewer.aspx?/CredentialSwipe&rs:Command=Render>

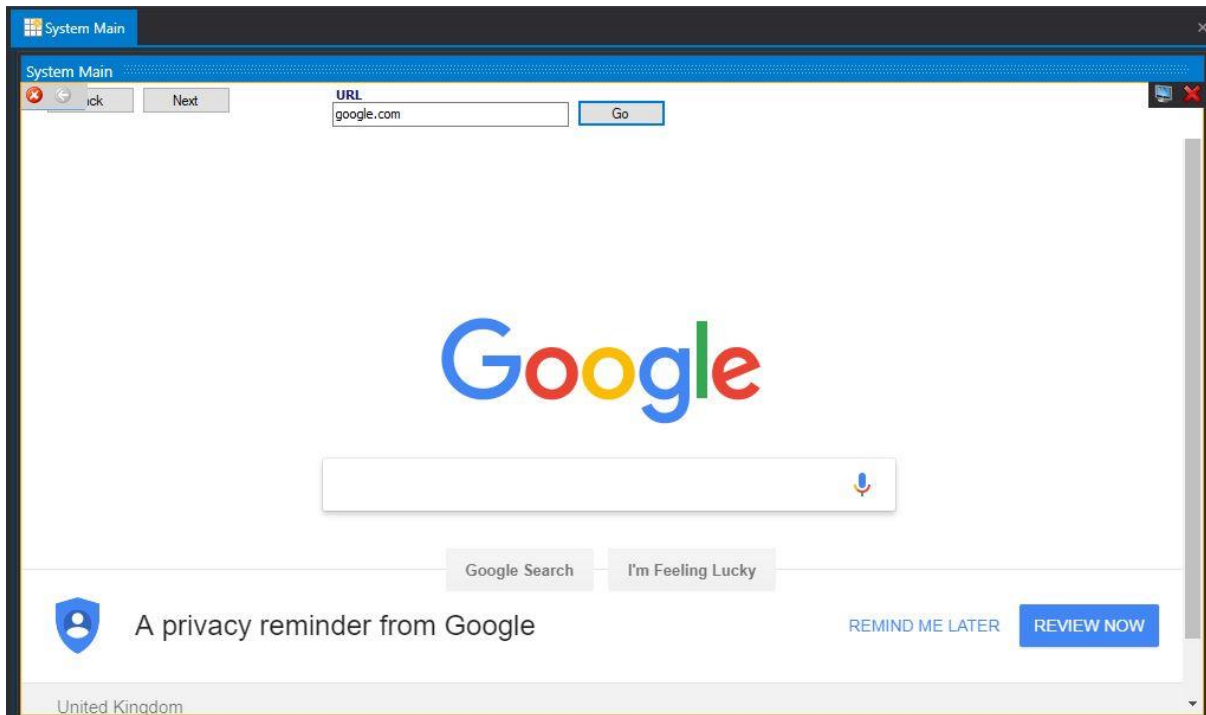
9. Save and close the GUI designer.
10. Locate the tile layout that was created at the beginning of the exercise and right-click it to select **Display Tile Layout > Right**.

Chromium Web Browser Plug-in

GUI framework can be used to display the plugin controls and manage it very effectively.

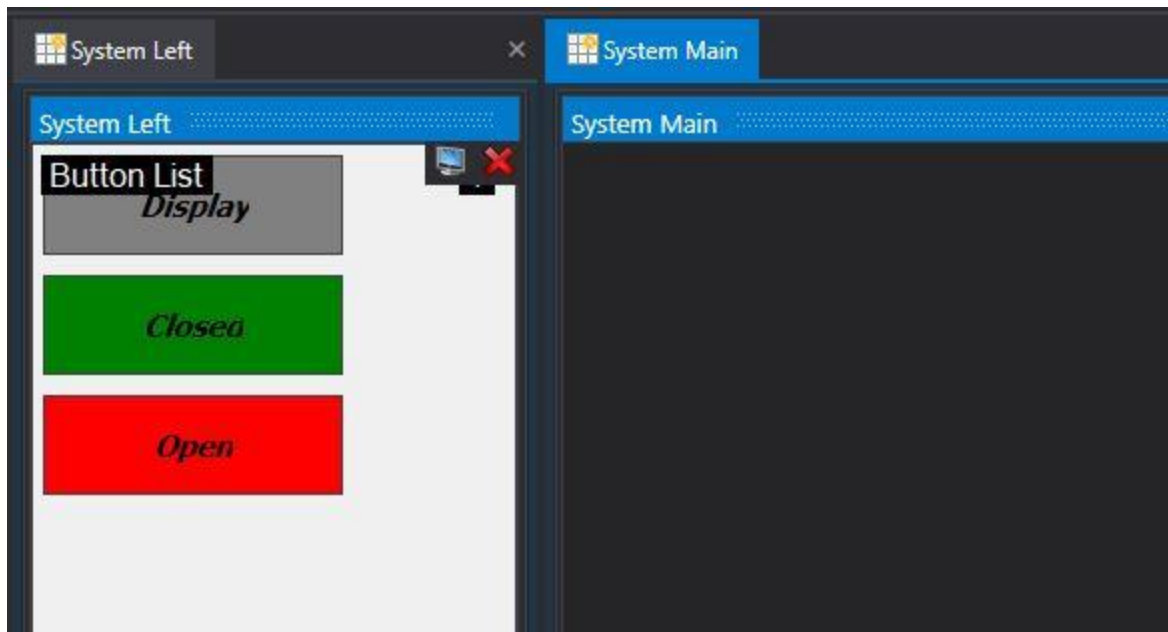
The Control Center is equipped with a Chromium Web Browser plug-in component that adds a specific feature to the application which integrates web-based framework within Control Center for viewing web pages or web reporting from a reporting server. This also extends its support for JavaScript and other technologies to be used within the browser and facilitates customization by the user as well by providing control to add button/buttons and assign it to perform a task on the web page. For example: Back, Next, Stop, and Go.

Apart from browsing the web pages, this feature can also be used to view web reporting by specifying the URL address to the reporting server. By establishing connection to the server, you will be able to view real time reporting or historic reports stored on the server.



Button List Plug-in

The Button List Plug-in is an add on feature of Control Center 5.9 which allows the user to create a Graphical User Interface and dynamically add the custom button/buttons which when clicked are defined to perform a certain task scripted in the response plan. The buttons can be actioned to view a camera feed from a location or open a gate or pop-up a message upon clicking.



This plug-in control comes with two functions :

- **Add Button**
- **Add Button with Colors**

Add button, by default will have a grey background and black font color. If you wish to have a colored button that represents the state of a device, it can be achieved by customizing the background color, font color, type and size in the response plan. The button size can also be defined in the properties of the GUI object.

RSS Feed

The Control Center RSS Feed UI control provides the ability to display RSS content within the Control Center user interface. This can be used to display news headlines or important pieces of information to all users across the site. For instance, these feeds can allow the user to keep track of any future changes or maintenance work coming up.

The control provides the user with a static or scrolling news ticker which displays RSS headlines with the ability for the user to click on a headline to read more information.

The RSS feed control supports a limited sub-set of RSS tags from either a file source or online source.

Configuring the News Scroll on the Main Screen

The news feed can be set to display on the main screen so that the user will not miss any important news or update. The administrator can configure the news feed by:

- Configuring the GUI
- Setting the properties of the GUI
- Displaying the GUI

Configuring the News Scroll on the Main Screen








The news feed can be set to display on the main screen so that the user will not miss any important news or update. The administrator can configure the news feed by:

- Configuring the GUI
- Setting the properties of the GUI
- Displaying the GUI

Configuring the GUI

To configure the GUI for the news feed you need to:

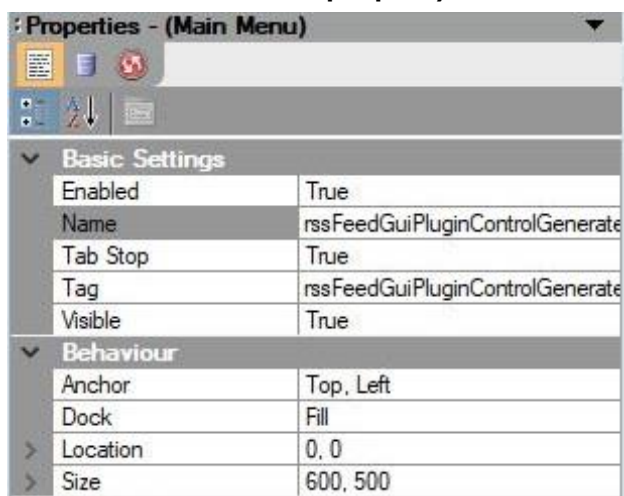
1. Go to **System Configuration > System Objects**.
2. Create a new GUI by right clicking on the window in the right pane. Name it appropriately, for example: News Scroll

⊕	 Administrator Interface	Create customised front-end's using Graphical User I...	Graphical User Interface	11/21/2018 3:39:57 PM
⊕	 Alarm Stack	System alarm stack GUI containing the alarm stack gri...	Graphical User Interface	11/21/2018 3:39:57 PM
⊕	 Auto	Create customised front-end's using Graphical User I...	Graphical User Interface	11/22/2018 2:31:50 PM
⊕	 Main Menu	Create customised front-end's using Graphical User I...	Graphical User Interface	11/21/2018 4:21:48 PM
⊕	 Map	System map GUI for showing maps to the end user.	Graphical User Interface	11/21/2018 4:21:59 PM
⊕	 News scroll	Create customised front-end's using Graphical User I...	Graphical User Interface	12/4/2018 3:07:53 PM
⊕	 System Explorer	Create customised front-end's using Graphical User I...	Graphical User Interface	11/21/2018 4:21:56 PM

3. Double click on the GUI to edit it.
4. Select **Plug-in Controls** tab, in the left pane of the toolbox.



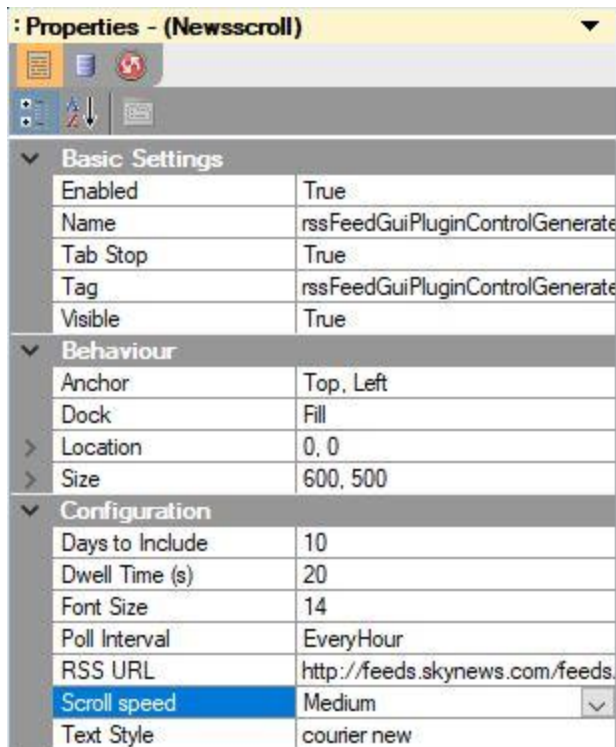
5. Drag and drop the **RSS Feed Control** onto the GUI.
6. Select the **Dock property** to fill on the properties window of the GUI.



7. Save GUI.

Setting the Properties of the GUI

The behavior of the news feed is controlled by setting the configuration properties of the GUI Control in the properties window.



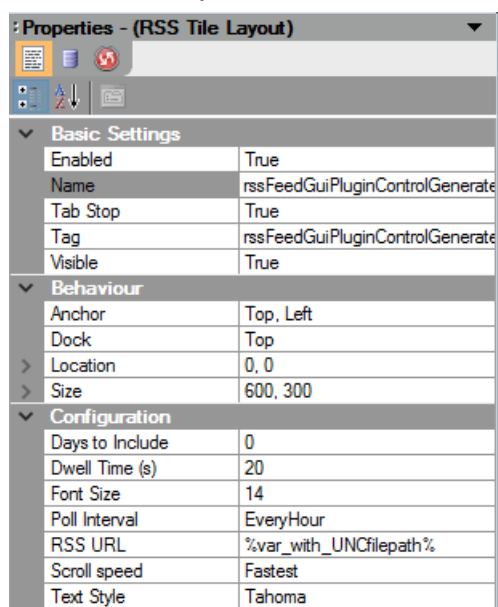
As seen in the figure above, there are six properties that manage the functioning of the news scroll. These will be explained in the table below.

Property	Description	Value
Days to Include	The maximum age of the RSS feeds in days to be shown on the display	0 - any value, depending on the source of the feed chosen
Dwell Time(s)	It is the time in seconds, a message is displayed for on the screen	Any value > 0. Dwell time applies to Fixed messages only
Font Size	Font size of the message appearing in the news feed	Greater than zero
Poll Interval	It is the time interval set to determine how often to reach to the source feed to refresh the messages	Several options available from the drop-down menu
RSS URL	URI or UNC path to an RSS source document.	File path (either local or UNC) or URI.

Scroll speed	The relative speed of the message to travel across the screen	There are five options that can be set from slowest to fastest. There is also a fixed option available, which when set, the message will not scroll.
Text Style	Font type of the message on the news feed	Any standard font type

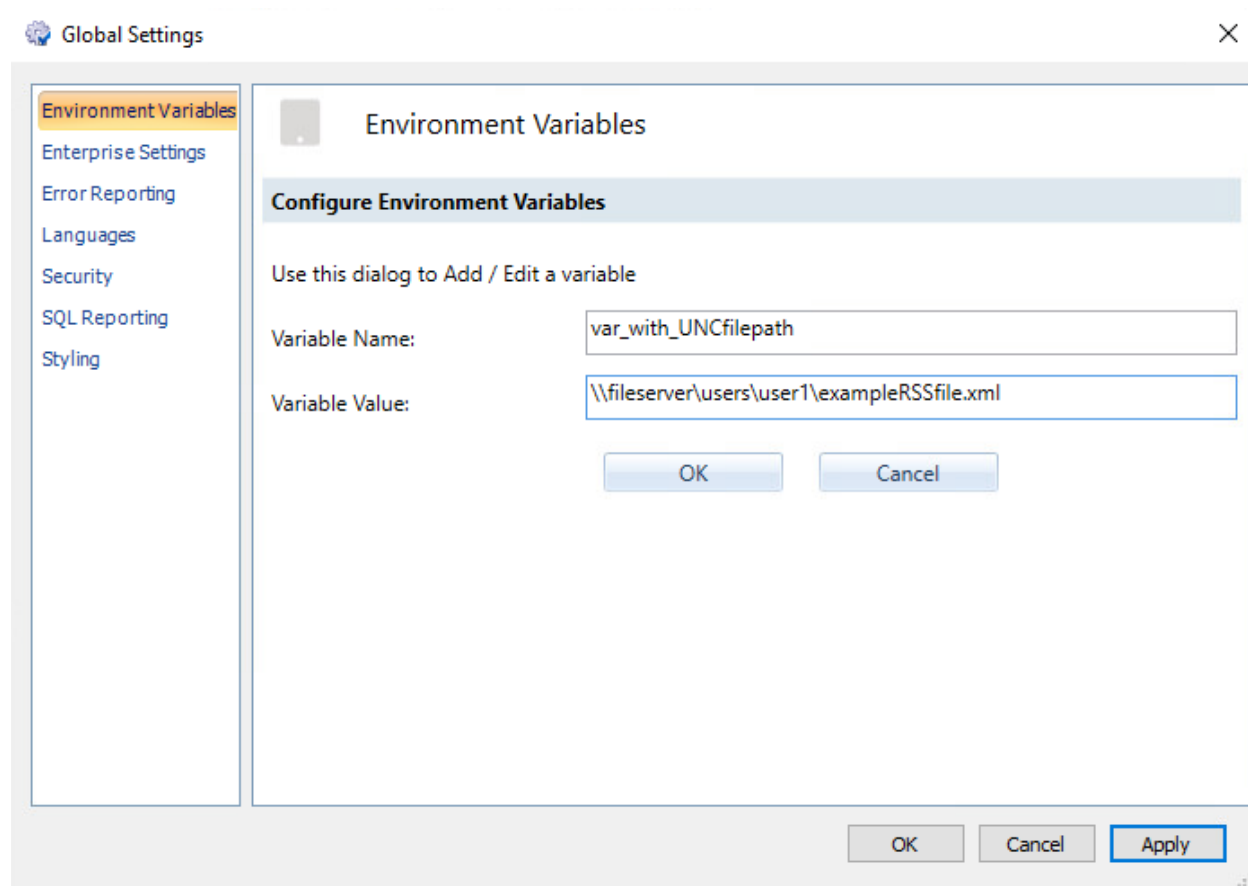
Using a File Path for the RSS Feed

The RSS feed can be sourced from an online source, from a file stored locally or on a shared Network drive (defined using UNC). The file path can be specified in the RSS URL property in the Property grid or can be saved as an Environment Variable and used as shown in the picture below.



Environmental variables can also be used to define the filepath. Standard Windows environment variables can be used or can be custom defined in the Global Settings to be used within Control Center. To define the environment variables, do the following:

1. Go to **System Configuration**.
2. Click on the **Global Settings** tab on the main toolbar ribbon at the top to see the **Global Settings** Window.
3. Select **Environmental Variables** from the options in the left pane.
4. Right Click on the empty space in the window to display the menu.



5. Select **New Variable** to create a new environment variable.
6. Enter a name and valid file path as a value and click on apply to save it.

Now, this variable can be used as explained in the previous section to set the path of the RSS feed.

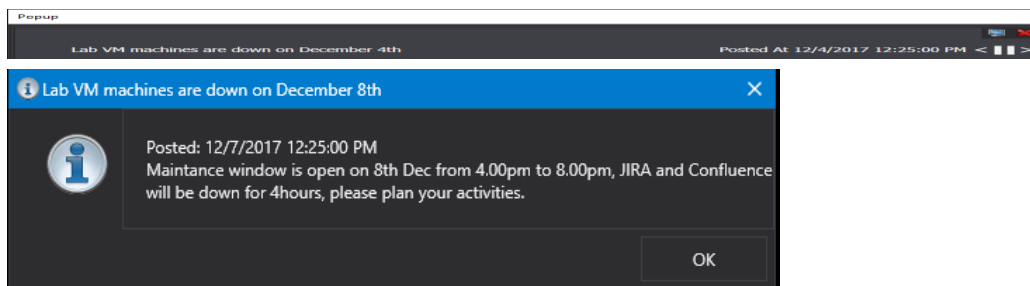
RSS Source Content

The first version of the RSS control supports a subset of RSS elements and does not render HTML formatting. Non-supported elements are ignored.

Supported elements:

Element	Description
<channel><lastBuildDate>	The last time the RSS source was refreshed. Used for refresh but not displayed.
<item>	Item displayed by the RSS feed

<item><title>	The title of the item shown in the feed
<item><description>	The description of the item shown when a user clicks on a title
<item><pubDate>	The time of an item shown in the UI



Sample contents of the RSS file is as shown below:

```
<?xml version="1.0" encoding="utf-8"?>
<rss version="2.0"
  xmlns:content="https://purl.org/rss/1.0/modules/content/">
<channel>
  <title>Not Used</title>
  <description>Not Used</description>
  <link>Not Used</link>
  <pubDate>Not Used</pubDate>
  <lastBuildDate>Mon, 26 Nov 2018 09:03:27 +0000</lastBuildDate>
  <managingEditor>Not Used</managingEditor>
  <docs>Not Used</docs>
  <generator>Not Used</generator>
  <item>
    <title>
      <![CDATA[Lab VM machines are down on December 4th]]>
    </title>
    <link>Not Used</link>
    <description>
      <![CDATA[Maintenance window is open on 22nd Dec from 4.00pm to 8.00pm,
      JIRA and Confluence will be down for 4hours, please plan your activities. ]]>
    </description>
    <pubDate>Mon, 4 Dec 2017 12:25:00 +0000</pubDate>
    <image>Not Used</image>
  </item>
  <item>
    <title>
```



```

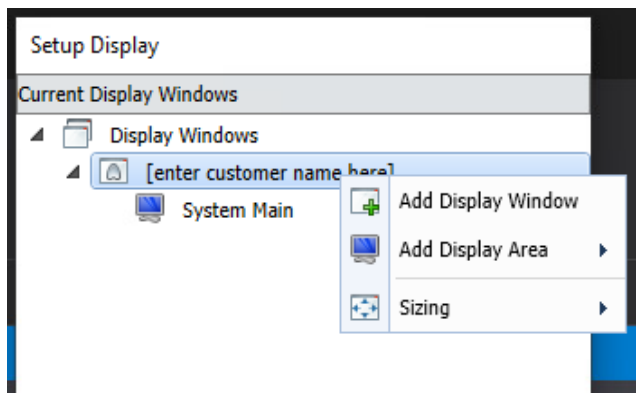
    <![CDATA[Lab VM machines are down on December 8th]]>
  </title>
  <link>http://www.codeguru.com/csharp/.net/net_general/keyboard/creating-
  an-ascii-table-in-.net.html</link>
  <description>
    <![CDATA[Maintenance window is open on 8th Dec from 4.00pm to 8.00pm,
  JIRA and Confluence will be down for 4hours, please plan your activities. ]]>
  </description>
  <pubDate>Mon, 7 Dec 2017 12:25:00 +0000</pubDate>
  <image>Not Used</image>
</item>
</channel>
</rss>undefined</xml>

```

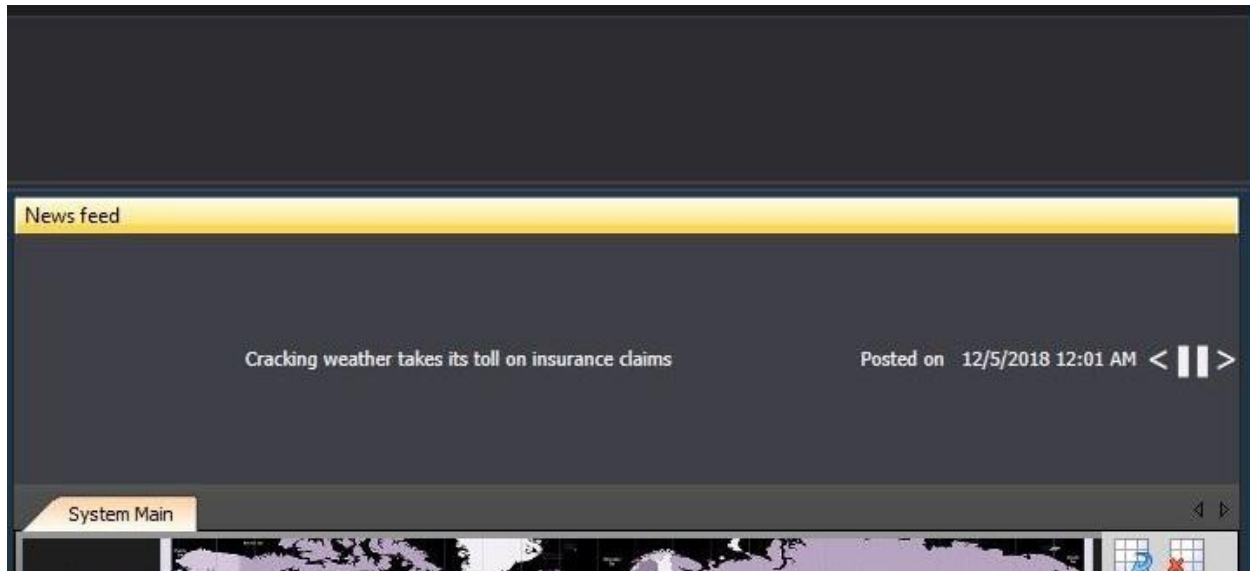
Displaying the GUI

You can display your GUI on the main screen of your Control Center as explained in the steps below:

1. Click on the **System > Setup Display**.
2. Add a new Display Window.
3. Add a new Display Area and name it News Feed.

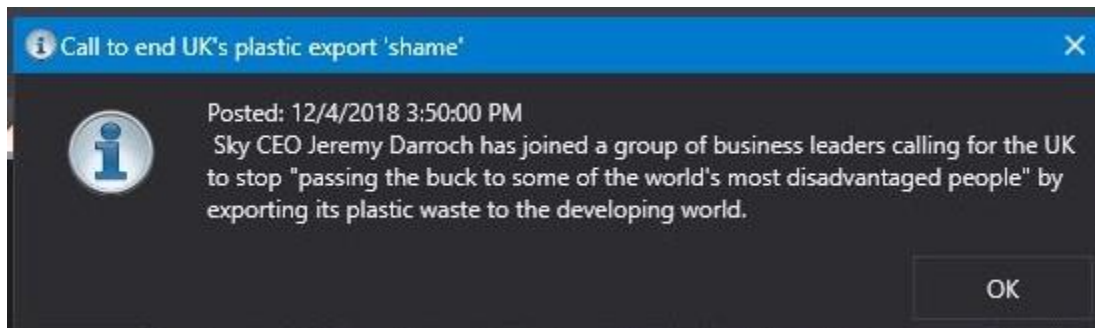


4. In the properties window of the display area, **Set Allow Drop to True**.
5. Save the display.
6. Drag and drop the **News Scroll** GUI onto the Display Area created above and pin it on the top of the Main screen of Control Center. The main screen will look like as seen below.



Viewing Details About a News Feed

The scroll bar of the News Feed window flashes the headlines or snippets of news from the source chosen. If you need to see more details regarding a news, you can click on the flashing news. A popup window appears with the headlines as the title and details about the news with time and date stamp at which the news was published.



You can also choose to see previous/succeeding news by clicking on the arrows in the top right corner of the window.

Unable to Get RSS Feed

The RSS feed can be fetched from a file path or an URI. In circumstances where the file path or URI is invalid, or the source is unreachable due to network issues or file not existing, the news scroll window displays the following error message.

The RSS Feed failed to load, please check that the RSS URL is correct.

Dashboards

Control Center Dashboards allow you to take your data and use it to create rich, interactive dashboards, that can be shared with other users in Control Center. This allows you to identify trends, patterns and relationships in your data like the events that are impacting your organization that may require deeper analysis. Key performance indicators can be displayed, allowing you to view information about each alarm, event or alert, for example.

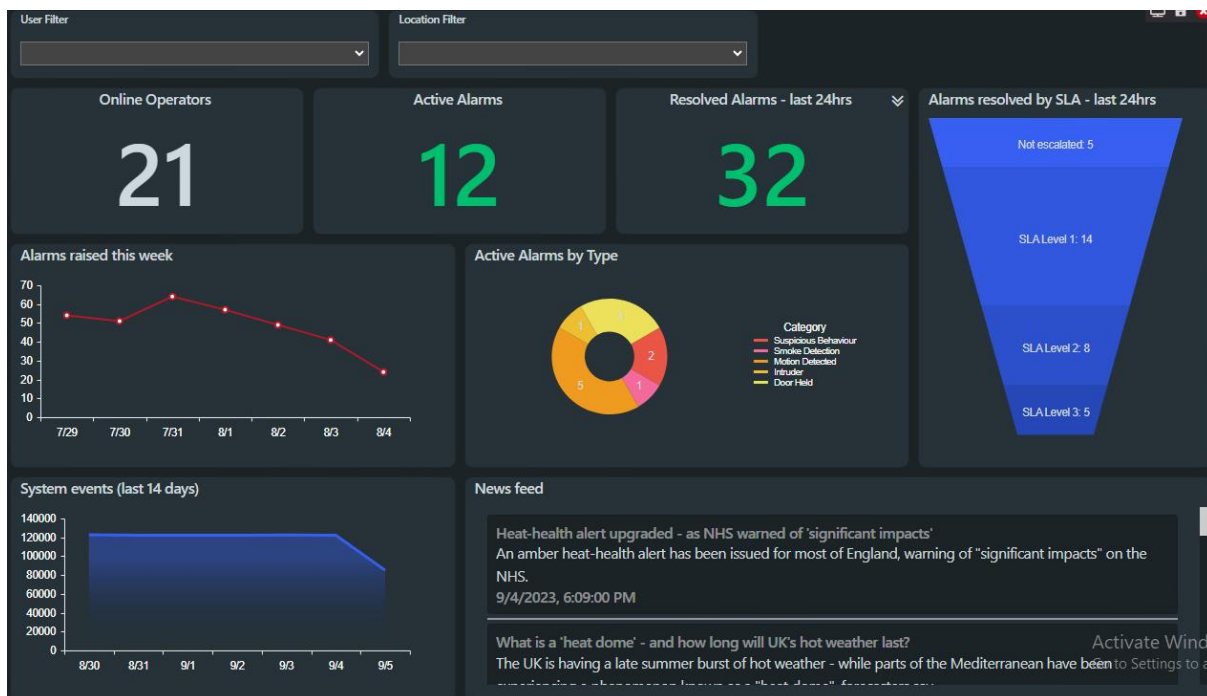
Control Center dashboards use widgets. Widgets are essentially types of reports, for example, charts, lists, grids, and so on. You can add any combination of widgets that you want.

Dashboards can be configured in a tile layout to be displayed in a display area or window, or displayed within a GUI using the Dashboard GUI control. See [Displaying Dashboards](#). You can configure which users have access to individual dashboards.

Using Control Center dashboards, you can:

- Use the out of the box System dashboard that Control Center provides.
- Create your own dashboards
- Add and configure dashboard widgets
- Configure your clients to display your dashboards. For example, you may want a dashboard to display on all clients or specific clients.

For example, you may want a dashboard that shows key metrics from across your sites.



Configuring Access to Dashboards

You can configure who can create dashboards using the **Dashboard** type permission. See [Type Permissions](#).

You can configure which users have access to individual dashboards using object permissions. See [Object Type Permissions](#).

Configuring Dashboards

Control Center dashboards use widgets. Widgets are essentially types of reports, for example, charts, lists, grids, and so on. You can add any combination of widgets that you want. Each widget must have a data source which defines where the data you want to display in the widget comes from.

When configuring a dashboard, you need to think about the type of data you want to display as this will help you to select the right type of widget for your data. For example, you may want a dashboard that has:

- A donut widget displaying devices by state.
- A list widget that is displaying information from an RSS feed.
- A chart widget displaying all your alarms by type.
- A grid widget displaying all your top 10 alarms by site.

Configuring Colors in Dashboards

By default, a color palette is available for dashboards. This means that when you configure your widgets, they automatically display in the colors that are available.

If you want to use custom colors, you can do this by adding colors as part of your SELECT statement when creating a SQL Query data source. You can:

- add the colors directly in the SELECT statement, for example, When I.Label='Sub location 1' then '#FF8B44'
- configure a color property for your Control Center object so that when the object is included in a SELECT statement, the color that you have configured for that object displays in the widget. See [Object Designer](#).

Colors can be:

- Web color format, for example, **white**.
- RGB, for example, **#FF8B44**.
- RGBA, for example, **#FF8B44FF**.

Adding Dashboards

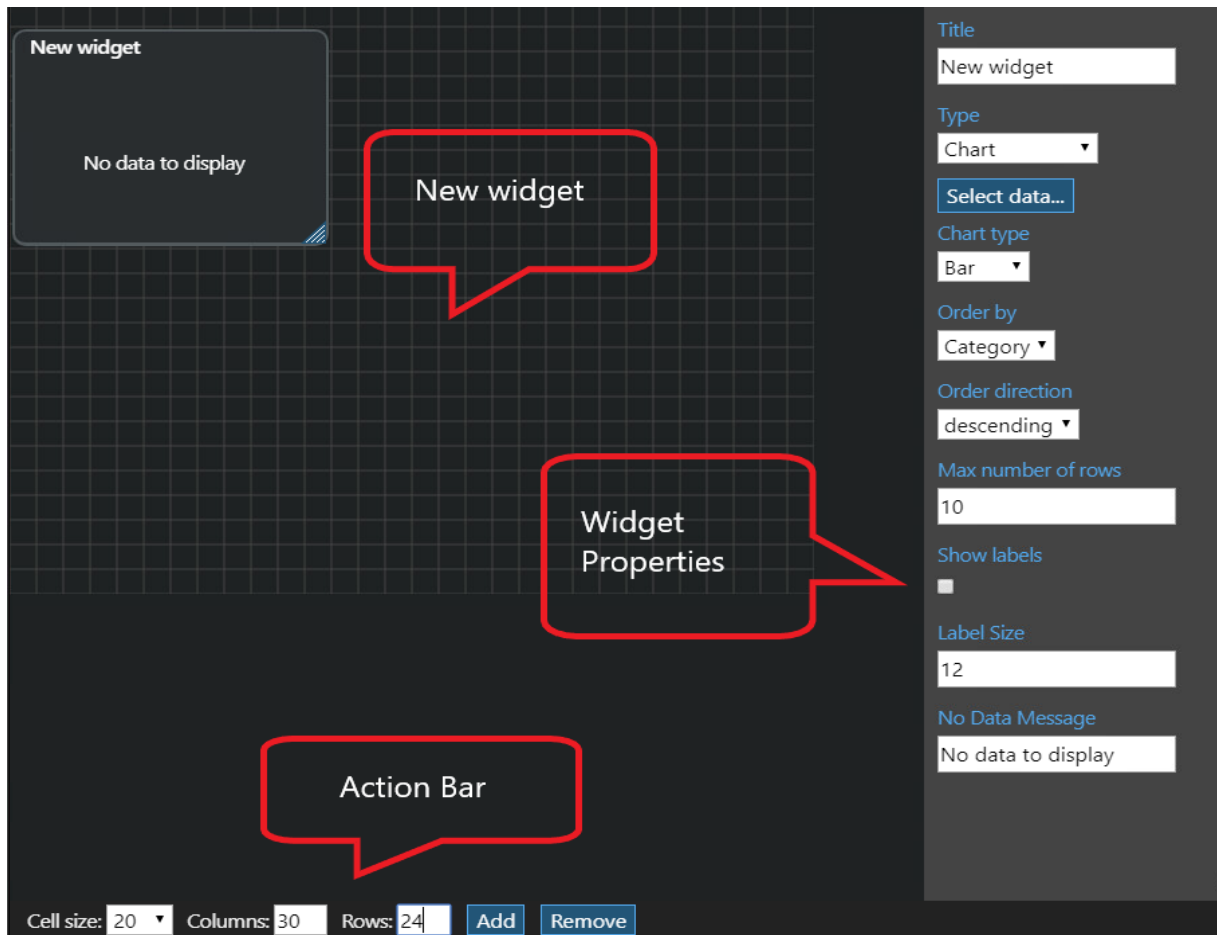
You can create as many dashboards as you like in Control Center. To do this:

- Create a new dashboard in **System Configuration**.

- Add your widgets to your dashboard.
- Configure your widgets.
 - Select your widget type. When thinking about the widget type you want to use, think about the type of data you want to display.
 - Configure the widget's data source.
 - Configure any properties specific to the widget type.
- Configure how you want your dashboards to display.

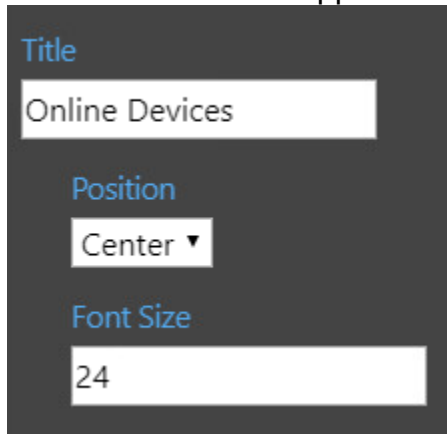
To create a new dashboard:

1. From **System Configuration**, select or create a folder where you want to add your dashboard.
2. Right-click and select **New > Dashboard**. A **Dashboard** object appears in the folder.
3. Rename your dashboard.
4. Double-click the newly created dashboard. The dashboard opens in Dashboard Designer.
5. You can use the dashboard configuration options, to increase or decrease cell size, and the number of columns or rows in the Dashboard Designer.
6. From the bottom of the page, select **Add**. The options to configure the widget appear:



- Everbridge recommends that you configure your design grid to match, as much as possible, the display area or window where you are going to display the dashboard. This makes it easier when sizing and positioning your widgets within in the dashboard.
- Specify the **Title** for the widget, for example, Online Devices. The new title appears on the dashboard. You can adjust the font size and alignment of the title

to further control its appearance.



The image shows a configuration panel for a widget. It has a dark background with white text and input fields. The options are:

- Title:** A text input field containing "Online Devices".
- Position:** A dropdown menu currently set to "Center".
- Font Size:** A text input field containing "24".

9. From the **Type** drop-down list, select one of the following:

Type	Description
Chart	Displays chart types on the dashboard, for example, bar, pie or donut charts. For example, if you are using an Object States or Alarms data source, where you want to show categories of alarms by type, or devices by state, a chart widget is the best way to display this. See Configuring Chart Widgets .
Filter	Displays a dropdown box on the dashboard that can be used to filter the data presented in other widgets. See Configuring Filter Widgets
Gauge	Displays a gauge visualization on the dashboard. See Configuring Gauge Widgets
Grid	Displays the selected data in a tabular format. A Grid widget is highly configurable, allowing you greater control over how and what data is displayed. See Configuring Grid Widgets .

List	Displays the selected data in a list. This widget type is best when using an RSS Feed or similarly serial data source. See Configuring List Widgets .
Machine Data	Displays machine data, for example, memory and disk consumption. See Configuring Machine Data Widgets .
Number	Displays a value based on the configured data source. For example, you may want to know the total number of devices whose state is Offline . See Configuring Number Widgets .
Scatter Chart	Displays data on two independent axes. See Configuring Scatter Chart Widgets .
Heatmap	Displays data as a heatmap. See Configuring Heatmap Widgets .
Threat Level	This is a variant of the Gauge widget better suited to displaying the system threat level. See Configuring Threat Level Widgets .

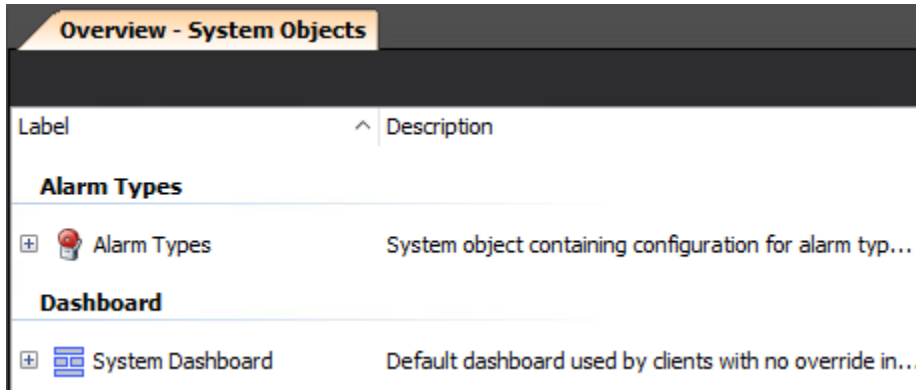
Using System Dashboard

Out of the box, Control Center provides a dashboard that provides performance information. The **System** dashboard displays the following widgets:

- Core Server statistics, for example, memory being used, disk reads and disk writes.
- Device States by Device Type
- Device States
- Alarms by Alarm Type
- Alarms by state

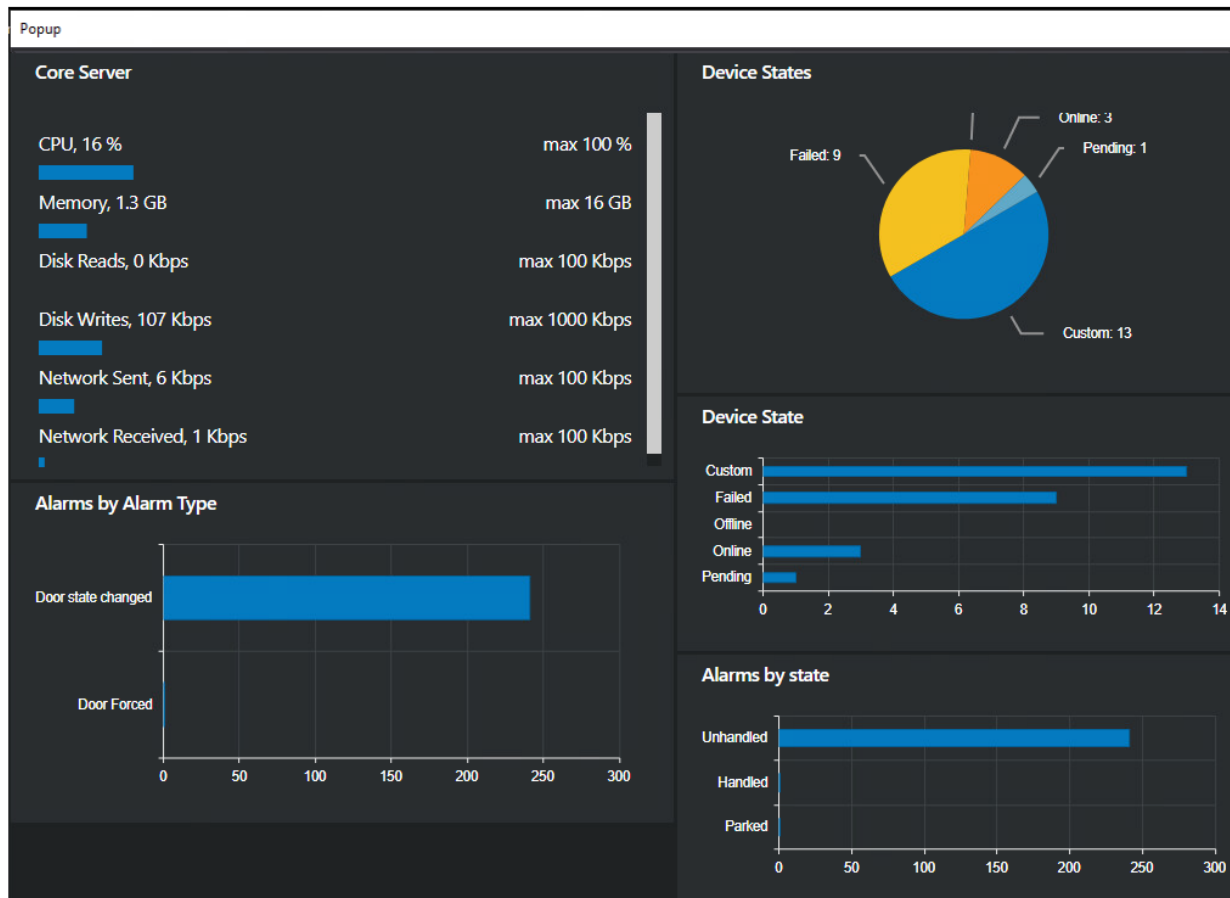
You can modify the widgets or add new widgets to this dashboard.

1. From **System Configuration**, navigate to the **System Objects** folder.
2. From **Dashboard**, double-click **System Dashboard** to open it in the Dashboard Designer.



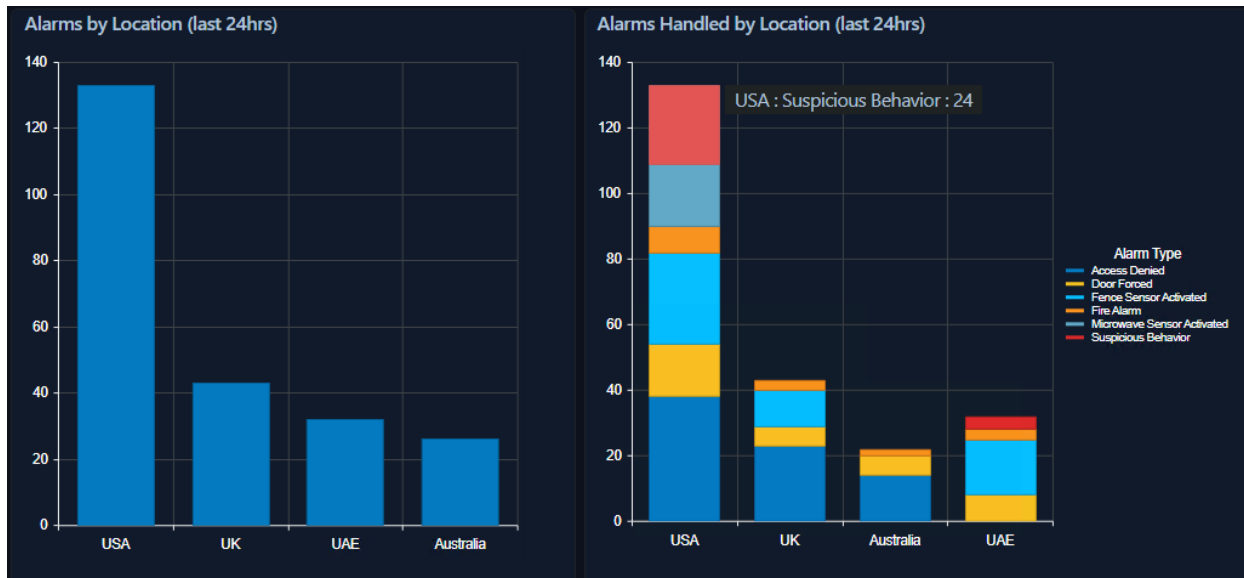
Label	Description
Alarm Types	
Alarm Types	System object containing configuration for alarm typ...
Dashboard	
System Dashboard	Default dashboard used by clients with no override in...

3. To display the System Dashboard in a display window or area, see [Displaying Dashboards](#).



Configuring Chart Widgets

Using chart widgets you can display your data as a number of different chart visualisations depending on your requirements. Chart widgets are useful for displaying data when you want to compare, for example, the frequency or number for different types of alarm or object state. Charts can support multiple series per category allowing for even more detailed comparisons.



A chart widget is more commonly used with SQL Query, Alarms or Object States data sources.

Once you select **Chart** from the **Type** drop-down list, the properties that you can configure for a chart widget display.

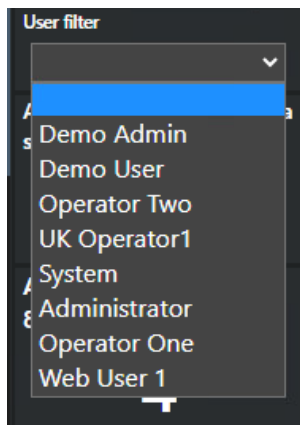
- From **Chart Type**, select one of the following from the drop-down list:
 - Area** – display data in an area chart.
 - Bar** - display data in a bar chart.
 - Column** – display data in a column chart.
 - Pie** - display data in a pie chart.
 - Donut** - display data in a donut.
 - Funnel** – display data in a funnel chart.
 - Line** – display data in a line chart
 - Pie** - display data in a pie chart.
 - Radar Line** – displays data in a radar chart with line joining each point
 - Radar Column** – displays data in a radar chart using solid columns
- Click **Select data...**
- Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).
- You can configure some or all of the following properties, depending on your requirements.

Property	Description
Stacked	If the data source contains multiple series, this checkbox controls whether series are stacked or shown individually.
Order by	select one of the following from the drop-down list: <ul style="list-style-type: none"> ○ Category - if you want your chart to display by category. For example, if you selected an object states data source, you may want your chart to display by object type, like Door, Camera and so on. ○ Value - If you want your chart to display by value. For example, if you selected an object states data source, you may want your chart to be organized by state, like Offline, Pending and so on. ○ Order - If you want your chart to display based on the data source column mapped to the Order property. This can be useful if your categories make more sense when displayed in a specific order, like day or month names.
Order Direction	select whether you want the data to be displayed in Ascending or Descending order.
Max number of rows	Type the maximum number of rows you want displayed in the widget. By default, this is set to 10.
Palette	Select from a number of color palettes to be applied to chart series.
Category Size	Type the font size that you want the category labels to be.
Show labels	Select this if you want the data labels to be displayed in the widget.
Show legends	Select this if you want to display a series legend. Valid for Donut, Funnel, and Pie chart types. If labels and legends are enabled, the label format is changed to display only the value.

Legend Heading	If legends are enabled, the text entered here will be displayed above the legend to explain the category.
Label Size	Type the font size that you want the labels to be.
Show gridlines	Uncheck this if you want to hide gridlines from Area, Bar, Column, or Line charts.
No Data Message	Type the message that you want to display in your widget if no data is available to display. By default, this is No data to display. Note: No data to display means the absence of data. Some properties may have a value of 0, so the 0 value displays.
Enable Drilldown	Select this if you want to enable drilldown functionality from this chart. See Configuring drilldown views for more information.

Configuring Filter Widgets

Filter widgets, when used with [Data Transformation](#), can be used to control the data presented in other widgets on the dashboard.



Currently, the filter widget is only useable when the dashboard is displayed in a Docked display area.

Once you selected **Filter** from the **Type** drop-down list, the properties that you can configure for a filter widget are displayed. You can configure the following options:

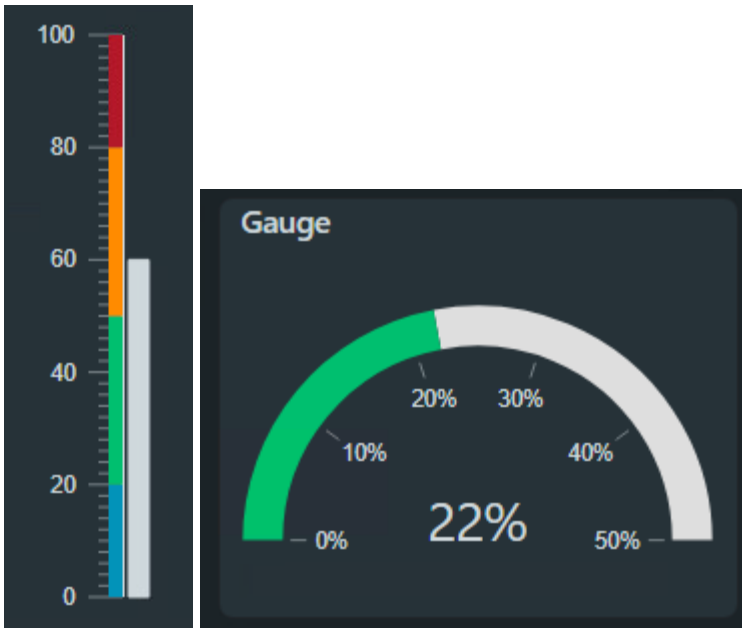
1. Click **Select data..**
2. Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).
3. The Filter widget maps the data source to two columns, **ID** and **Label**. The data in the **Label** column will be shown in the dropdown on the dashboard while the data in the **ID** column will be used as the value of the filter. This means that you can show a friendly name to users but utilize a GUID or other identifier in your data transformations.
4. You can configure some or all of the following properties, depending on your requirements.

Option	Description
Filter Variable	This is the name of the variable that will be controlled by the filter widget. This can be referenced in the Data Transformation step of other widgets to make them respond to changes in the filter widget. See Data Transformation for further information on using Filter Variables.
Filter Color	This field takes either a hex color code (including hash) or an HTML color name. When configured, the filter and any widgets on the dashboard that include the filter variable will show a border of the color entered here when the filter is in use.
No Data Message	Type the message that you want to display in your widget if no data is available to display. By default, this is No data to display. Note: No data to display means the absence of data. Some properties may have a value of 0, so the 0 value displays.

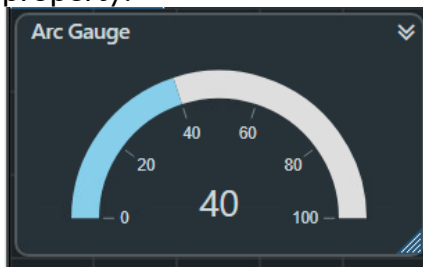
Configuring Gauge Widgets

Gauge widgets combine visual elements of the Chart and Number widget to quickly convey information to users.

Gauge widgets are most commonly used with a SQL query data source but can work with any data sources providing a numeric value.



By default the gauge uses a scale of 0-100 and is displayed as a 180 degree arc. The gauge color is based on the current value compared to the maximum scale value, with color changes at 20%, 50% and 80%. Custom colors can be used by selecting a data source with a column containing a color value and linking it to the 'Color' data source property.



Once you select **Gauge** from the **Type** drop-down list, the properties that you can configure for a Gauge widget are shown.

1. Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).

2. You can configure some or all of the following properties, depending on your requirements and the type of gauge visualization selected.

Option	Description
Gauge type	Allows the user to select between Linear and Arc gauge types.
Min	A numeric value that will be used as the start of the scale.
Max	A numeric value that will be used as the end of the scale.
Start angle	Valid for Arc gauge only. A numeric value that defines where the gauge will start.
End angle	Valid for Arc gauge only. A numeric value that defines where the gauge will finish.
Labels enabled	Select this if you want the labels to be displayed below the gauge.
Show Ranges	Valid for Linear gauge only. If deselected, no range indicators will be displayed and the pointer color will take the range color instead.
Orientation	Valid for Linear gauge only. Allows the user to select between horizontal and vertical orientation.
Pointer	Allows the user to select between a bar and arrow pointer type.
Center Template enabled	Valid for Arc gauge only. Select this if you want the current value to be displayed below the gauge.
Center Template	Valid for Arc gauge only. Text entered here will be added as a suffix to the current value displayed in the center of the widget.
Enable Drilldown	Select this if you want to enable drilldown functionality from this gauge. See Configuring drilldown views for more information.

Configuring Grid Widgets

Using grid widgets you can display your data in a grid. This is useful, for example, if you want to list top 10 alarms by location and you want to include the ID, status and alarm type description in the grid.

Top 10 Alarms

ID	Status	Alarm Type	Description	Location	Date/Time
279		Door state changed alarm		Site A	Dec 1 2020 10:45AM
278		Door state changed alarm		Site A	Dec 1 2020 10:45AM
277		Door state changed alarm		Site A	Dec 1 2020 10:45AM
276		Door state changed alarm		Building 11	Dec 1 2020 10:45AM
275		Door state changed alarm		Building 11	Dec 1 2020 10:45AM
274		Door state changed alarm		Building 11	Dec 1 2020 10:45AM
273		Door state changed alarm		Site A	Dec 1 2020 10:45AM

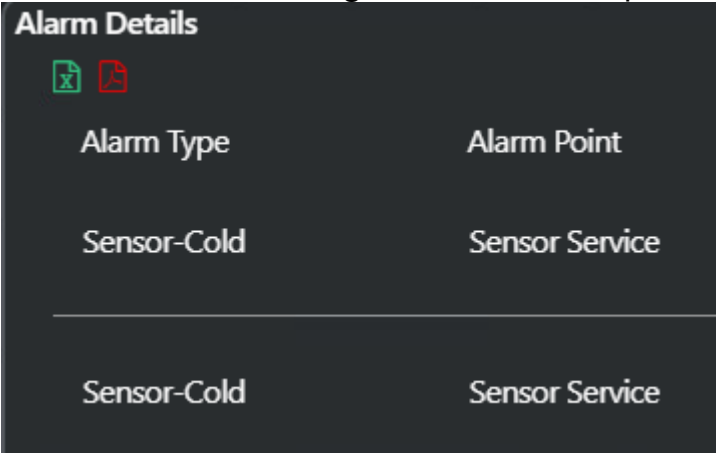
Grid widgets are more commonly used with SQL query and RSS feed data sources.



Grid widgets are highly configurable giving you greater control on how the information is displayed in your grid.

Once you selected **Grid** from the **Type** drop-down list, the properties that you can configure for a grid widget are displayed. You can configure the following options:

5. Click **Select data..**
6. Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).
7. You can configure some or all of the following properties, depending on your requirements.

Option	Description
Number of columns	The number of columns you want to display in your grid.

Headings On	Select if you want each column in your grid to have a heading.
Font Size	Type the font size that you want the heading to be.
Separator On	Select if you want a separator between entries in your grid.
Row Font Size	Type the font size that you want the row text to be. Text will scale to the size of the display area the dashboard is displayed in.
Enable Export to Excel/PDF	<p>Select if you want to enable users to export grid data to Excel or PDF. When enabled an icon will be displayed at the top of the widget that allows users to save the grid data in .xlsx or .pdf format.</p>  <p>The screenshot shows a dark-themed widget titled "Alarm Details". At the top left, there are two icons: a green Excel icon and a red PDF icon. Below the icons, there are two columns of data. The first column is labeled "Alarm Type" and contains the text "Sensor-Cold". The second column is labeled "Alarm Point" and contains the text "Sensor Service". A horizontal separator line is visible below the first row of data, and a second row of data is shown below the line, with "Sensor-Cold" in the first column and "Sensor Service" in the second column.</p>
No Data Message	<p>Configure the message you want to display when there is no data to display in a widget. By default, this is</p> <p>No data to display</p>
Column <i>n</i>	If you specify 5 columns, you can specify a column heading, the text, icon (depending on how you have configured your SQL query) to display in each column in the grid.
Columns Heading	Select the column heading from the available fields in the drop-down list.
Text	Select the text you want to display from the available fields in the drop-down list.
Icon	Select the icon that you want to display from the available fields in the drop-down list. Icons must use their Font Awesome CSS Identifier. For example, the cog icon is

	<p>fa-cog Font awesome names can be found at https://fontawesome.com/</p>
Background Color	<p>If a background color is available in your SQL query, select the background color. Colors can be:</p> <ul style="list-style-type: none"> • Web color format, for example, white. • RGB, for example, #FF8B44. • RGBA, for example, #FF8B44FF.
Is Pill	<p>Select this checkbox if you want your icon to display as a pill shape. For example:</p> <ul style="list-style-type: none"> • Is Pill is not selected  • Is Pill is selected 

An example of how column 2 is configured for the above grid is shown below

Column 2

Columns Heading

Status

Text

Icon

Icon

Background Colour

Background

Is Pill

Configuring List Widgets

Using list widgets you can display your data in a list. This is useful, for example, if you want to list posts from an RSS feed.

Top Stories

Critical Event Management Category Leader Everbridge Makes Key Appointments to Expand its Global Marketing and Communications Functions 11/24/2020, 2:00:00 PM

Veteran marketing executive and MIT Sloan School of Management graduate Stacey Wu , former head of global marketing at security software leader Fortinet where she helped grow the company's market cap from \$5B to over \$20B , joins Everbridge as Chief Marketing Officer Three-time CMO and Harvard

Everbridge Recognized in the Gartner 2020 Market Guide for Crisis/Emergency Management and COVID-19 Safe Return to Work Solutions 11/24/2020, 1:30:00 PM

Report calls for leaders responsible for crisis management to “deploy solutions to facilitate command and control before and during a crisis,” including having a management plan to mitigate the coronavirus pandemic BURLINGTON, Mass. --(BUSINESS WIRE)--Nov. 24, 2020-- Everbridge , Inc.

Everbridge Named Top Three Highest-Rated Public Cloud Company to Work For During COVID-19 11/23/2020, 1:30:00 PM

Global investment firm Battery Ventures recognized Critical Event Management (CEM) leader Everbridge as top place to work amid the coronavirus pandemic, as measured by employee satisfaction provided by Glassdoor BURLINGTON, Mass. --(BUSINESS WIRE)--Nov. 23, 2020-- Everbridge , Inc.

Everbridge Wins Top Tech Company Awards in the Categories of COVID-19 Response and Business Accomplishment for 2020 11/16/2020, 1:30:00 PM

The Massachusetts Technology Leadership Council recognizes Everbridge for both its significant impact on helping organizations respond to the coronavirus pandemic and for its business accomplishments over the prior year BURLINGTON, Mass. --(BUSINESS WIRE)--Nov. 16, 2020-- Everbridge , Inc.

Once you select **List** from the **Type** drop-down list, the properties that you can configure for a list widget display. You can configure how you want the information to display in your widget.

1. Click **Select data..**

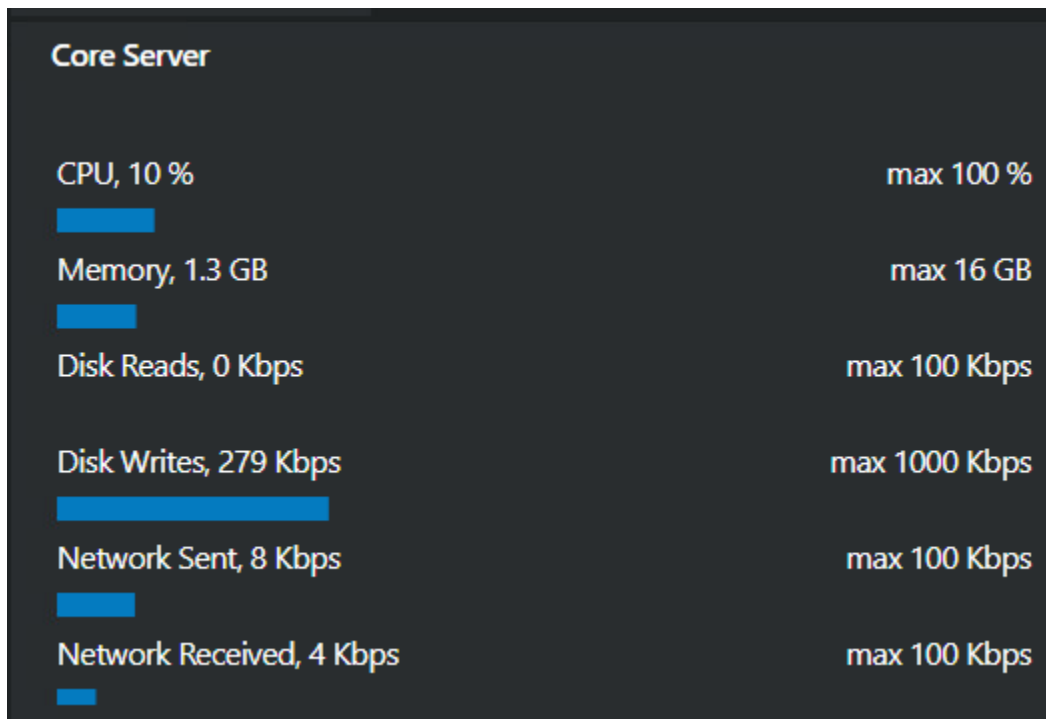
2. Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).
3. You can configure some or all of the following properties, depending on your requirements.

Option	Description
Title Field	Include a title name.
Title Icon	Include an icon for your widget title.
Subtitle Field	Include a sub title name.
Font Size	Type the font size that you want the subtitles to be.
Subtitle Icon Field	Include an icon for your sub-title.
Footer Field	Include a footer.
Font Size	Type the font size that you want the footers to be.
Footer Icon Field	Include a footer icon.
Badge Field	Include a badge.
Badge Icon Field	Include a badge icon.
Badge Color Field	Include a badge color field.
Background Color Field	Include a background color
Render HTML	Select to True to render any HTML tags. This only renders text markup tags and strips out any other tags.
Separator	Select True

	to display a separator.
No Data Message	<p>Type the message that you want to display in your widget if no data is available to display. By default, this is</p> <p>No data to display</p> <p>.</p> <p>Note</p> <p>:</p> <p>No data to display</p> <p>means the absence of data. Some properties may have a value of 0, so the 0 value displays.</p>

Configuring Machine Data Widgets

Using machine data widgets you can display performance statistics about your machine.




Machine data widgets use the machine data source.

Once you select **Machine data** from the **Type** drop-down list, the properties that you can configure for a machine data widget display.

1. Click **Select data...**
2. Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).

3. You can configure some or all of the following properties, depending on your requirements.

Property	Description
No Data Message	Type the message that you want to display in your widget if no data is available to display. By default, this is No data to display . . Note : No data to display means the absence of data. Some properties may have a value of 0, so the 0 value displays.
CPU Warning (%)	Select the percentage of CPU usage that you want to be warned at. 
Memory Warning (%)	Select the percentage of memory usage that you want to be warned at.
Show disk data	Select if you want to display performance statistics about your disk.
Show network data	Select if you want to display performance statistics about your network.

Configuring Number Widgets

Using number widgets allows you to display key values from your data such as the total number of alarms you have in your system.

Although it is called the Number widget it will happily display text values.

Number widgets are most commonly used with a SQL query data source.

For example, the SELECT statement below:

```
SELECT Count(*) as AlarmCount
    , 'Blue'
FROM [pacific].[IPSC].[DeviceStatusCurrentView]
```

displays a number widget like the one shown below:



Once you select **Number** from the **Type** drop-down list, the properties that you can configure for a Number widget are shown. You can configure how you want the information to display in your widget.

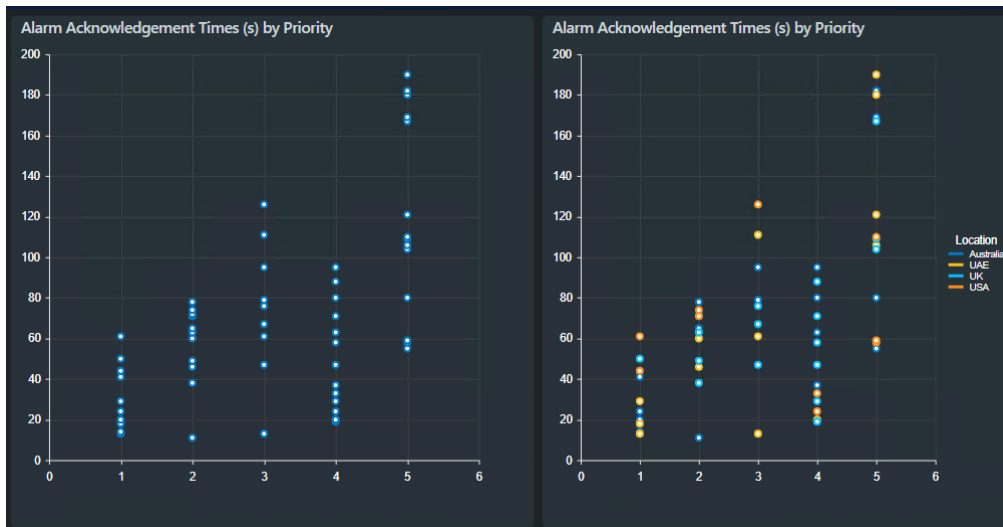
3. Click **Select data...**
4. Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).
5. You can configure some or all of the following properties, depending on your requirements.

Option	Description
Value	Select a value from the drop-down list. The values available depend on how you have configured your SELECT statement.
Label	Type the text that you want to use as a label.
Font Size	Type the font size that you want the label to be. This value will be scaled to fit the display area that the dashboard is visible on.
Text Color Field	Select the color that you want from the dropdown list.
No Data Message	Type the message that you want to display in your widget if no data is available to display. By default, this is

	<p>No data to display.</p> <p>Note: No data to display means the absence of data. Some properties may have a value of 0, so the 0 value displays.</p>
<p>Enable Drilldown</p>	<p>Select this if you want to enable drilldown functionality from this widget.</p> <p>See Configuring drilldown views for more information.</p>

Configuring Scatter Chart Widgets

Using Scatter Chart widgets you can plot data points on two independent axes in order to observe relationships between numeric variables. Scatter Charts can support multiple series per category allowing for even more detailed comparisons.



Once you select **Scatter Chart** from the **Type** drop-down list, the properties that you can configure are

- From **Chart Type**, select one of the following from the drop-down list:
 - Scatter Plot** – display data as an X/Y scatter plot.
 - Scatter Line** - display data as an X/Y plot with lines joining each point.
- Click **Select data...**
- Select an existing data source or create a new data source. Scatter chart data sources need at least two numeric columns for X and Y values. See [Creating Dashboard Data Sources](#).

4. You can configure some or all of the following properties, depending on your requirements.

Property	Description
Max number of rows	Type the maximum number of rows you want displayed in the widget. By default, this is set to 10.
Palette	Select from a number of color palettes to be applied to chart series.
Show legends	Select this if you want to display a series legend. Valid for Donut, Funnel, and Pie chart types. If labels and legends are enabled, the label format is changed to display only the value.
Legend Heading	If legends are enabled, the text entered here will be displayed above the legend to explain the category.
Show gridlines	Uncheck this if you want to hide gridlines from the scatter chart.
No Data Message	Type the message that you want to display in your widget if no data is available to display. By default, this is No data to display. Note: No data to display means the absence of data. Some properties may have a value of 0, so the 0 value displays.
Enable Drilldown	Select this if you want to enable drilldown functionality from this chart. See Configuring drilldown views for more information.

Configuring Threat Level Widgets

The Threat Level widget is a version of the Gauge widget better suited to displaying the system Threat Level with a variety of visualization options and customizable levels.



Once you select **Threat Level** from the **Type** drop-down list, the properties that you can configure are shown.

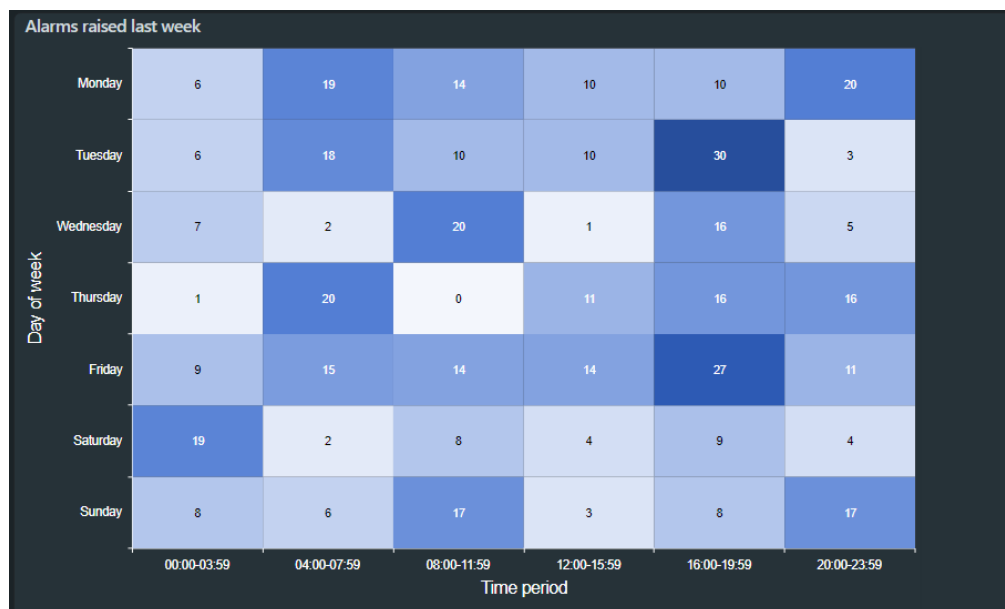
1. Select an existing data source or create a new data source. See [Creating Dashboard Data Sources](#).
2. You can configure some or all of the following properties, depending on your requirements and the type of gauge visualization selected.

Option	Description
Gauge type	Allows the user to select between Linear, Arc, and Radial gauge types.
Start angle	Valid for Arc and Radial gauges only. A numeric value that defines where the gauge will start.
End angle	Valid for Arc and Radial gauges only. A numeric value that defines where the gauge will finish.
Labels enabled	Select this if you want the labels to be displayed below the gauge.

Show Ranges	Valid for Linear gauge only. If deselected, no range indicators will be displayed and the pointer color will take the range color instead.
Orientation	Valid for Linear gauge only. Allows the user to select between horizontal and vertical orientation.
Pointer	Valid for Linear gauge only. Allows the user to select between a bar and arrow pointer type.
No. of Levels	Allows the user to select the number of threat levels in use from 2-5.
Level [#] Label	Determines the label text for this threat level on the widget.
Level [#] Color	Determines the color used for this threat level on the widget. Accepts a hex code or html color name.
Enable Drilldown	Select this if you want to enable drilldown functionality from this gauge. See Configuring drilldown views for more information.

Configuring Heatmap Widgets

The Heatmap widget plots values against two axes and provides an intuitive way to visualize relationships and identify hotspots in complex datasets.



Once you select **Heatmap** from the **Type** drop-down list, the properties that you can configure are

1. Click **Select data...**
2. Select an existing data source or create a new data source. Heatmap data sources need at least three values to use for the X axis, Y axis, and value component. See [Creating Dashboard Data Sources](#).
3. You can configure some or all of the following properties, depending on your requirements.

Property	Description
Palette	Select from a number of color palettes to be applied to the heatmap.
X Axis Label	Enter text here to be shown beneath the X axis on the heatmap
Y Axis Label	Enter text here to be shown to the left of the X axis on the heatmap
Marker Type	Choose between Rectangle or Circle for the heatmap markers
Show gridlines	Uncheck this if you want to hide gridlines from the heatmap.
No Data Message	Type the message that you want to display in your widget if no data is available to display. By default, this is No data to display . Note: No data to display means the absence of data. Some properties may have a value of 0, so the 0 value displays.
Enable Drilldown	Select this if you want to enable drilldown functionality from this chart. See Configuring drilldown views for more information.

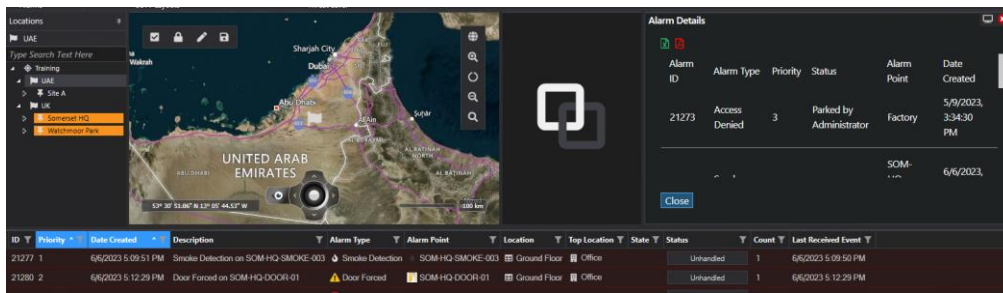
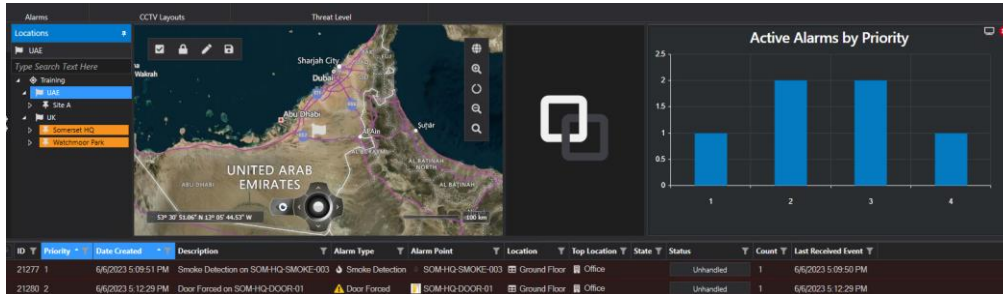
Configuring Drilldown views

Drilldown views can be added to display additional information when a widget is clicked. Currently chart, gauge and number widgets can be used with drilldown views.

Chart, Gauge, or Number widgets that have an associated drilldown view will show an icon to indicate this to users.



In this example when the 'Active Alarms by Priority' chart is clicked, a grid widget with active alarm details is displayed.

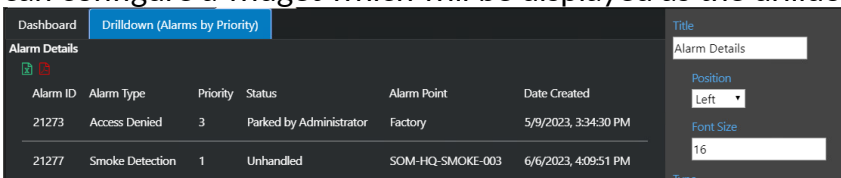


To configure a drilldown view:

1. Open the dashboard object that you want to add the drilldown view to.
2. Select the widget you want to add drilldown functionality to and press the **Add Drilldown** button in the bottom action bar.



3. A new tab will be added to the dashboard configuration screen. On this tab you can configure a widget which will be displayed as the drilldown view.



Any data source and widget type can be used for the drilldown view allowing for it to be used flexibly. Examples include:

- A detailed version of data summarized in a chart e.g., Active alarms by priority -> table of active alarm details
 - An alternative grouping of the same data e.g., Active alarms by priority -> active alarms by location
 - A view of the same data for a different time period e.g., Average time to resolve alarms this week -> Average time to resolve alarms last week
4. The **Drilldown Filter Parameter** dropdown allows you to choose a column from the data source used in the drilldown widget. When a user clicks on a specific category in the chart, the drilldown view will be filtered to display only the data where the chosen column matches the category value.

For example, you have a chart showing alarms categorized by priority linked to a drilldown widget showing alarm details. If the dropdown on the drilldown widget is set as the “Priority” column then when a user clicks on priority 1 from the chart the drilldown view will only show alarm details where the Priority is equal to 1. If there is no match then the entire drilldown data set is displayed. Users can click elsewhere within the chart area to display the unfiltered drilldown data set.

Creating Dashboard Data Sources

Once you have added a widget to a dashboard, see [Adding Dashboards](#), you need to select a data source for the widget. To do this, from the widget configuration tools, click **Select data...** and select **Create a new data source** from the **Configure a Data Source** dialog. Once a data source is created, it can be used again for other widgets.

Control Center dashboards provide the following data sources.

Source Type	Description
SQL Query	Enter a SQL query and connection string to query the data in any SQL database.
Native SQL Query	Enter a SQL query to query the data in the Control Center database.
Object States	View your object states in your widgets. You can view states by device type or for all devices.

Alarms	View your alarms in your widgets. You can view alarms by state, by priority or by alarm type.
Machine Data	View information about your machine, for example, memory and disk consumption.
RSS Feed	View information from an RSS Feed.

The information you need to configure can be different depending on the type of widget you are configuring.

Configuring a SQL Query Data Source or Native SQL Query Data Source

The SQL Query data source is the data source that provides the greatest flexibility when selecting what data to display, as you can perform powerful queries.

The Native SQL Query data source, added in Control Center v5.67, simplifies the process of querying the Control Center database by removing the need to enter a connection string.








By default, only 100 rows will be used in dashboard widgets. If you need to display more rows than this please see [Configuring the Data Source row limit](#)

Never configure SQL queries directly against database tables as these might change. Instead, query views as these are maintained across releases.

For example, the following SELECT statement gives you the top 10 alarms by location.

```
SELECT top 10 FriendlyID,
  case when [status] = 'Unhandled' then 'red'
  when [status] like 'Parked By%' then 'Yellow'
  when [status] Like 'Handled By%' then '#00FF00'
  when [status] = 'Resolved' then 'rgb(255,140,0)'
  else ''
  end as Background,
  case when [status] = 'Unhandled' then 'fa-warning'
  when [status] = 'Handled By Administrator' then 'fa-cog'
  when [status] = 'Parked By Administrator' then 'fa-radiation'
  when [status] = 'Resolved By Administrator' then 'fa-thumbs-up'
  else ''
  end as Icon
  ,[AlarmTypeDescription],[Location], convert(VARCHAR, DateCreated, 0) AS DATE,
```


DateCreated from IPSC.AlarmDetailsView where [status] <> 'Resolved' order by DateCreated desc

Top 10 Alarms					
ID	Status	Alarm Type	Description	Location	Date/Time
279		Door state changed alarm		Site A	Dec 1 2020 10:45AM
278		Door state changed alarm		Site A	Dec 1 2020 10:45AM
277		Door state changed alarm		Site A	Dec 1 2020 10:45AM
276		Door state changed alarm		Building 11	Dec 1 2020 10:45AM
275		Door state changed alarm		Building 11	Dec 1 2020 10:45AM
274		Door state changed alarm		Building 11	Dec 1 2020 10:45AM
273		Door state changed alarm		Site A	Dec 1 2020 10:45AM

A SQL Query data source can be used with any type of widget.

Once you select **SQL Query** from the **Source type** drop-down list, the **Settings** you can define for the SQL query display.

1. In **Connection string**, type your database connection string or use an environment variable. For example, *Data Source=(local);Initial Catalog=pacific;Integrated Security=SSPI; or %dashboard_connection%* .

Using an environment variable instead of a connection string can help when creating multiple widgets or dashboards, or moving dashboards between environments. See [Creating an Environment Variable](#) for further information. If you want to query the Control Center database it is easier to use the Native SQL Query data source.

2. In **SELECT statement**, type your SELECT statement. For example,

```
SELECT Count(*) as AlarmCount
    , 'Blue'
FROM [pacific].[IPSC].[DeviceStatusCurrentView]
```

3. In **Refresh Interval (sec)**, type the number of seconds that you want Control Center to refresh the data.

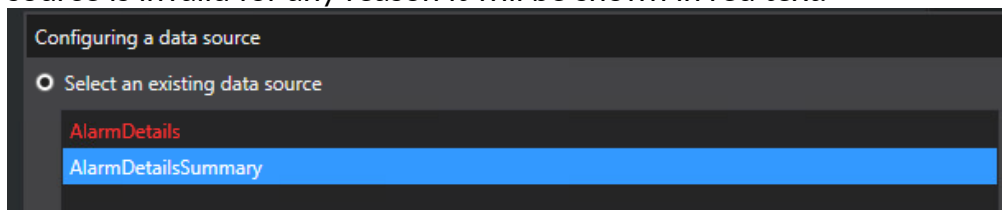
4. In **Name**, type a name for your data source.

See [Example SQL Queries](#) for some examples of SQL queries that you could use in a SQL Query data source.

Editing a SQL Query Data Source

SQL Query data sources can be edited if they are not linked to more than one widget on a dashboard.

1. Find and select the widget that is using the data source you want to edit.
2. Press **Select Data...** to open the **Configuring a data source** window. If a data source is invalid for any reason it will be shown in red text.



3. Select the data source you want to edit and press **Next**.
4. The **Connection string** and **SELECT statement** fields can now be edited from this screen. If the Connection string and SELECT statement fields are greyed out this means the data source is being used elsewhere in the dashboard.
5. Press **Next** again and map the results to the data source. Once done, press **Finish** to complete the editing process and apply the changes to the widget.

Configuring the Data Source row limit

By default, only 100 rows will be held in dashboard widget data sources. This can be changed by adding a key called 'DatasourcesSchemaMaxSize' to the Everbridge.ControlCenter.AlarmTypes.WindowsService.exe.config file. This has been tested up to 10000 rows.

```

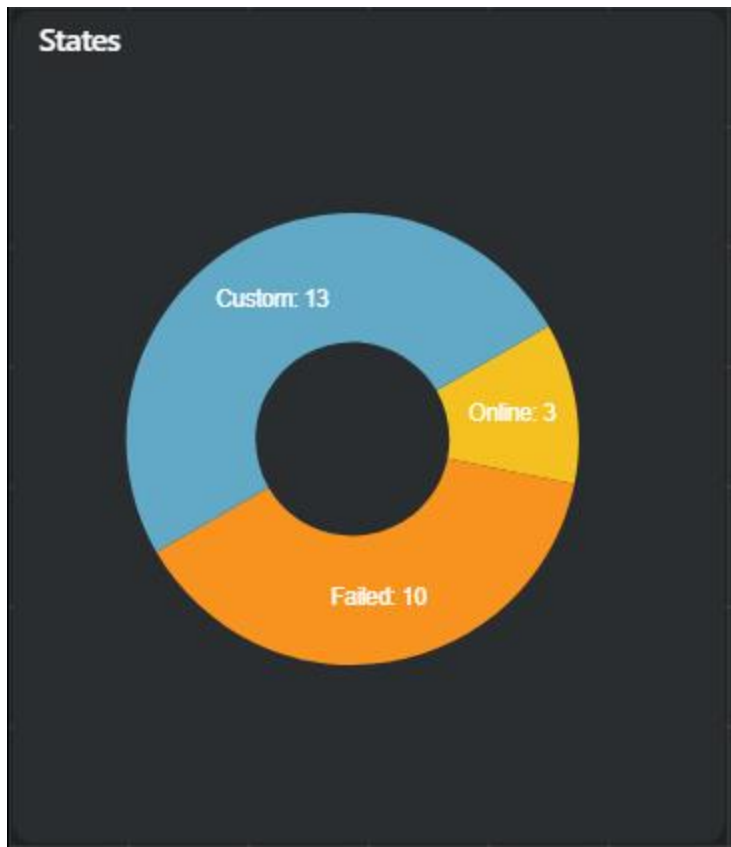
<!-- Cache Capacity for Track Headers -->
<add key="TracksHeaderCapacity" value="10000" />
<add key="DatasourcesSchemaMaxSize" value="500"/>
</appSettings>
<connectionStrings configSource="connectionstrings.config" />
    
```

Configuring Object States Data Source

When using the Object States data source, you have 2 options. You can choose to display information about

- states by device type
- states for all devices

The Object States data source displays best with a chart widget.



Once you select **Object States** from the **Source type** drop-down list, the **Settings** you can define for object states display.

1. In **Refresh periods**, set a duration for refreshing the selected data source
2. In **Name**, type a name for your data source.
3. Select a table from the data source. You can select either:
 - **By Device Type** - displays states by individual device type for all available devices
 - **All Devices** - Displays totals for object types for all devices.
4. Configure the property values.

Property	Description
Category	Select an object state. You can select one of the following types: <ul style="list-style-type: none"> ○ Type - Name of device type ○ Offline ○ Pending ○ Online

	<ul style="list-style-type: none"> ○ Failed ○ Custom
Value	<p>Select a value for your object state.</p> <ul style="list-style-type: none"> ○ Offline - Count of offline devices ○ Pending - Count of pending devices ○ Online - Count of online devices ○ Failed - Count of failed devices ○ Custom - Count of custom devices

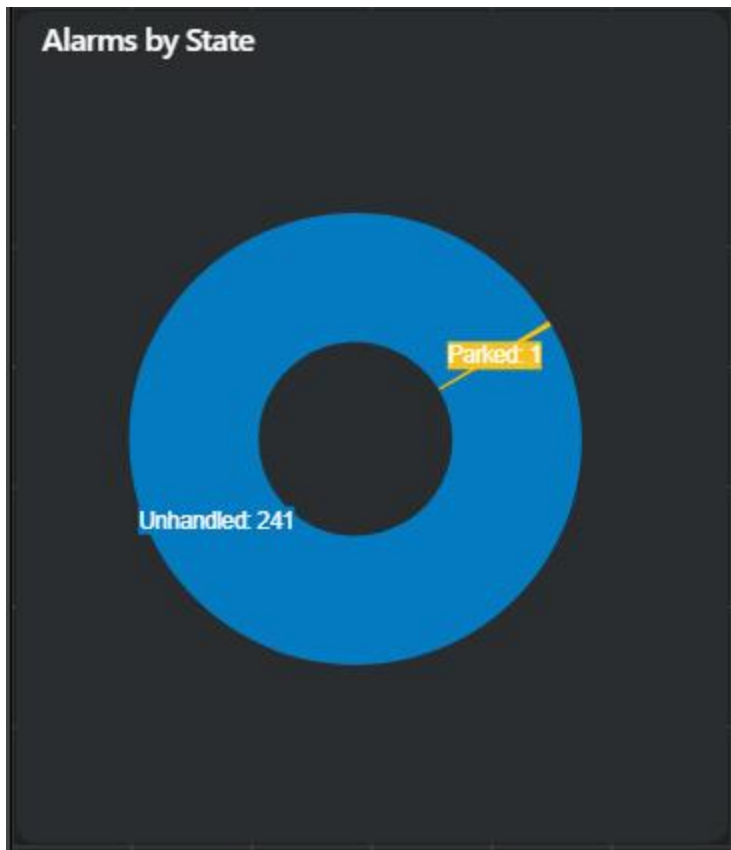
5. Select **Finish**.

Configuring Alarms Data Source

When using the Alarms data source, you have 3 options. You can choose to display information about

- Alarms by State
- Alarms by Priority
- Alarms by Alarm Type

The Alarms data source displays best with a chart widget.



Once you select **Alarms** from the **Source type** drop-down list, the **Settings** you can define for alarms display.

1. In **Refresh periods**, set a duration for refreshing the selected data source
2. In **Name**, type a name for your data source.
3. Select a table from the data source. You can select either:
 - **Alarm by State** - displays alarms by state for all available alarms.
 - **Alarms by Priority** - Displays alarms by priority for all available alarms.
 - **Alarms by Alarm Type** - Displays alarms by alarm type for all available alarms.
4. Configure the property values.

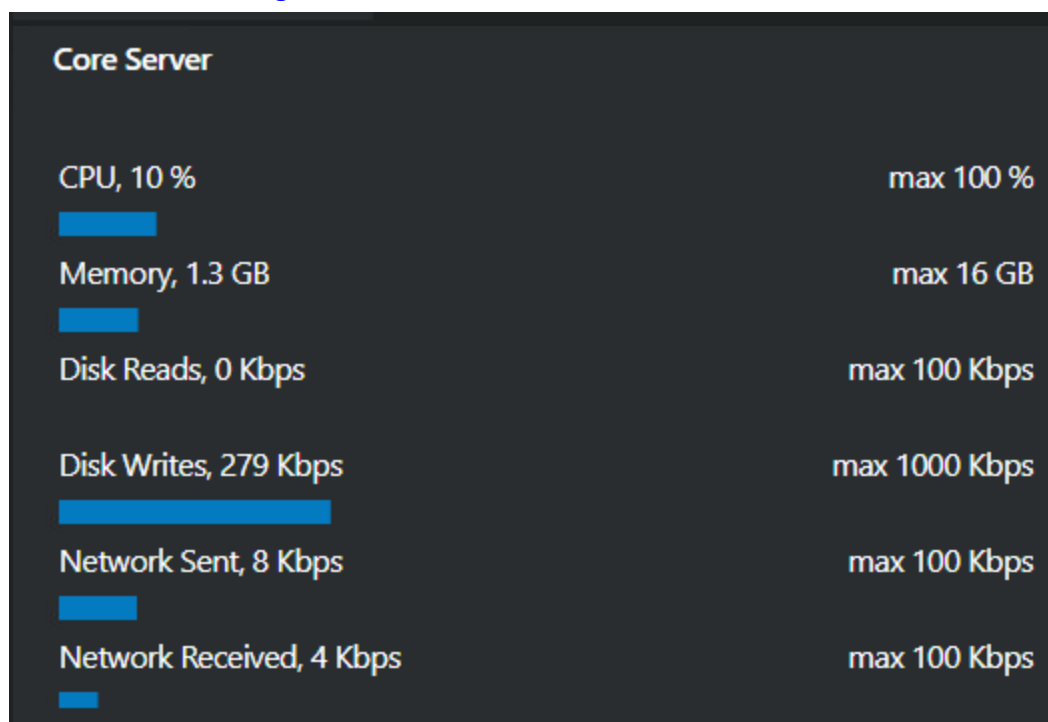
Property	Description
Category	Depending on which table you have selected, you can select: <ul style="list-style-type: none"> ○ <i>table</i> where table is the table you selected. For example, if you selected Alarms by Priority, the category is Priority.

	<ul style="list-style-type: none"> ○ Count to give a count of the number of alarms, in this case, by priority.
Value	Depending on which table you have selected, you can select: <ul style="list-style-type: none"> ○ <i>table</i> where table is the table you selected. For example, if you selected Alarms by Priority, the category is Priority. ○ Count to give a count of the number of alarms by priority.

5. Select **Finish**.

Configuring Machine Data Source

The machine data source must be used with a machine data widget. See [Configuring Machine Data Widgets](#).



The example below describes configuring a machine data source for a machine data widget.

Once you select **Machine Data** from the **Source type** drop-down list, the **Settings** you can define for alarms display.

1. In **Machine Name**, type the name of the machine whose data you want to display.
2. In **Refresh periods**, set a duration for refreshing the selected data source.
3. In **Name**, type a name for your data source.

4. Machine Data is already select as the table as this is the only table available for this data source type.
5. Configure the property values.

Property	Description
Category	Select from: <ul style="list-style-type: none"> ○ DateUpdated - to display the date the machine data was updated. ○ CPU - to display the CPU usage. ○ Memory - to display the memory usage. ○ TotalMemory - to display total memory. ○ DiskReads - to display disk reads. ○ DiskWrites - to display disk writes. ○ NetworkRecd - to display number of network packages received. ○ NetworkSent - to display number of network packages sent.

6. Select **Finish**.

Configuring RSS Feed Data Source

An RSS Feed data source displays best with a **List** or **Grid** widget. Using these widgets gives you greater control as to how the data from your RSS feed is displayed. Below is an example of an RSS feed in a **List** widget.

Top Stories

Critical Event Management Category Leader Everbridge Makes Key Appointments to Expand its Global Marketing and Communications Functions 11/24/2020, 2:00:00 PM

Veteran marketing executive and MIT Sloan School of Management graduate Stacey Wu , former head of global marketing at security software leader Fortinet where she helped grow the company's market cap from \$5B to over \$20B , joins Everbridge as Chief Marketing Officer Three-time CMO and Harvard

Everbridge Recognized in the Gartner 2020 Market Guide for Crisis/Emergency Management and COVID-19 Safe Return to Work Solutions 11/24/2020, 1:30:00 PM

Report calls for leaders responsible for crisis management to "deploy solutions to facilitate command and control before and during a crisis," including having a management plan to mitigate the coronavirus pandemic BURLINGTON, Mass. --(BUSINESS WIRE)--Nov. 24, 2020-- Everbridge , Inc.

Everbridge Named Top Three Highest-Rated Public Cloud Company to Work For During COVID-19 11/23/2020, 1:30:00 PM

Global investment firm Battery Ventures recognized Critical Event Management (CEM) leader Everbridge as top place to work amid the coronavirus pandemic, as measured by employee satisfaction provided by Glassdoor BURLINGTON, Mass. --(BUSINESS WIRE)--Nov. 23, 2020-- Everbridge , Inc.

Everbridge Wins Top Tech Company Awards in the Categories of COVID-19 Response and Business Accomplishment for 2020 11/16/2020, 1:30:00 PM

The Massachusetts Technology Leadership Council recognizes Everbridge for both its significant impact on helping organizations respond to the coronavirus pandemic and for its business accomplishments over the prior year BURLINGTON, Mass. --(BUSINESS WIRE)--Nov. 16, 2020-- Everbridge , Inc.

See [Configuring List Widgets](#), [Configuring Grid Widgets](#).

Once you select **RSS Feed** from the **Source type** drop-down list, the **Settings** you can define for RSS feed display.

1. In **Address**, type the address of the RSS feed whose data you want to display. For example, <http://feeds.bbc.co.uk/news/rss.xml?edition=uk> This can also be a local RSS XML file.
2. In **Refresh interval**, set a duration for refreshing the selected data source.

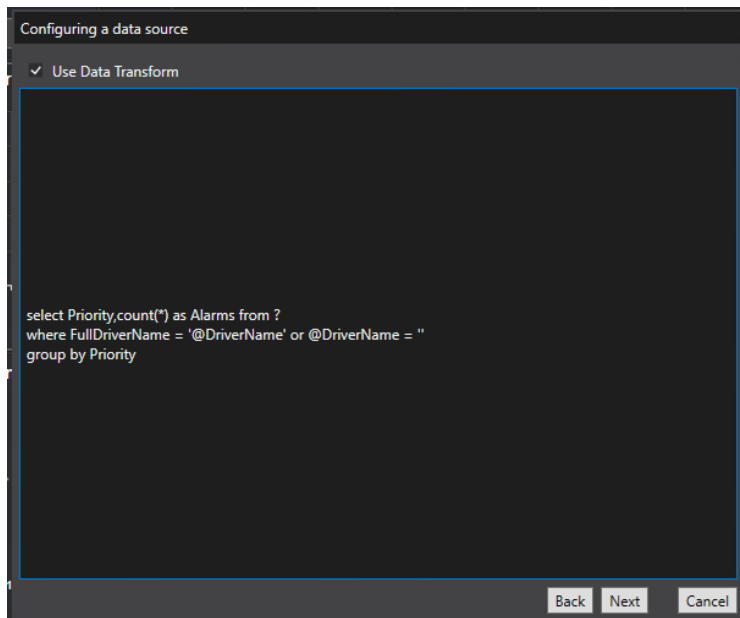
3. In **Name**, type a name for your data source.
4. **RSS Feed** is already selected as the table as this is the only table available for this data source type.
5. Configure the property values.

Property	Description
Title	The title of RSS feed. Select Exclude? if you do not want the title of the RSS feed to display in the widget.
Description	A description of the RSS feed. Select Exclude? if you do not want the description of the RSS feed to display in the widget.
PublishDate	The date and time the information is published in the RSS feed. The date and time is converted to the local time of the Control Center client viewing the dashboard. Select Exclude? if you do not want the date and time an entry in the RSS feed was published to display in the widget.

6. Select **Finish**.

Data Transformation

Data transformation is an optional step in the Data Source selection process.



Data transform uses [AlaSQL](#) to perform SQL-like operations on the data set returned by the data source selected in the previous step. This data set is represented as '?' in the data transform step. These operations are performed on the client side and enable the use of variables controlled by filter widgets or scripting within other widgets.

An example of the typical syntax to enable a widget to respond to a filter widget with a variable name *FilterVariable* would be:

```
SELECT * FROM ? WHERE Column1 = '@FilterVariable' or '@FilterVariable' = '';
```

This means that when the filter widget is not in use all data from the original source is returned. When the filter is set and the value of @FilterVariable is set then only records matching that will be returned.

Please note that single quotes are required around the filter variable when the value of that variable is a string.

Data transform can also be used to perform aggregations or other complex operations on an existing data source.

Some notes on using Data Transformation effectively:

- Only columns included in the original data source are available in the data mapping step of the process.
- Column names are case sensitive.
- To add a new column as part of the transform step you need to first add an empty column to the original data source – e.g. `Select *, '' AS NewColumn from [Table]` – this then allows you to define the value of NewColumn as part of the transform step and map it to your widget in the next step.
- If you perform an aggregation on a column you must use AS and assign the aggregation the same name as the original column – e.g. `'SELECT COUNT(Alarms) AS Alarms'`

Displaying Dashboards as a tile

Once you have created your dashboards, you must configure them to display on your Control Center clients.

1. From **System Configuration** window, navigate to the folder where you have created your dashboards.
2. Right-click and select **New > Tile Layout**.
3. Type a name for your new tile layout.

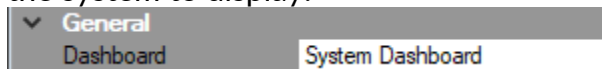
4. Double-click your new tile layout to edit it.
5. From the **Layout** drop-down list in the tile layout menu bar, select **1-way**.
6. Go back to the tab where your dashboard is stored.
7. Drag your dashboard to the new tile layout tab. The tile layout displays and you can drop your dashboard onto the layout.
8. Save the changes to your tile layout.
9. Go back to your Control Center client and select **System > Setup Display**.
10. Create a display area to display your new tile layout. See [Adding a Display Area](#).

Displaying Dashboards as part of a GUI

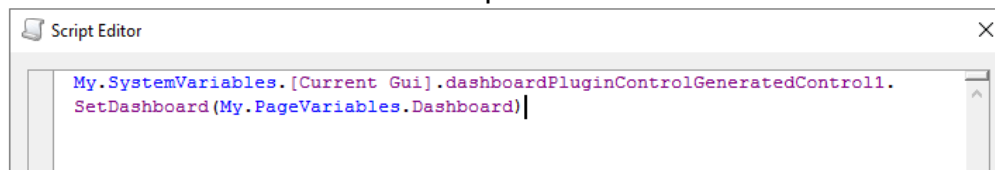
Dashboards can also be displayed as part of a GUI by using the Dashboard Plug-in control. This allows for scripting from other parts of the system to interact with the GUI, setting filters or changing the displayed dashboard dynamically.

To add a dashboard to a Control Center GUI:

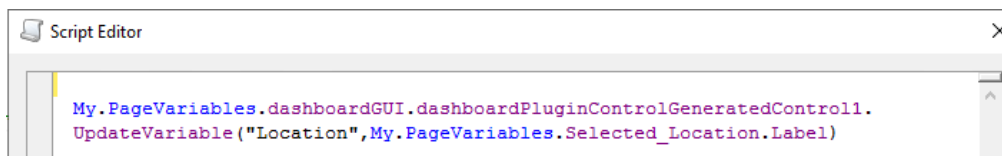
1. Open a GUI, or create a new GUI, that you want to add a dashboard to.
2. Expand the Plug-in Controls section of the Toolbox window.
3. Drag the Dashboard Control to the GUI design surface.
4. In the properties section of the control, you can select a dashboard object from the system to display.



5. Alternatively, you can select the dashboard to be displayed using a scripting method **SetDashboard** which accepts a Dashboard variable.



The plug-in control has additional scripting methods **UpdateVariable** and **UpdateVariableAndColor** which can be utilized from other parts of the system to set the value of filter variables within the dashboard.



These filter variables can be used in the Data Transform step of dashboard data source(s) to filter the data displayed to the end user.

When put together, this enables dashboards that can be filtered dynamically based on user actions within the system.

Example SQL Queries

Here are some examples of SQL queries that you could use in a SQL Query data source. See [Configuring a SQL Query Data Source](#).

Never configure SQL queries directly against database tables as these might change. Instead, query views as these are maintained across releases.

Alarm Details View - Color

This query builds a custom version of the **Alarm Details View**. It uses an additional field in the **Location** object that you can configure in Object Designer. See [Object Designer](#). If you configure a color for each custom field for each object, you can represent each location in the query below with a specific color. See [Configuring Colors in Dashboards](#) for information about defining custom colors in dashboards. If you leave the custom field blank, the object displays as a default color.

```
USE [pacific]
```

```
GO
```

```
SET ANSI_NULLS ON
```

```
GO
```

```
SET QUOTED_IDENTIFIER ON
```

```
GO
```

```
CREATE VIEW [IPSC].[AlarmDetailsView_color]
```

```
AS
```

```
SELECT A.ID AS AlarmID,
```

```
    A.FriendlyID,
```

```
    A.Priority,
```

```
    A.SlaLevel,
```

```
    A.DateCreated,
```

```
    LCF.Value,
```

```
    F.Label,
```

```
    Alarms.AlarmResolution.DateResolved,
```

```
    Alarms.AlarmResolutionType.Name AS ResolutionType,
```

```
    (CASE
```

```

        WHEN A.AlarmTypeID IS NOT NULL
        THEN Alarms.AlarmType.Label
        ELSE Alarms.CorrelatedAlarmType.Label
    END) AS AlarmType,
    (CASE
        WHEN A.AlarmTypeID IS NOT NULL
        THEN Alarms.AlarmType.ID
        ELSE Alarms.CorrelatedAlarmType.ID
    END) AS AlarmTypeID,
    (CASE
        WHEN A.AlarmTypeID IS NOT NULL
        THEN Alarms.AlarmType.Description
        ELSE Alarms.CorrelatedAlarmType.Description
    END) AS AlarmTypeDescription,
    AlarmLocation.Label AS Location,
    A.Status,
    IPSC.[User].Label AS [User],
    IPSC.AlarmPointForAlarmIDView.ObjectID,
    IPSC.AlarmPointForAlarmIDView.AlarmPoint
FROM Alarms.Alarm A WITH (NOLOCK) LEFT OUTER JOIN
    Alarms.AlarmResolution WITH (NOLOCK) ON A.AlarmResolutionID =
Alarms.AlarmResolution.ID LEFT OUTER JOIN
    Alarms.AlarmResolutionType WITH (NOLOCK) ON
Alarms.AlarmResolution.ResolutionTypeID = Alarms.AlarmResolutionType.ID LEFT
OUTER JOIN
    ipsc.Folder F ON F.ID = A.AlarmLocationID LEFT OUTER JOIN
    IPSC.LocationCustomField LCF ON LCF.LocationID = F.ID LEFT OUTER JOIN
    IPSC.[User] WITH (NOLOCK) ON IPSC.[User].ID =
Alarms.AlarmResolution.OperatorID LEFT OUTER JOIN
    Alarms.AlarmType WITH (NOLOCK) ON A.AlarmTypeID =
Alarms.AlarmType.ID LEFT OUTER JOIN
    Alarms.CorrelatedAlarmType WITH (NOLOCK) ON A.CorrelatedAlarmTypeID
= Alarms.CorrelatedAlarmType.ID LEFT OUTER JOIN
    IPSC.AlarmPointForAlarmIDView WITH (NOLOCK) ON A.ID =
IPSC.AlarmPointForAlarmIDView.AlarmID LEFT OUTER JOIN
    (SELECT DISTINCT Alarms.Alarm.ID,
        Alarms.Event.LocationID,
        IPSC.Folder.Label
    FROM Alarms.Event WITH (NOLOCK) INNER JOIN
        Alarms.AlarmEvent WITH (NOLOCK) ON
Alarms.AlarmEvent.EventID = Alarms.Event.ID INNER JOIN
        Alarms.Alarm WITH (NOLOCK) ON Alarms.AlarmEvent.AlarmID
    
```

```
= Alarms.Alarm.ID INNER JOIN
    IPSC.Folder WITH (NOLOCK) ON Alarms.Event.LocationID =
IPSC.Folder.ID) AS AlarmLocation ON A.ID = AlarmLocation.ID
```

```
GO
```

Top Unresolved Alarm by Location

This query returns a single unresolved alarm per location.

```
USE [pacific]
GO
```

```
SET ANSI_NULLS ON
GO
```

```
SET QUOTED_IDENTIFIER ON
GO
```

```
CREATE VIEW [IPSC].[TopAlarmByLocation]
AS
  With MyRowSet AS
(SELECT [AlarmID]
  ,[FriendlyID]
  ,[Priority]
  ,[SlaLevel]
  ,CONVERT(varchar(20),[DateCreated],113) as Date
  ,[DateResolved]
  ,[ResolutionType]
  ,[AlarmType]
  ,[AlarmTypeID]
  ,[AlarmTypeDescription]
  ,[Location]
  ,[Value]
  , case when [status] = 'Unhandled' then 'fa-warning'
  when [status] = 'Handled By Administrator' then 'fa-cog'
  when [status] = 'Parked By Administrator' then 'fa-radiation'
  when [status] = 'Resolved By Administrator' then 'fa-thumbs-up'
  else ''
  end as Icon
  ,[Status]
  ,[User]
  ,[ObjectID]
```

```

        ,[AlarmPoint]
        ,Row_Number() OVER (PARTITION BY [Location] ORDER BY Priority ASC) as
    RowNum
    FROM [pacific].[IPSC].[AlarmDetailsView_color] WHERE DateResolved is null)
    Select * from MyRowSet WHERE RowNum <= 1
    GO
    
```

Unresolved Alarms by Priority

This query returns all unresolved alarms ordered by highest priority.

```

USE [pacific]
GO
    
```

```

SET ANSI_NULLS ON
GO
    
```

```

SET QUOTED_IDENTIFIER ON
GO
    
```

```

CREATE VIEW [IPSC].[AlarmsByPriority]
AS
    Select [Priority],Count(AlarmID) as AlarmCount,
    Case
    when [Priority]='1' then '#b50000'
    when [Priority]='2' then '#f7931e'
    when [Priority]='3' then '#f4c120'
    when [Priority]='4' then '#047bc0'
    end as Colour
    From IPSC.AlarmDetailsView Where DateResolved Is Null Group By [Priority]
GO
    
```

Alarms by Location

This query returns a count of alarms by location.

```

USE [pacific]
GO
    
```

```

SET ANSI_NULLS ON
GO
    
```

```

SET QUOTED_IDENTIFIER ON
GO
    
```

```

CREATE VIEW [IPSC].[AlarmsByLocation]
AS
Select [Location],
Count([AlarmID]) as AlarmCount,
[Value]
From IPSC.AlarmDetailsView_color Where DateResolved Is Null Group By [Location],
[Value]
GO

```

Alarms by Alarm Type

This query returns a count of alarms by alarm type.

```

USE [pacific]
GO

```

```

SET ANSI_NULLS ON
GO

```

```

SET QUOTED_IDENTIFIER ON
GO

```

```

CREATE VIEW [IPSC].[AlarmsByAlarmType]
AS
Select [AlarmType],Count(AlarmID) as AlarmCount,
Case
when [AlarmType]='Door Forced' then '#0077C8'
when [AlarmType]='Door Held' then '#DF1883'
when [AlarmType]='Motion Detected' then '#C273B2'
when [AlarmType]='Tamper' then '#E6AC73'
end as Colour
From IPSC.AlarmDetailsView_color Where DateResolved Is Null Group By [AlarmType]
GO

```

Top 10 Unresolved Alarms by Created Date

This query returns the top 10 unresolved alarms by the date the alarms were created.

```

USE [pacific]
GO

```

```

SET ANSI_NULLS ON
GO

```

```

SET QUOTED_IDENTIFIER ON

```


GO

```

CREATE VIEW [IPSC].[Top10Alarms]
AS
  SELECT top 10 FriendlyID,
  case when [status] = 'Unhandled' then '#b50000'
  when [status] like 'Parked By%' then '#f4c120'
  when [status] Like 'Handled By%' then '#f7931e'
  when [status] = 'Resolved' then '#1E824C'
  else ''
  end as Background,
  case when [status] = 'Unhandled' then 'fa-warning'
  when [status] = 'Handled By Administrator' then 'fa-cog'
  when [status] = 'Parked By Administrator' then 'fa-radiation'
  when [status] = 'Resolved By Administrator' then 'fa-thumbs-up'
  else ''
  end as Icon
  ,[AlarmTypeDescription],[Location], CONVERT(varchar(20),[DateCreated],113) as
  DateCreated from IPSC.AlarmDetailsView where [status] <> 'Resolved' order by
  DateCreated desc
GO

```

Reports

You can generate reports using Microsoft SQL Server Reporting Services (SSRS) to enable closer integration with other business intelligence reporting systems.

Several views of the data have been included in Control Center to expose data in a usable format. These are part of the Pacific database schema.

In addition to the Pacific database schema, the optionally installed Auditing database schema has been included which is a transaction database of all activities that have occurred within Control Center.

Business Reporting Integration Prerequisites

- A version of SQL Server that includes SSRS must be installed.
- The SQL Server Reporting Services feature must have been selected during SQL Server installation. SSRS is a component of SQL Server that runs as a separate process and configured through separate tools to the main database engine. It can be optionally deployed on a separate server or cluster for performance reasons.
- Internet Explorer (Version 6.0 or above) is required for access to the Report Manager.

Control Center Server Deployment

Control Center and SQL Server Reporting Services can be deployed in two ways:

- Control Center can be installed on the SQL Server that is configured for reporting.
- Otherwise, if SSRS and the Control Center Server are not deployed on the same machine then Control Center should be configured to run as a domain user rather than a local Windows user.

SSRS Security Considerations

The list below is a guideline on limitations to consider when commissioning the Control Center SSRS integration on a SQL Server, as SQL Server security itself is a complex subject that is already well-documented elsewhere.

- SSRS has options to restrict permissions on individual reports. However, these permissions are applied based on the credentials used to connect to the report service. Control Center always uses the Windows user that its server process is running as to connect to SSRS, so permissions are all-or-nothing for Control Center users.
- If the SSRS installation is used for reporting tasks other than Control Center, Control Center should be denied permissions on those report templates, and to any databases that it does not need access to.

- Care should be taken to limit the users authorized to connect to the SSRS Web interface.
- Control Center permissions are not evaluated during report generation, so a report could reveal covert users unless this is specifically added to the report query.
- SSRS uses the credentials specified in the Data Source object to connect to the database. In the configuration example outlined in the document, this will cause it to impersonate the Windows user that the Control Center Server process is running as.

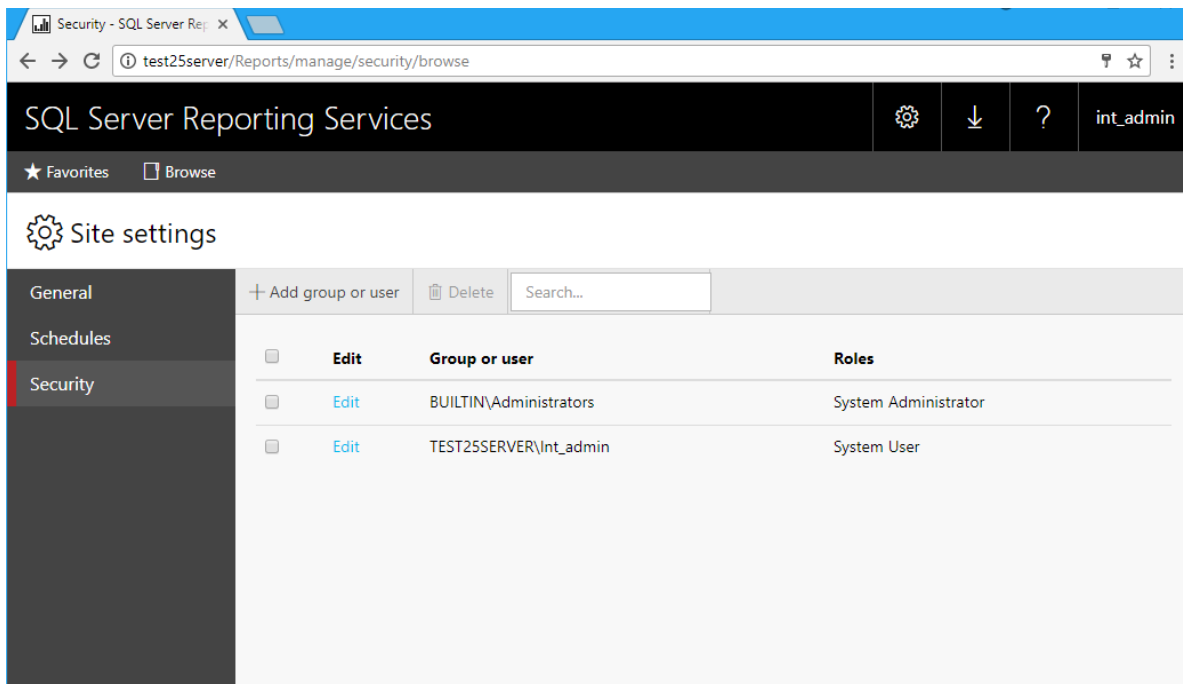
Setting SSRS Permissions

Permissions must be set to allow users to use the service and access the reporting features.

To set SSRS permissions:

1. Browse to the SSRS Report Manager in Internet Explorer using the URL that was provided in the SSRS Configuration Manager.

Bookmark the page to navigate to it more quickly next time.

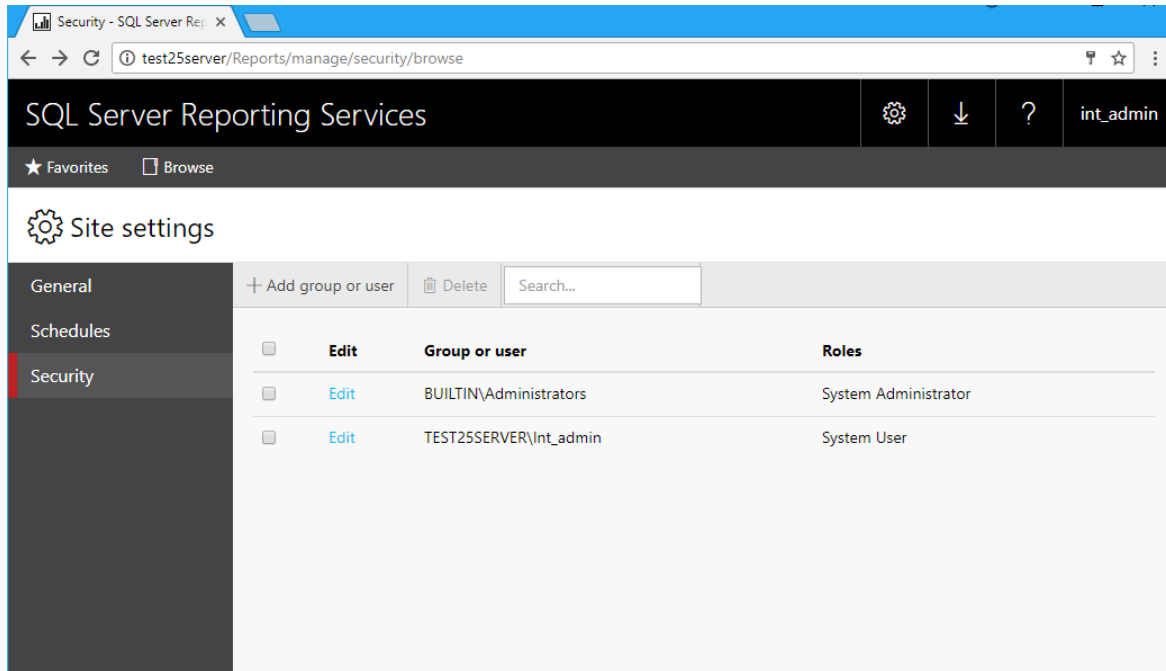


	Edit	Group or user	Roles
<input type="checkbox"/>	Edit	BUILTIN\Administrators	System Administrator
<input type="checkbox"/>	Edit	TEST25SERVER\Int_admin	System User

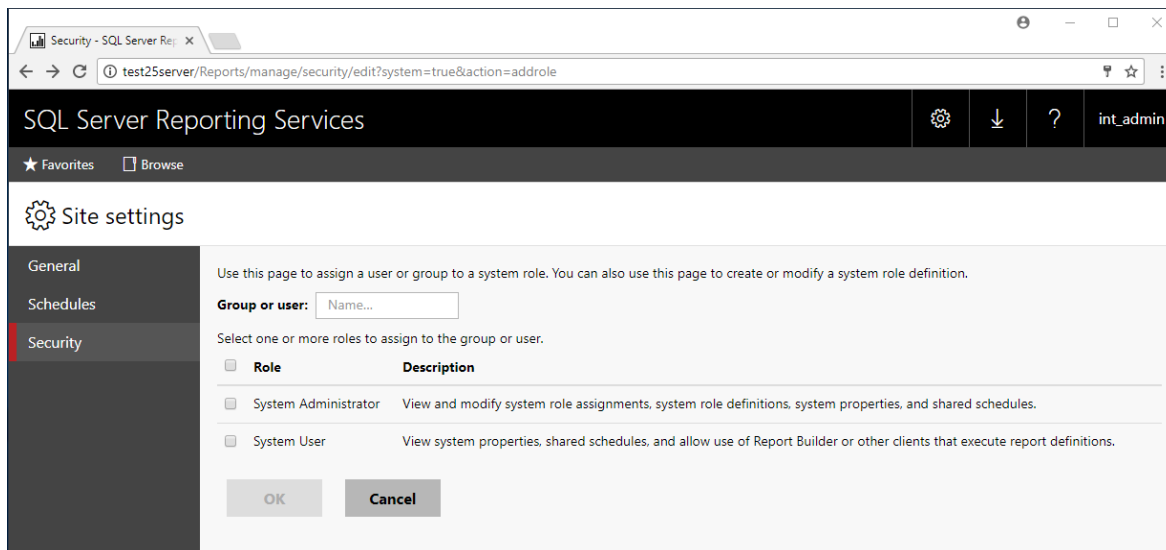
The site may be blocked by Internet settings or the service unavailable.

2. Click the **Site Settings** link located in the ribbon in the top right. The **Site Settings** menu appears.
3. Click the **Security** menu on the left.

4. Click the **New Role Assignment** button in the tool bar. The **New System Role Assignment** menu appears.
5. In the **Group or Username** field, enter the username of the user authorized to run server processes. Select **System User** and click **OK**. This will configure SSRS to allow Control Center to connect and generate reports. Additional Users can be added in the same way to allow them to create and manage reports.



The New System Role Assignment menu appears.

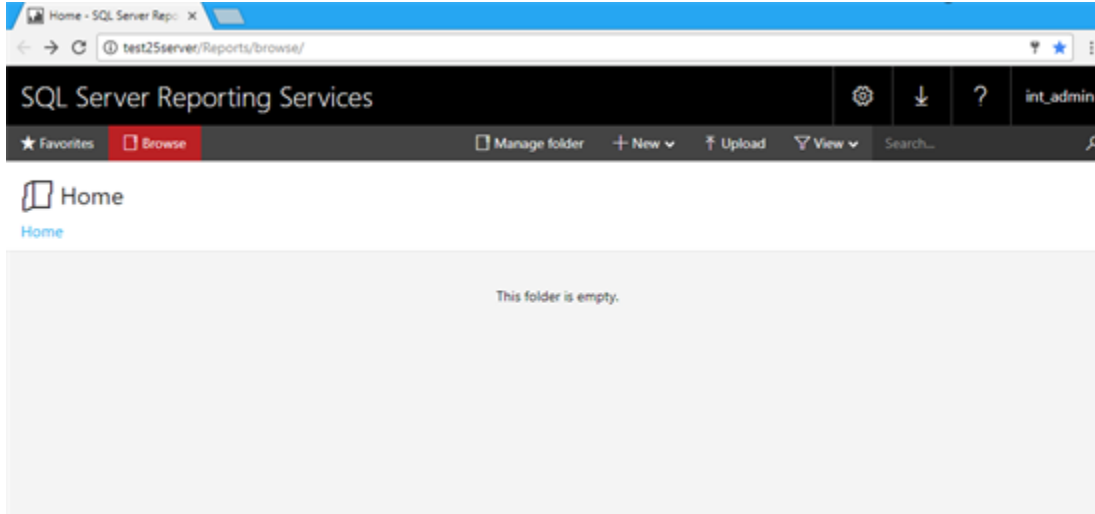


6. In the **Group or username** field enter the username of the user authorized to run server processes. Select System User and click **OK**. This will configure SSRS to allow Control Center to connect and generate reports. Additional Users can be added in the same way to allow them to create and manage reports.

Creating a Data Source

To create a data source:

1. Open a browser and enter the URL for the SSRS Report Manager generated as a result of in the process above.



2. From the menu, click the **New > New Data Source** drop down.

[Home](#) > [Pacific](#)

Properties
Subscriptions
Dependent items
Security

↑ Replace
↔ Move
🗑 Delete

Properties

Name

Description

Credentials

Log into the data source

As the user viewing the report
 Using the following credentials
 By prompting the user viewing the report for credentials

Type of credentials

Windows user name and password ▼

Prompt

Without any credentials

Test connection

Apply
Cancel

The **New Data Source** dialog appears.

3. Enter the data source **Name** and a **Description**.
4. Enter the **Data Source Type**, **Microsoft SQL Server**.
5. Enter the **Connection String**. If using the SSRS default, enter Data Source=localhost; Initial Catalog=pacific. If using your own settings, change the source to the correct server.
6. Select the **Using the following credentials** option. To be able to generate reports from different workstations with different user credentials, the authorized user credentials need to be stored for the data source in the Report Server. Failing to do this will result in an error.

7. Click **Test Connection**. If the connection is correct, **Connection created successfully** appears below the **Test Connection** button.

If an error message appears, check that the Pacific database is installed, and the current logged in user account has permissions to read the database.

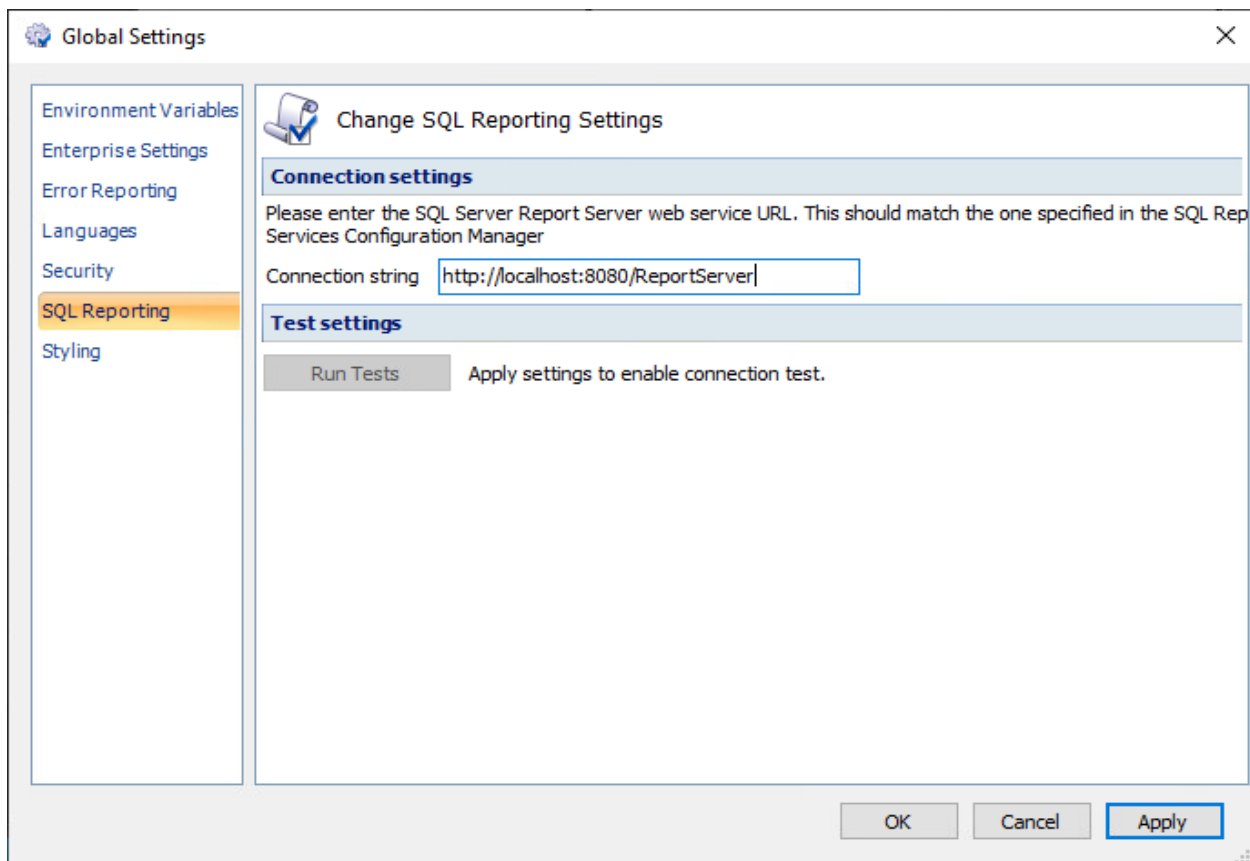
8. Click **OK**.

Configure Control Center Connection to SSRS

To utilize SQL reporting with Control Center, a connection string must be specified in Control Center Global Settings. This enables a Generate External Report VRP shape to generate reports.

To configure Control Center connection:

1. Open Control Center and select **System Configuration**.
2. Click **Global Settings** in the toolbar. The **Global Settings** dialog appears.
3. Click the **SQL Reporting** menu item.



4. In the **Connection String** field, type the report server web service URL from the SSRS Configuration Manager (for example, <http://localhost:80/ReportServer>) and click **Apply**.

5. Click the **Run Tests** button. Connection tested successfully appears in the dialog to verify a successful connection.

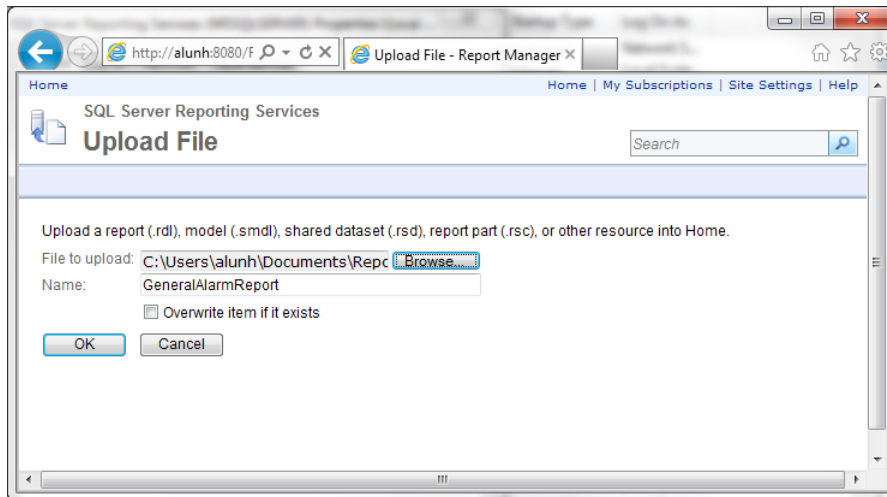
Permission error messages at this point can be caused by the Control Center service user account not having permissions.

Uploading SSRS Report Templates

To save time, existing report templates can be uploaded into SQL Reporting to facilitate sharing.

To upload report templates:

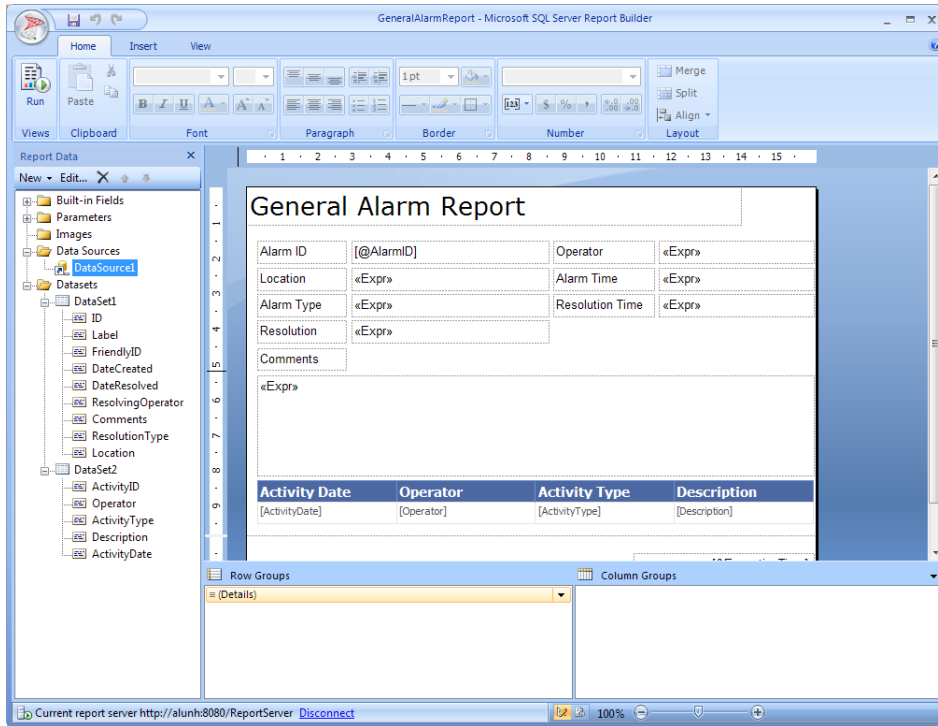
1. On the home screen of the SSRS Report Manager, click **Upload File**.



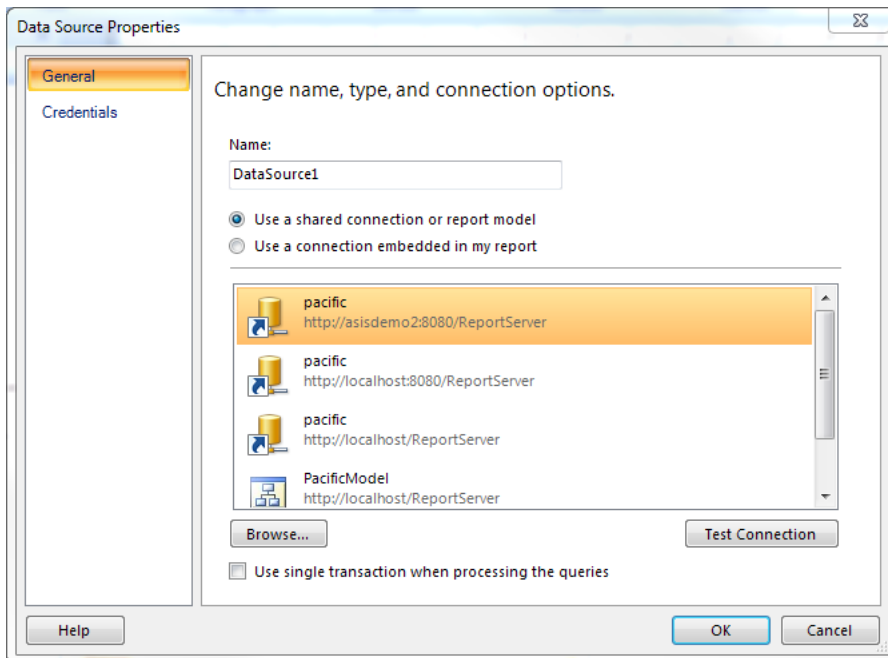
2. Click **Browse** and find the report template RDL file to use.

New report templates can be created using Report Builder.

3. Change the **Name**, if required, and click **OK**. The report template now appears as an icon on the home screen of the Report Manager.
4. Hover the mouse over the report icon in the Report Manager and use the drop-down menu to select **Report Builder**. The **Report Builder** appears.

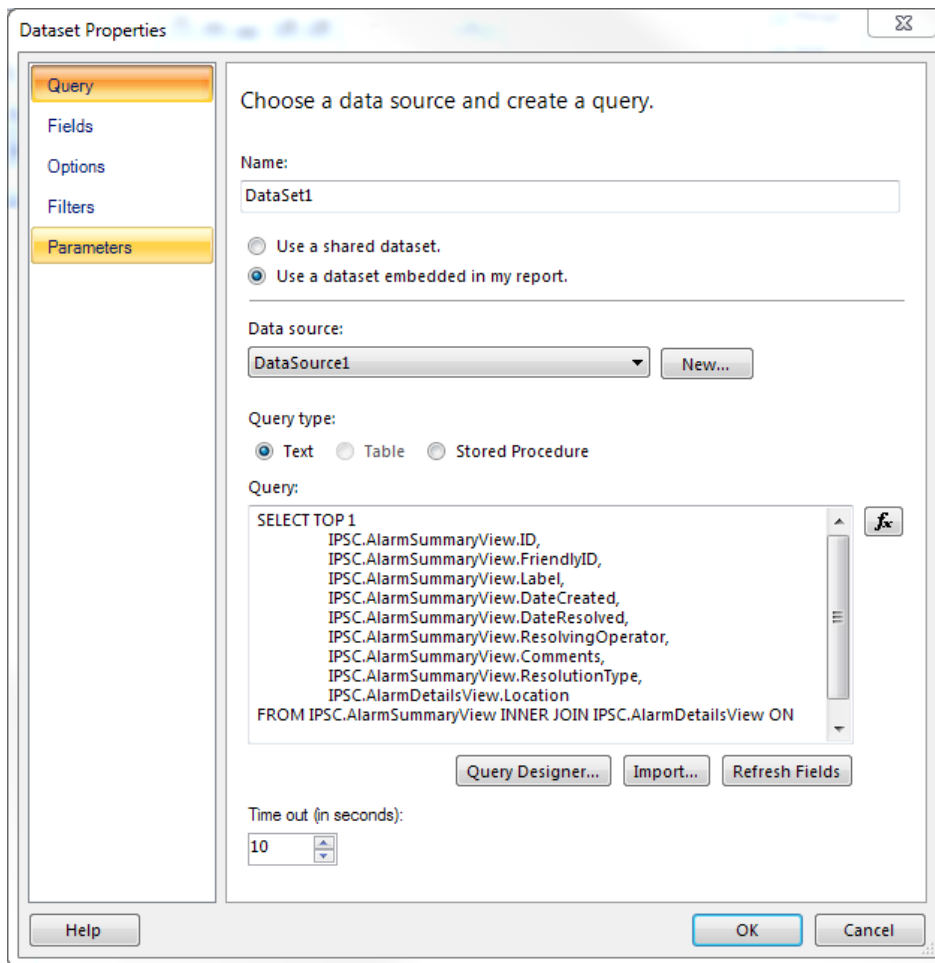


- From the left panel, select the **Data Sources** folder and then right-click to select **Properties**. The **Data Source Properties** dialog appears.



- In the **General** menu item, click **Browse** and select the data source that was created on this server. Click **OK**. Make sure to confirm that each Dataset refers to the data source just created.

7. In the Report Builder, click each Dataset in turn and right-click to select **Properties**.



8. On each Dataset item, confirm that the Data source displayed is the one just created (for example, DataSource1). If it is not, use the drop-down arrow to select the correct Data source and click **OK**. Only after the Data Source on each Dataset has been checked, test the report.
9. You can either:
 - o In the Report Builder, right-click the **Report** and select **Run** from the menu, or
 - o In Report Manager, hover over the report and select **Run** from the drop-down.

Report parameters appear on the screen.

10. Select the required report variables and click **View Report**. The report appears in the screen ready for use.

Downloading SSRS Report Templates

For ease of use and to save time, report templates (RDL files) can be downloaded from SSRS to use with other reporting tools.

Open the Report Manager, as outlined in the previous section. Select the report icon and select Download from the drop-down menu and click Save.

Generating a Report via the SSRS Web Interface

To do this:

1. Open **Report Services Home** Page and select the report. If the report uses parameters, a prompt appears at the top of the screen.
2. Select the necessary parameters and click **View Report**. An HTML view of the report appears in the browser. The **Save** button in the toolbar allows for exporting the report as XML, CSV, PDF, Compiled HTML, Excel (in the older XLS format), TIFF, and Word file. Selecting this option regenerates the report in real time so the data might not match the HTML view.

Generating a Report via Control Center

The **Generate External Report** shape allows Control Center to request a report from SSRS. Before configuring the **Generate External Report** shape, ensure the following:

- You have configured SQL Reporting in Global Settings.
- At least one report template exists.

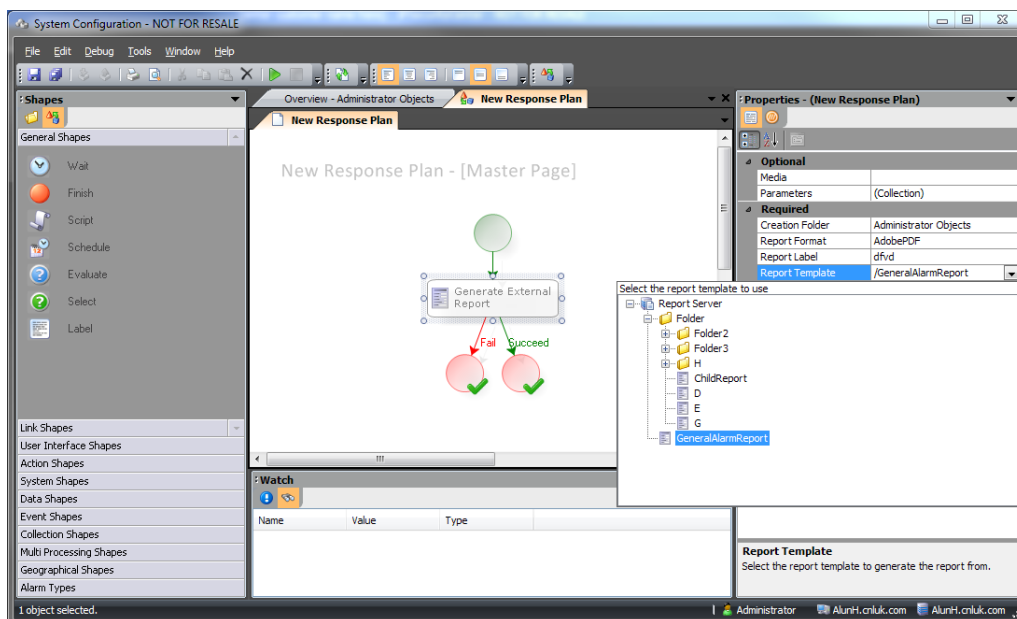
To configure the Generate External Report VRP shape:

1. From Control Center, open **System Configuration**, and select the folder to store the logic for the report.
2. In the middle pane, right-click and select **New** and then **Response Plan**.
3. Label the Response Plan and select **Generate device status report**.
4. Press **Enter**.
5. Right-click the report and select **Edit**. The **Response Plan Designer** appears.
6. In the **General Shapes** tab, select the **System Shapes** pallet.
7. Locate **Generate external report** and drag it to the **Designer**. Properties are automatically shown on the right of the window.
8. Set the following properties.

Creation Folder	The folder in Control Center to store the generated report.
------------------------	--

Report Format	The media type to export, such as PDF, XLS, etc.
Report Label	The label to apply to the generated media object.
Report Template	The report template within SSRS to use for generating the report (see image below for example of the selection tool).
Media (optional)	A variable of type Media to populated with the generated report.
Parameters (optional)	A collection of bindings between Control Center variables and report parameters. The Report Template property must have been set before Parameters can be configured. Right-click anywhere on the Design surface and select Finish all routes from the menu.

- Right-click anywhere on the Design surface and select **Finish all routes** from the menu.



In addition, you can perform the following actions on the report:

- To save the report, click Save in the tool bar.
- To run the report, click Play in the tool bar.
- To verify the report has run successfully, check the folder containing the report.

- To verify an error message if the shape fails or debugging, click the Fail route path.

Depending on the complexity of the report and the load on the server, this could take a few minutes to appear. Complicated or large reports should not be generated in time-sensitive response plans.

Generating Permission-Aware Reports

You can generate permissions-aware reports that enable you to view the changes in user sessions in Control Center. The reports must be run from within Control Center or by specifying a valid user session at the point of report execution. These reports only reveal information about locations, devices, and alarms that were available to view at the time the report was run.

Prerequisites:

- Installed SQL Server Reporting Services (SSRS).
- Configured the reporting services as specified in the Configuring SSRS section.
- Followed the Dynamic Permissions section to configure users and groups for permission aware settings.
- Log in to a second Windows Client as another user (CNL User) to be able to validate permission-based aware reports.
- Copy the Session ID for the CNL User's Client machine.

To generate a permission aware report:

1. Open a browser of your choice and enter the URL to the Report Server that you configured before. For example, <http://localhost/Reports>, where Local Host should be replaced with the machine name where the Reporting Services are installed.
2. Upload an existing report template or use the report builder to define a template, for example, a permission-based Alarms Report.
3. Create a new response plan by clicking **New > Response Plan**. A new response plan is created.
4. Configure the following options:
 - a. Provide a meaningful name, for example, Permission Aware Report and open it.
 - b. Add two new Text variables: **error**, **sessionID**.
 - c. In the **Report Designer**, drag and drop the **Generate External Report System Shape**.
 - d. Configure the following **System** shape properties:

Variable Mappings		
Use the grid below to map variables in this Response Plan to parameters in the Report Template		
Parameter	Action	Value
- Required		
SessionID	<input type="radio"/> Static	92db09bf-a644-4ef8-9286-...

The Session Id must be copied each time the second client is logged off from an existing session. To view the session ID, run the following query in SQL Server:

- **Creation Folder** – The folder in which the report will be located. For example, Devices or Media.
- **Report Format** – The format in which the report will be generated. The options are: Adobe PDF, Microsoft Excel, and Plaint text.
- **Report Label** – The label of the report.
- **Error** – The Error variable as specified earlier.
- **Parameters** – The Session ID parameters for the second Client (CNL User) copied from SQL Server > Pacific > Tables > IPSC.SecurityAccessToken table.
- **Report Label** – Specify a label for your report.
- **Report Template** – Select the report template that was defined in the Report Server: Select *from IPSC.SecurityAccessToken

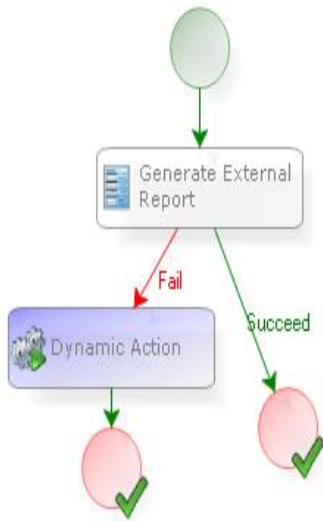
100 %

Results Messages

	Id	UserId	ClientId	ServerId	ClientAddress	ClientType	CreationTime	ExpirationTime
System User ID	5F892F8C-C07D-4358-B5D8-6FE075AB40EF	85B9E342-38A8-E711-9632-0050568CA7A8	NULL	82B9E342-38A8-E711-...	test2server.cnuk.com	0	2017-10-03 12:4...	9999-12-31 23:59...
CNL User ID	92D809BF-A644-4EF8-9286-8FB855A8030E	502C6140-A8A8-E711-9634-0050568CA7A8	E98291A9-3AA8-E711-...	NULL	test1server.cnuk.com	1	2017-10-09 07:5...	2017-10-09 10:14...
Administrator	F70FD36B-1167-4D90-92B7-F58D78B500ED	91B9E342-38A8-E711-9632-0050568CA7A8	0250C62E-3AA8-E711-...	NULL	test2server.cnuk.com	1	2017-10-09 08:0...	2017-10-09 10:14...

- e. From the **Shapes** palette, drag and drop off a **Dynamic Action** shape, and configure the following message:
 - i. Click **Next** until the **Target Object** page displays and select the target as your computer name.
 - ii. On the **Actions** page, click the **Message Box** field and then click **Variable** to assign the error variable.
 - iii. Click **Next** until you reach the **Finish** page.
- f. Complete the response plan by adding **Finish** shapes to all the routes and save it.

Permission Based Alarms Report [Master Page]



5. Create a new GUI by clicking **New > Graphical User Interface**. A new Graphical User Interface appears in the list of GUIs ready to be named. Configure the GUI by performing the following steps:
 - a. Specify a name for the new GUI and double-click to open it. The new GUI is loaded in the **Design Surface**.
 - b. From **Toolbox**, drag and drop a button control and rename it to something meaningful, for example, **Run Report**.
 - c. From the first dropdown, select **guiButton1** and then select the **Clicked** event. The **guiButton1_Clicked** response plan appears.
 - d. Add the following page variables with visibility set to optional:
 - **Text type** – Session ID
 - **Windows Client** – Client
 - **User** – User
 - e. Drag and drop the **Script** shape and add one of the following scripts:

```
My.PageVariables.SessionID = My.PageVariables.client.[Get Sessions For Client]()
```

```
My.PageVariables.SessionID = My.PageVariables.user.[Get Sessions For User]()
```

- f. Drag and drop the **Link** shape and then link it to the Permission Aware Report response plan. Complete the response plan by adding a **Finish** shape.
 - g. Assign the newly created GUI to a display area, for example, **System Left** by dragging and dropping it to the display area. The newly created GUI appears in the display area.
6. Click the **Run Report** button. A new file for the Permissions based Alarms report is created in the folder that was defined in the Permissions based Alarms Report response plan > Creation Folder field. The title of the report depends on the name provided in the **Report Label** field.

Everbridge recommends to moving all the files relevant to Permission-Aware reporting to a separate folder for ease of access.

7. Double-click and open the report. The report displays all alarms that are visible to the Admin user.

Alarm Details

ID	Alarm Type
30	Intruder Alarm
31	Fire Alarm
32	Fire Alarm
33	Fire Alarm
34	Intruder Alarm
35	Intruder Alarm
36	Fire Alarm
37	Fire Alarm
38	Fire Alarm
39	Fire Alarm
40	Intruder Alarm
41	Intruder Alarm
42	Fire Alarm
43	Fire Alarm

8. To view an Alarms report for a specific user (in this case, CNL User) similar to Dynamic Permissions functionality, follow these steps:
 - a. Create an Alarm Stack View for the CNL Users' Group and make sure only alarms that are relevant to the CNL User are visible.
 - b. In the **Users > CNL User > Properties > Member of** dialog, remove membership of one of the other user groups.
 - c. Raise an alarm, for example, using the device change state type.
 - d. Navigate to the second Windows Client.
 - e. Ensure that the alarms are visible in the **Alarm Stack View**.
 - f. Go back to the main client and delete the Permissions based report.

- g. Click the **Generate Report** button and view the newly created report. Notice only Alarm details relevant to CNL user are displayed.

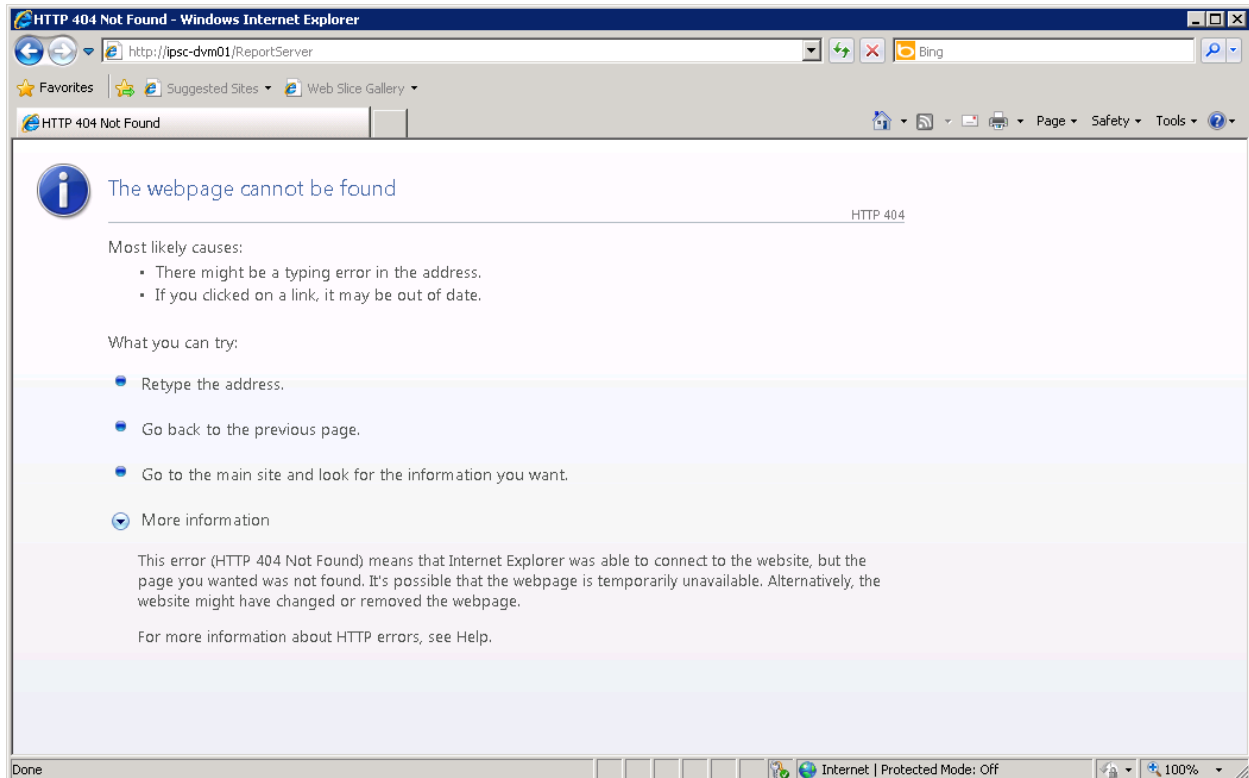
Alarm Details

ID	Alarm Type
31	Fire Alarm
33	Fire Alarm
37	Fire Alarm
38	Fire Alarm
42	Fire Alarm
43	Fire Alarm

Troubleshooting SSRS Reports

Report Server Unavailable on Host Machine

The report server webpage fails to show on the host machine after the configuration of SQL Server Reporting Services and the “webpage cannot be found” message is displayed.

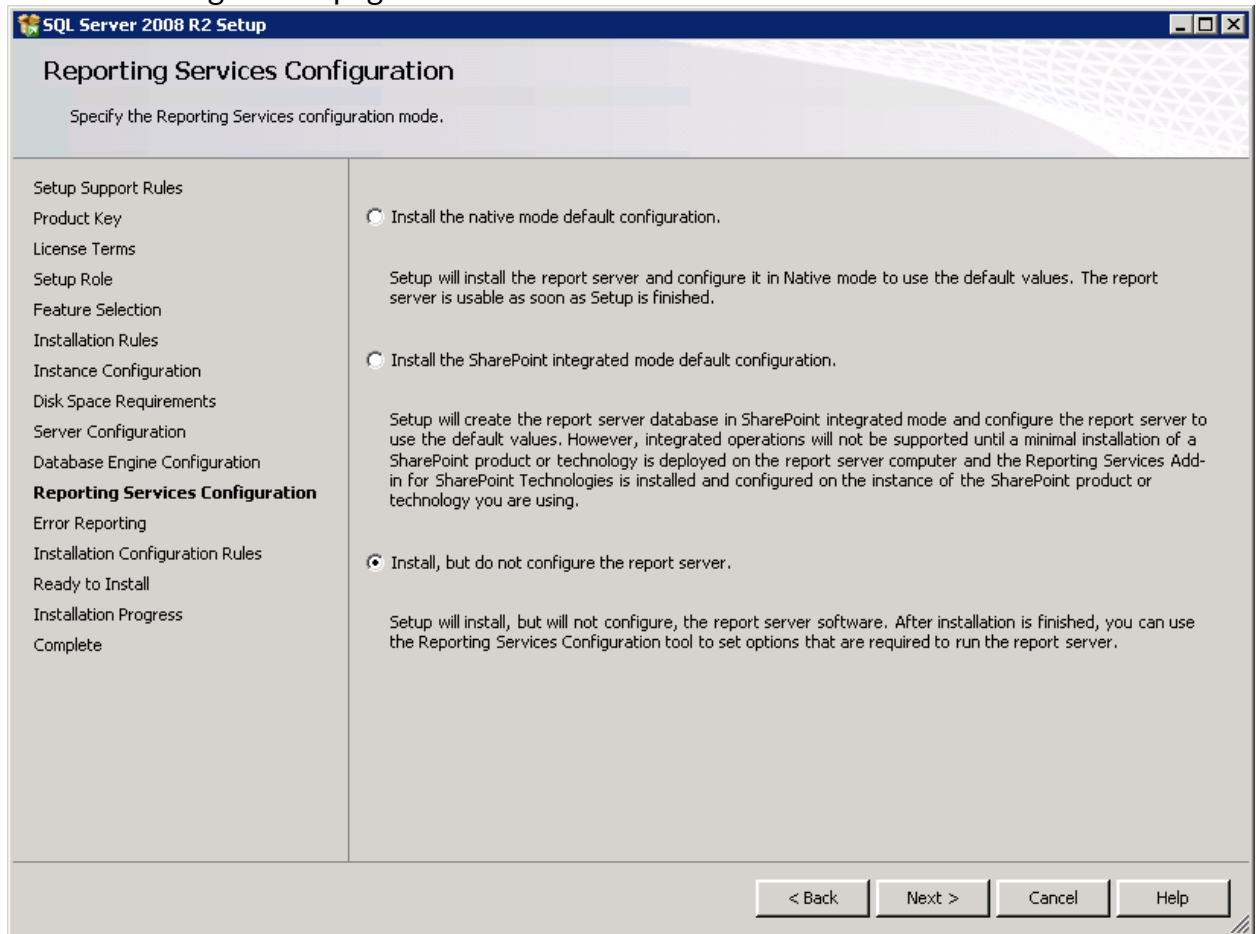


The installation of SQL Reporting Services is incorrect. This can occur if the default configuration is selected for reporting service during the SQL Server installation wizard.

To fix this issue:

1. Uninstall the Report Services component of the SQL Server installation.
2. Delete the ReportServer and ReportServerTempDB databases.
3. Re-run the SQL Server installer and select the Report Services component.

- Select the Install, but do not configure the report server option on the Reporting Services Configuration page.



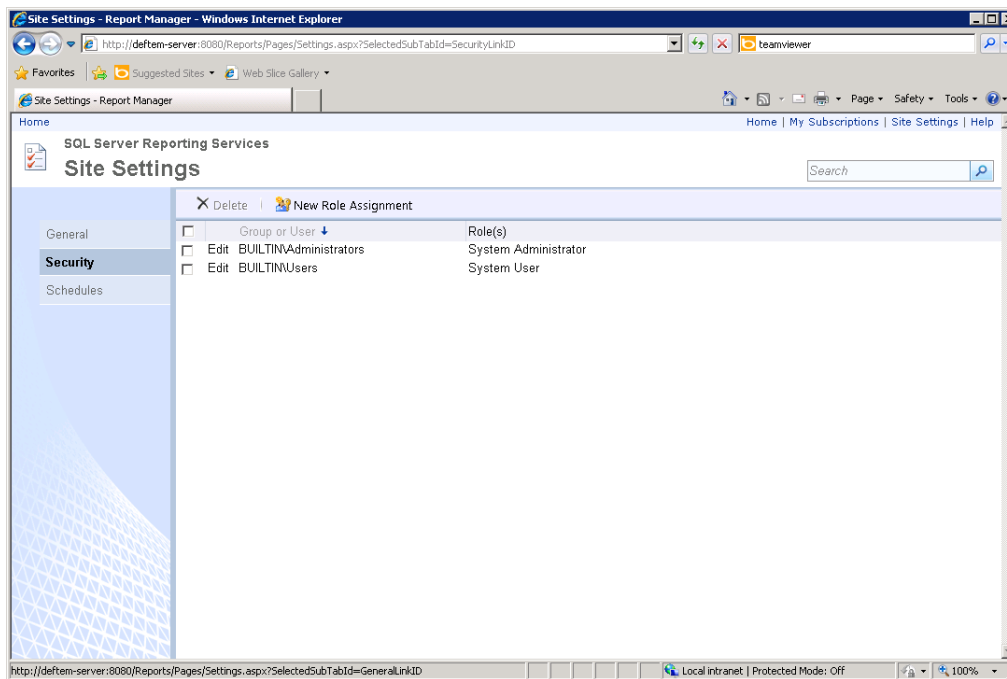
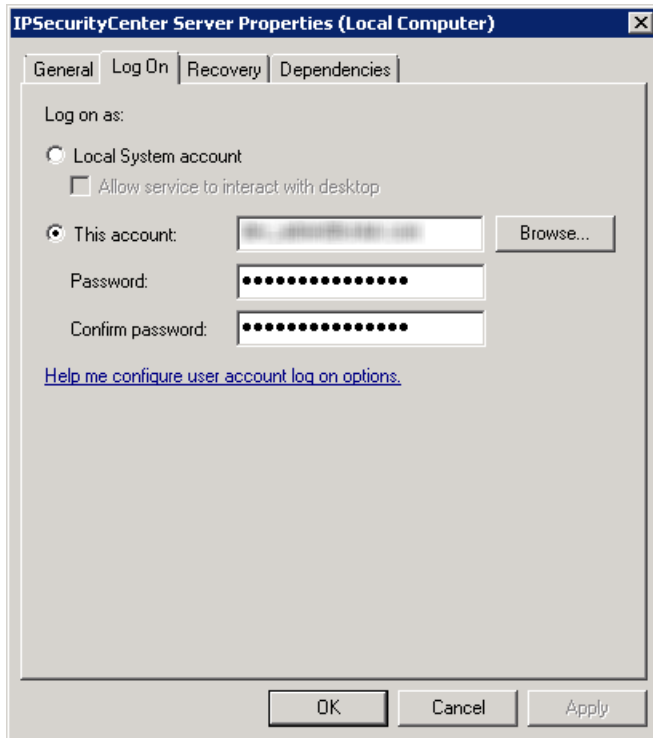
Permission Denied by SQL Report Server

When attempting to test the SQL Reporting the connection fails with the message **Permission was denied by report server.**

This message appears if the account under which the Control Center Server service is running does not have administrative privileges in either Windows or SQL Reporting.

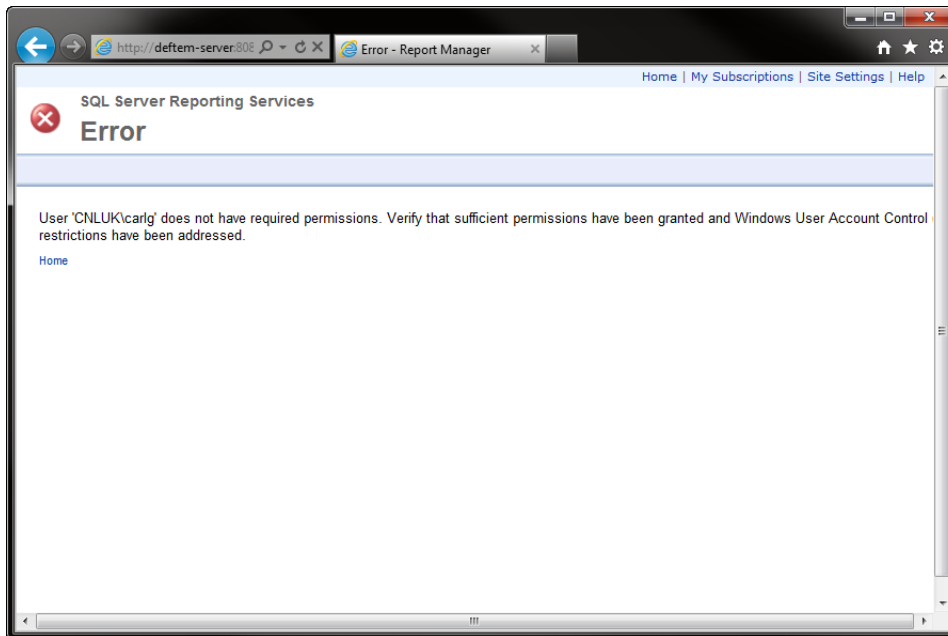
To fix this problem, set the Control Center Server service to log on as an account with administrative privileges or as an account that has sufficient permissions in SQL Reporting.

Uninstalling and reinstalling Control Center automatically resets this.



User Does Not have Required Permissions For SSRS

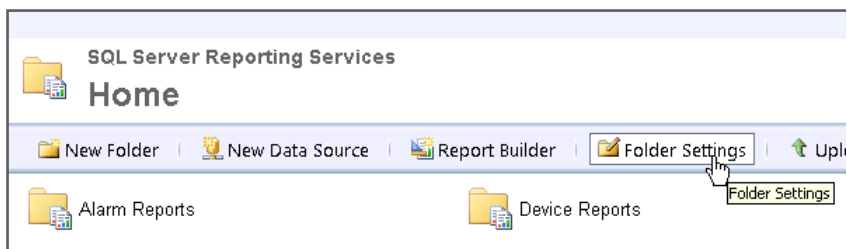
When navigating to the report homepage from a remote workstation, an error message is shown stating that the user does not have required permissions.



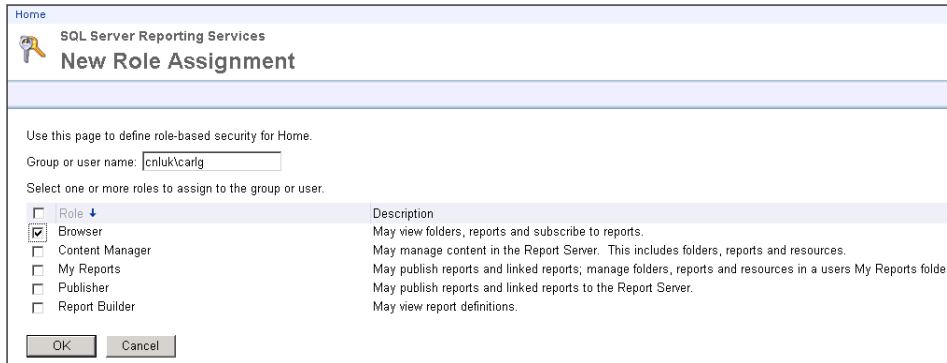
This error occurs when the currently logged in user does not have permission to view the contents of the report server.

To fix this issue:

1. Update the Report Server to provide the user with permission to view the contents of the folder.
2. Click **Folder Settings** on the Report Server home page toolbar.

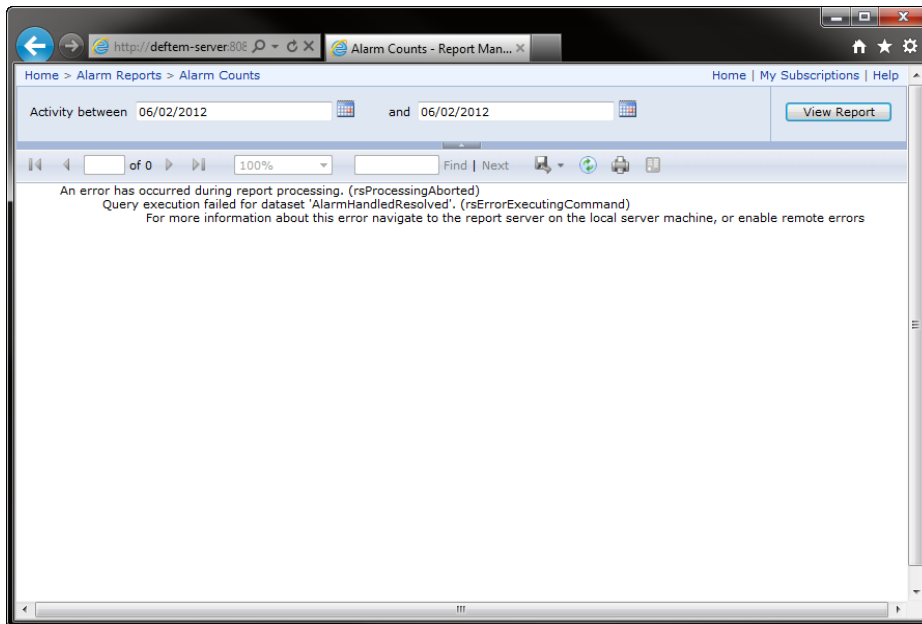


3. Create a new role assignment for the required user and select **Browser** to provide access to folders and reports only.



SSRS Report Fails to Show

When attempting to view a report, an error message is shown stating that an error occurred during report processing.



This error occurs if the currently logged in user does not have permission to access the underlying data source.

Workaround:

Configure the data source to store the connection credentials in the Report Server instead of using the Windows integrated security.

To change connection details:

1. Click the data source to edit the properties.
2. Under **Connect using**, select **Credentials** stored securely in the report server.
3. Enter a valid username and password.
4. Select the **Use as Windows** credentials when connecting to the data source.

5. Click **Test Connection** and then click **Apply** if the connection is created successfully.

CONTROL CENTER Administrator Interface \ Configuration Authorisation \ Status					
Configuration Authorisation					
Full Text Search					
	Description	Requested User	Requested Date	Requested Client	Status
	Add Test user	Limited Admin User	12/12/2018 2:16:05 PM	DEVnetClient174.CNLUKDE	Pending
	Add djokdj	Limited Admin User	12/12/2018 1:31:32 PM	DEVnetClient174.CNLUKDE	Pending
	Open System Configuration DEVnetClient174	Limited Admin User	12/11/2018 12:08:17 PM	DEVnetClient174.CNLUKDE	Rejected
	Open System Configuration DEVnetClient174	Limited Admin User	12/11/2018 11:41:31 AM	DEVnetClient174.CNLUKDE	Rejected
	Add test user	Limited Admin User	12/11/2018 10:59:42 AM	DEVnetClient174.CNLUKDE	Approved

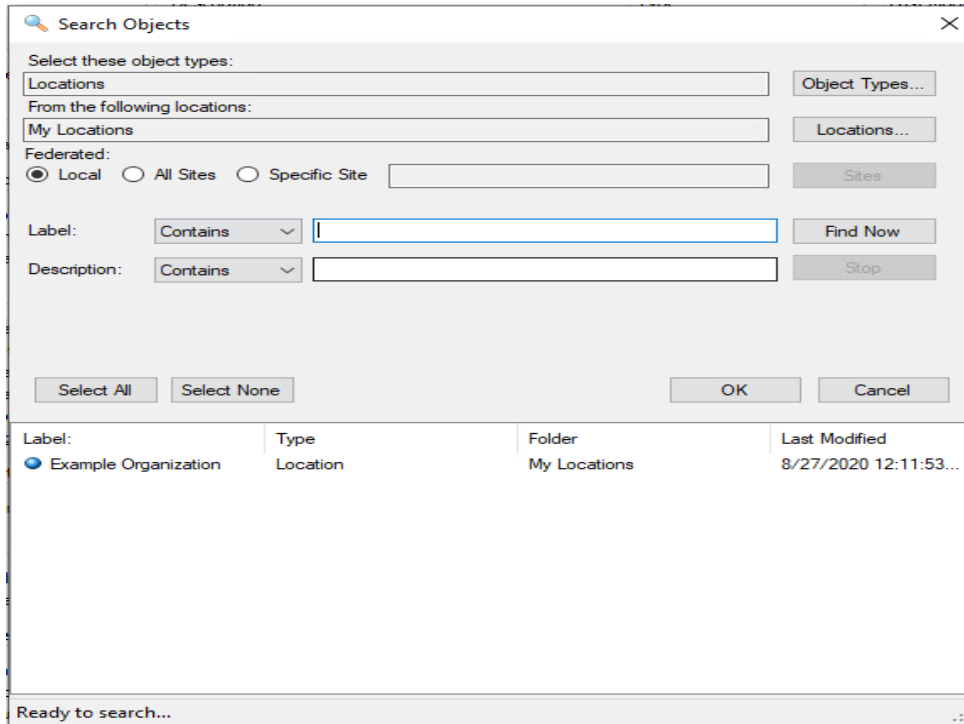
Locations

Configuring a Location to Appear as Base Location

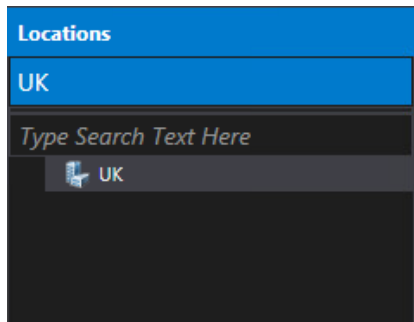
You can configure a location of your choice to appear as a base location in the System Explorer GUI.

To configure a location to appear as base location:

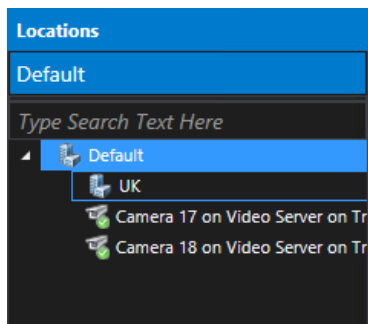
1. From **System Objects**, open **System Explorer** and edit Locations by selecting the Base Locations property. The following dialog appears:



2. Leave the default option **Local** selected and click **Find Now**. The available locations are displayed.
3. Select the location you want to display as the base location and click **OK**.
4. In the following figure, the site **UK** is configured as the base location.



5. Selecting **Default** as the base location would display the locations and devices underneath the **Default** folder.



Mapping

Control Center revolves around locations and maps. Maps can be used to illustrate to users where both static and moving assets are located.

GIS (Geographic Information System) in Control Center allows for maps and data to be shown to the user for locations setup in the solution. Control Center allows for two different types of maps to be used; schematics and geographic.

A schematic map typically consists of a raster image, such as floor plans, CAD files, or big image imports, whereas a geographic map is typically a more interactive map such as WMS/WMTS map.

The mapping capabilities in Control Center are such that different maps and different data layers can be easily consumed and combined to provide a rich mapping experience. The following sections describe the steps to configure maps in Control Center.

Mapping Prerequisites

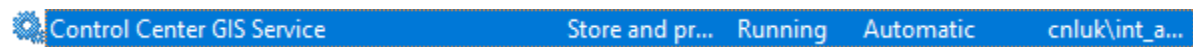
Before any maps can be added into Control Center, you must first source them. For schematics, this simply involves identifying the images which are to be used and importing them if necessary. For geographic maps, different map sources must be identified, for example, this may include a WMS path to a mapping server.

Suitable network connectivity must be available based on the maps used. Map sources such as Google Maps and OSM will require an internet connection. If a mapping server is

available on the local network, then suitable network connectivity must be in place between the mapping server and all Control Center servers/clients.

GIS Server Architecture

The Control Center server installer includes an option for a GIS Service. When selected, the Control Center GIS Service is created along with a corresponding database called Atlantic. The Atlantic database is used to hold spatial data and is complementary to the pacific database.



Layers and Scenes

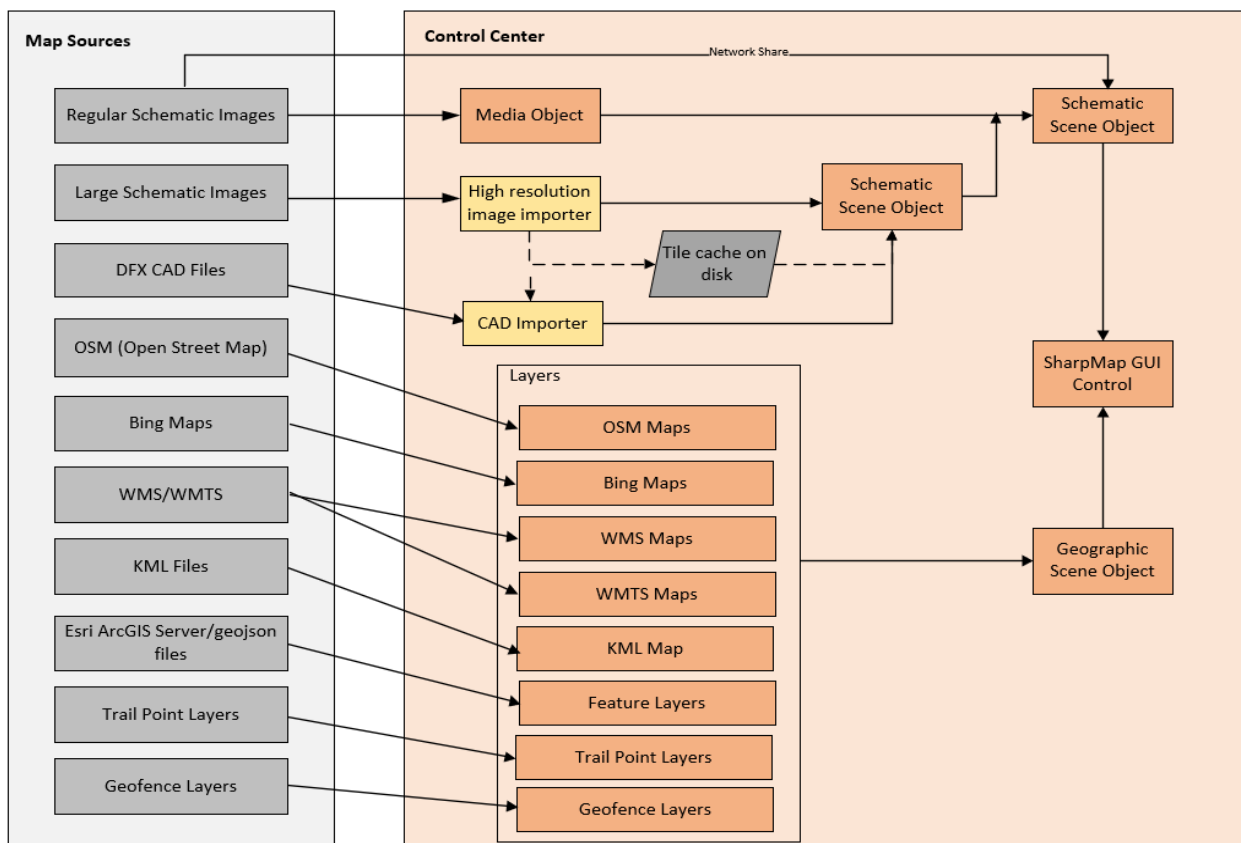
The configuration of maps in Control Center consists of several objects which link together to provide a complete solution.

Supported GIS Sources

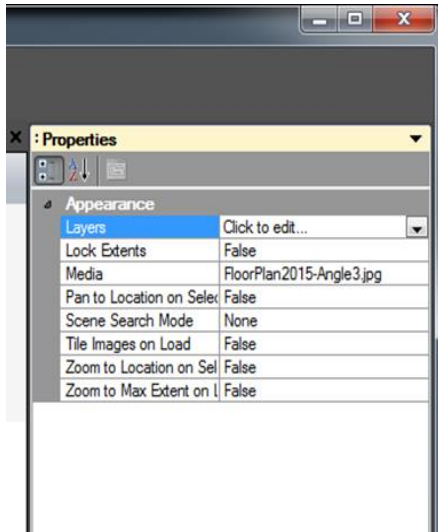
Source / Version	Formats	Limitations/Notes
OSM		Requires 3 rd party license
Bing Maps Road & Aerial		GIS Module includes up to 100,000 API requests annually. Requires online connection to Bing.
WMS 1.0.0, 1.1.0, 1.1.1, 1.3.0	EPSG:3857, EPSG:4326	
WMTS 1.0.0	EPSG: 3857 and 900913	
KML		Static. Basic annotation. Base layer from other source required. Supports Point, Lin, Polygon.
Trail Point		Requires Geo-aware Assets or Events

Geofence		Requires Geofence capable Connectors
Feature GeoJSON	ESRI ArcGIS Feature Layer	Limitations to number of concurrent features and refresh rates apply

The diagram below shows the different components involved in taking an external map source and making it available in Control Center within a GUI.



The locations required in the solution and the source of the maps will determine the Control Center objects required. Typically, only one GUI containing the SharpMap GUI Control will be required in a solution as this will accept a location and then show the corresponding scene. For more information, see [Configuring Visibility Range, Zoom Levels and Clustering](#).



Therefore, each location must be associated with a geographic scene or schematic scene. A scene can be used by more than one location which is particularly useful when working with Geographic scenes.

The following sections describe how to add and configure each component in the solution based on the Sample Locations Configuration section in Appendix.

A default GIS layer for Open Street Map is created when Control Center is installed.

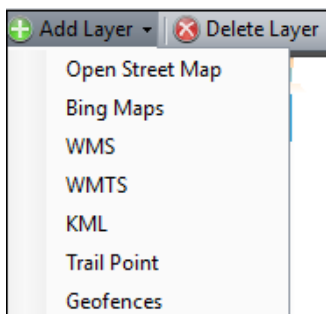
The map automatically filters out the visual effects of any alarms that are not visible to the user. You can also apply alert states to parent Location Types to highlight the affected site of an alarm to the user.

Configuring GIS Map Layers

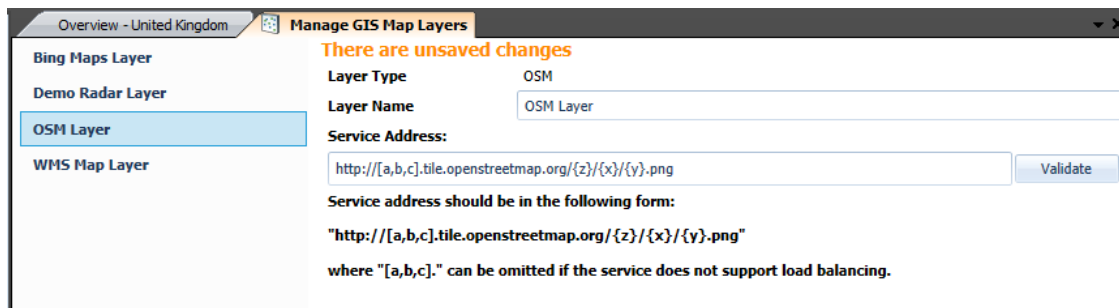
You must configure the GIS layers in a Control Center solution before creating geographic scenes for locations.

To add a GIS Map Layer:

1. In **System Configuration > Toolbar**, click **GIS Layer Manager**.
2. Click the **Add Layer** button on the toolbar and then click the required layer, for example, **OpenStreetMap** (OSM Maps).



3. A new layer is added to the list of layers on the left of the editor. Selecting a layer will show the properties of the layer on the right.



4. Click **Save** and then exit the editor.

When adding an OSM Map Layer, use the following format for the Service Address:

```
http[s]://[a,b,c].tile.openstreetmap.org/{z}/{x}/{y}.png
```

Where "[a,b,c]" can be omitted if the service does not support load balancing. When a map tile is requested, {z}, {x} and {y} will be replaced by numbers representing the current zoom level, x-tile number and y-tile number respectively. For more details, see the [Wiki for OSM](#).

If the Service Address is left blank, then the default OSM server will be used.

To delete a GIS Map Layer:

1. In **System Configuration > Toolbar**, click **GIS Layer Manager**.
2. Select the required layer and click **Delete Layer** on the toolbar. The selected layer is deleted.

Adding WMTS and WMS Layers

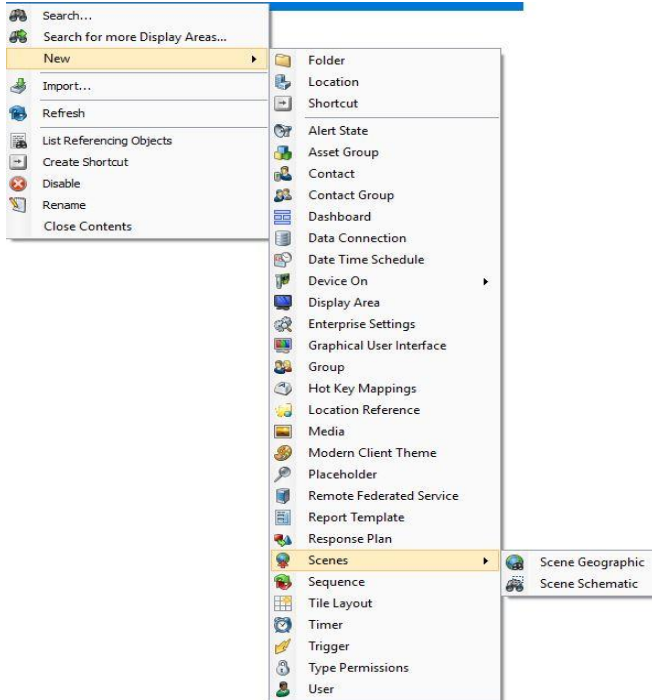
Using the GIS Layer Manager, you can configure both WMTS and WMS layers for use on geographic maps. In Control Center, WMTS and WMS layers can be used as both map background and overlay layers. For basic understanding on what WMTS and WMS are used for, refer to [Wikipedia](#).

To configure a WMS/WMTS Layer:

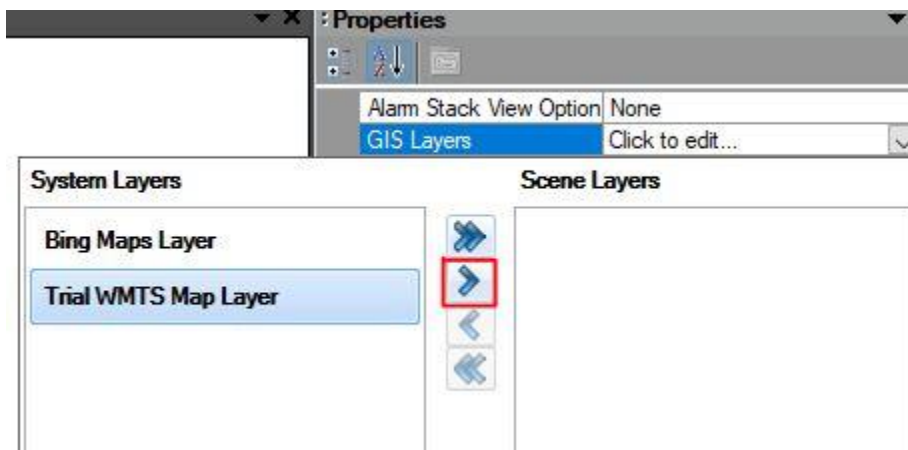
1. Select the **GIS Layer Manager** on the Main toolbar. Manage **GIS Map Layers** Window opens up.
2. Click the **Add Layer > WMS / WMTS** option. The **WMS / WMTS Layer** is added to the list of layers on the left of the editor.
3. Configure the following settings and click **Go**.
 - **Layer Type** – Displays the layer type depending on your selection, for example, WMS or WMTS.
 - **Layer Name** – Type a name for the layer.

- **Is Base Layer** – Select whether you want the selected layer to be a base layer or not.
- **Layer Background** – Optionally select a specific color to use as the layer background for base layers. If not entered, the background color will be derived from the Control Center client theme.
- **Version**– Select the version of the layer from the drop-down list. Currently, only 1.0.0 of the WMTS standard is supported for the modern client. For WMS layer, we support 1.0.0, 1.1.0, 1.1.1 and 1.3.0 versions.
- *(Applies to WMS Layers Only)* **Enable Tile Caching** - Select if you want to enable tile caching. The tile caching options are displayed.
 - From the **Tile Caching Type** drop-down list, select:
 - **Memory** - By default, memory is selected as access to memory is faster than to your file system. However, when a Control Center client is closed, the cache is cleared and so must be repopulated on first load of the map tiles.
 - **FileSystem** - select if you want to cache your maps in the file system. Although access to your file system is slower, the cache is persisted when a Control Center client closes or a machine is restarted, and more space is available for the tile cache.
 - **Max Cache Size (MB)** - By default, this is set to 1000. Selecting the arrows you to change the maximum allowed size of the cache.
- **Address**– Type the URL address of the mapping data source for WMTS / WMS. This URL must be accessible from both the GIS Windows Service and the Control Center Windows Client. We support both http and https URL addresses.

- Once the **Address** entered is established, a list of layers supported by that particular map source is displayed. You are allowed to choose only one layer as the background layer for the WMTS and multiple layers for WMS setting.
 - Enter the **Authentication** token provided by the map source provider, if applicable.
 - Select the relevant EPSG from the list which provides a projected coordinate system used for rendering the map. The most common ones used are EPSG:3857 and EPSG: 4326 for WMS and EPSG: 3857 and 900913 for WMTS.
4. Click **SAVE** to save the configuration settings.
 5. Go to **System Objects** and create a new **Scene Geographic Object** by right clicking on an empty space > **New** > **Scenes** > **Scene Geographic**.



6. Double-click on the object to edit it. The **Scenic Geographic** editor opens up.
7. From the **Properties** window on the right, click on **GIS layers** and choose the object you created from the list and move it to the Scenic Layers box.



8. Save the settings to view the Map projection from the source selected.

Adding a Trail Point Layer

The Trail Point Layer enables you to configure how geo-aware objects are displayed on a map surface in Control Center, whether schematic or geographic.

Control Center supports two types of geo-aware objects:

- **Geo-aware devices** – Control Center objects which send events showing their current location.
- **Detected geo-aware objects** – Objects that appear on the map when detected by a device, for example, radar, sonar, analytics camera.


Layer configuration settings enable you to define the appearance of the trail. For a geo-aware device, the icon representing the current position will be the device icon. For a detected object the icon can be configured in this layer.

If the displayed object is associated with an alarm, and the alarm has an alert state associated with it, then the object will use the alert icon and the trail will change to use the alert color.

Before configuring Trail Paths, ensure the following prerequisites are met.

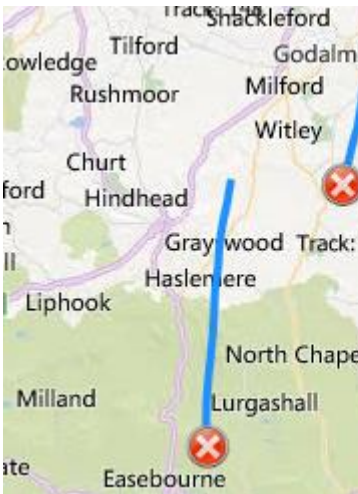
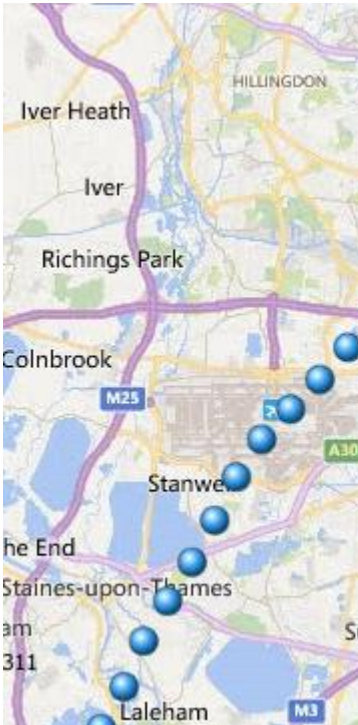
- Install a connector that can generate events representing the changing location of an object, for example, a Radar or Sonar connector and a connector that supports trails for devices. In the following example, Everbridge's internal Demo Radar connector has been used for the GIS Trail Point layer and the 2D Track Simulator connector for the Schematic Trail Paths.
- Once the connectors are installed, you must add the required device and enable it from System Configuration.



To configure a Trail Points Layer:

1. In **System Configuration > Toolbar**, click  **GIS Layer Manager**.
2. Click the **Add Layer > Trail Point** option. The **Trail Points Layer** is added to the list of layers on the left of the editor.
3. Configure the following settings and save the changes to the layer.

Layer Details:	
Layer Type	By default, this is set to TrailPoints. This is a non-editable field.
Layer Name	The name of the trail point layer. Rename it to a meaningful title for the kind of objects whose trails are to be displayed.
Device:	


Device Type	Select a Device Type for the trail path that can generate position-aware events.
Event	Select an event for the selected device type, for example, TraceUpdated for GIS and Position Changed for Schematic. Only geo-aware events are available for selection.
Devices to Track	When checked, all Geo-aware devices are selected. If not, the available trackable devices for the connector appear for you to select individually.
Only show tracks in alarm	When checked, only tracks that have alarms associated with them are displayed.
Style:	
Trail Color	The color of the trails. By default, this is set to blue.
Heading Color	The color of the header trail. By default, this is set to red.
Trail selection color	The color of the trail when hovered over or selected.

<p>Show Trails as Discrete Points</p>	<p>By default, trails are displayed as lines.</p>  <p>Select this if you want your trail to be displayed as discrete points rather than a line.</p> 
<p>Trail Width</p>	<p>The width of the trail, for example, thin,</p>

	<p>medium, wide. By Default, this is set to Medium.</p>
<p>Icon</p>	<p>The icon configured for a trail object. Click the  button to open the Icon Picker dialog. If no icon is selected, a red cross will be displayed.</p> <p>If an Alarm is configured, and the scene has been configured such that alarms should be displayed on the map, the Alarm icon will take precedence over the icon selected here.</p> <p>Note: This icon is only relevant for detected objects and not for geo-aware devices.</p>
<p>Stale Icon</p>	<p>The icon configured for a stale track. Click the  button to open the Icon Picker dialog. If no icon is selected, a red cross will be displayed.</p> <p>A stale track is one that has no new trail points coming in within the stale period configured in Time to go stale field.</p> <p>The trail disappears once both Geo-aware devices and detected geo-aware objects</p>

	<p>become stale. However, for a detected geo-aware object, the icon will also disappear unless it is associated with an alarm which has not been resolved.</p>
Label	
Override Track Label	<p>When selected, the label defined in the script field will replace the original label.</p> <p>The script is a sub-set of VB script and only allows the '+' and '&' operators for string concatenation. The My namespace includes Event which contains properties available to the event that has been selected. For example, Track ID, Trace, Device ID, Date and so on.</p>
Hide Label	<p>When selected, the script field will be disabled, and no track label will appear on trail paths on the end-user map surface.</p>
Override Alarm Label	<p>When selected, the label defined in the script field will replace the original alarm description as configured in the Alarm</p>

	<p>Types dialog for the alarm.</p> <p>Note: The script is a sub-set of VBScript and only allows the '+' and '&' operators for string concatenation. The My namespace contains three sub namespaces, AlarmType, AlarmPoint, and Event which contains relevant properties for each of them.</p> <p>The default description is a copy of the Alarm Type label. The script is run once on initial alarm creation and not run again.</p>
Hide Label	<p>When selected, the script field will be disabled, and no alarm label will appear on trail paths on the end-user map surface.</p>
Label Size	<p>Size of the label. By default, it is set to 12.</p>
Label Font	<p>Font type for the Label description appearing on the map</p>
Label Text Bold	<p>If checked, the label text will appear in bold on the map</p>
Label Text Color	<p>Color of the label Text</p>

Label Background Color	Color of the text background
Label background Opacity	By default, it is set to 0.00 which means the label background will not be present
Label Halo Color	The halo color is the outline to the label text
Lifetime:	
Maximum age (in Seconds)	Determines the maximum age of trail points to be displayed. Older trail points will not be displayed.
Maximum trail points	Represents the maximum number of trail points for any displayed trail appear on the end-user map surface.
Time to go stale (in Seconds)	Determines the time (in seconds) after which the track should go stale. By default, this is set to 60 seconds.
Classifications:	
	Buttons used to Add a new Classification or Delete an existing one. By default, three classifications are created; Friend, Foe and Unknown. These classifications are only

	applicable for Radar track objects.
--	-------------------------------------

Notes:

- To delete a trail point layer, in the **GIS Layer Manager**, select the **Trail Point** layer and click the **Delete Layer** button on the toolbar.
- In federated environment, if a trail point layer is published to an older Control Center version, the published scene will not include any classification data.

Adding Geofences Layer


A Geofence is a virtual perimeter of the actual geographic boundary, drawn on the map that enables the application to trigger an event when an object enters or leaves a particular area. Geofences can be predefined on a map in a connected subsystem that can then be imported to be used within the Control Center.

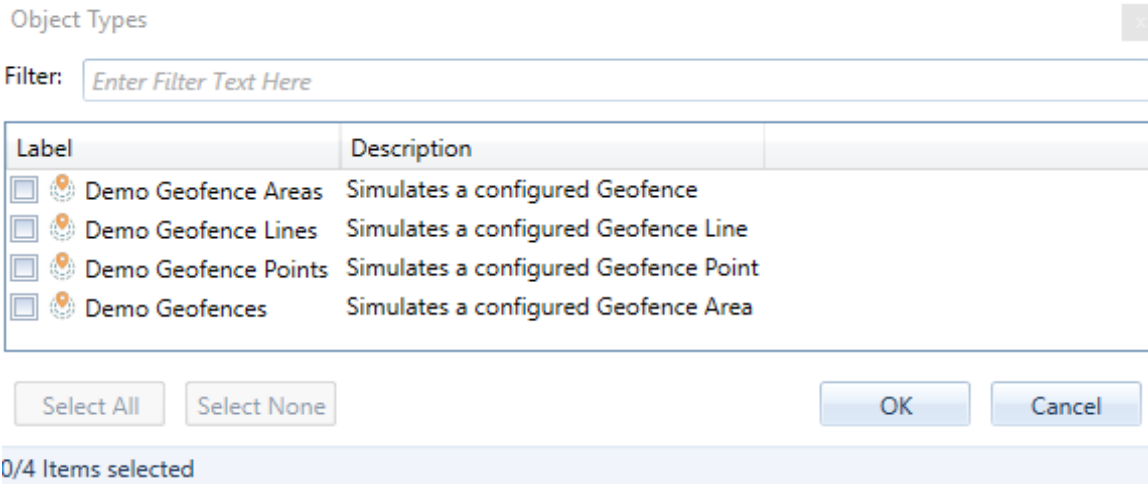
Currently Geofences cannot be created within Control Center and hence need to be imported from any subsystem monitoring the Radar information and then displayed in Control Center during commissioning.

The Geofence can be of three Types/Shapes and needs a separate map layer to be created for each type. More than one layer can also be created for each type. The three types of Geofences available are:

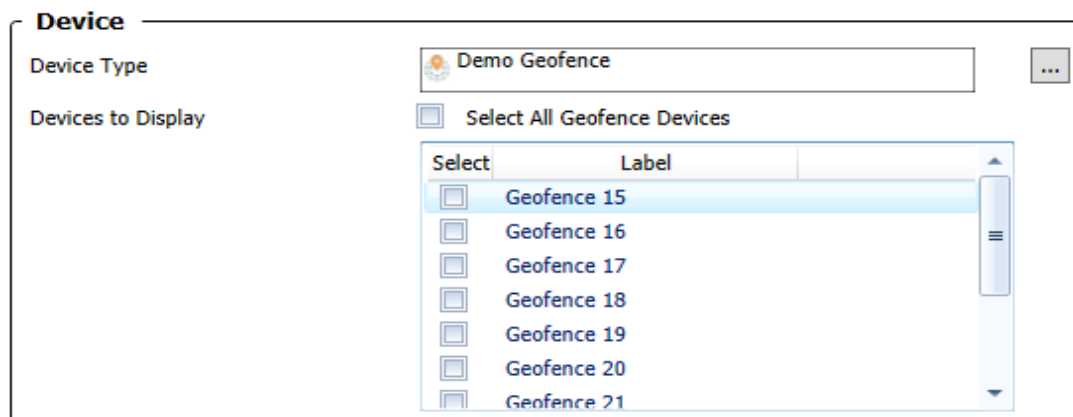
- Geofence Area
- Geofence Line
- Geofence Point

To configure a Geofence Layer, do the following:

1. Go to **System configuration > GIS Layer Manager** on the **Toolbar**.
2. Click on **Add Layer** drop down menu and select **Geofences**. A new Geofence Layer will be created and the properties that can be configured for displaying the Geofences within Control Center are shown.
3. Type in an appropriate **Layer Name** based upon what **Geofence** shape you would be using
4. In the **Devices** section, click on  against the **Device Type** to choose a type of Geofence Device and click **OK**.



5. Select all Geofence devices to be rendered on the map by selecting **Select All Geofence Devices** option or clear it to choose the devices of your choice. The list displayed in the box below will depend on the device type selected above.



6. In the **Style** section, you have the option to display the disabled devices on the map, hide it or keep it transparent so that they stand out from enabled devices. The **Disabled Device Opacity** when set to Zero will completely hide it from the scene and 100% will make it appear just as normal to other devices. Sliding to a number in between will make it transparent to the level selected
7. Save the Geofences Layer.

When you publish GIS Layer Manager in a federated environment, the Geofence layer will be blocked from being published while other layers will still be published with the scene as normal.

Adding a Feature Layer

You can display geographical features from GeoJSON sources, for example, bus stops, stations, metro lines, parking zones, traffic lights, hospitals, shopping, and restaurants, on

your maps. To do this, add a new **Feature** layer in GIS Layer Manager and configure it to use the URL or the path to your GeoJSON file.

For the best performance when rendering features, on both static and dynamic feature layers, in Control Center, Everbridge recommends the following number of features.

Optimum	Recommended	Maximum
6,000	8,000	10,000

The feature layer uses the source layer name and feature ID property name to identify the feature that is used for any Control Center events, for example, any alarms raised for that feature. Therefore, when defining a feature layer, you must:

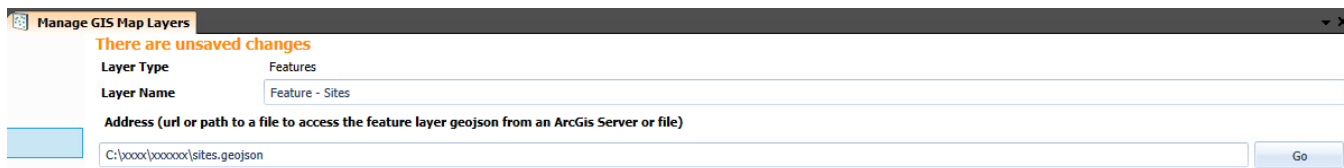
- in **Layer Name**, specify the source layer name.
- in **Feature ID Property Name**, specify a feature ID property name. You only need to select one of the feature IDs, as the feature layer assumes that all features in the source have the same set of properties. The feature ID you select must be unique.

You can also pass the feature ID to third-party applications, which you can configure to display in dashboards when a user clicks a feature, for example. For more information, see [Configuring Map Object Interaction](#).

The feature properties can be configured to display in a tooltip and the feature source can use authentication.

To improve performance, Everbridge recommends that you enable clustering on your map when using feature layers. See [Using Clustering](#).

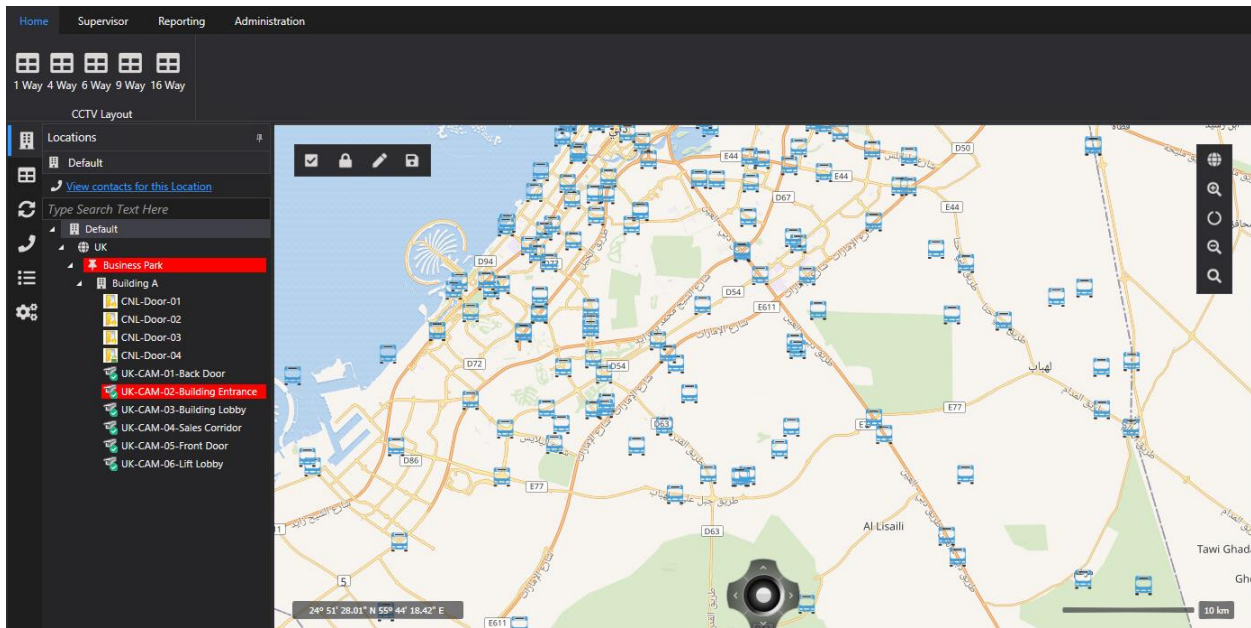
1. Go to **System Configuration > GIS Layer Manager**.
2. Select **Add Layer > Feature**. A new **Feature Layer** displays. In **Layer Name**, type the name of your feature layer.
3. In **Address**, type the URL the path to your GeoJSON file.



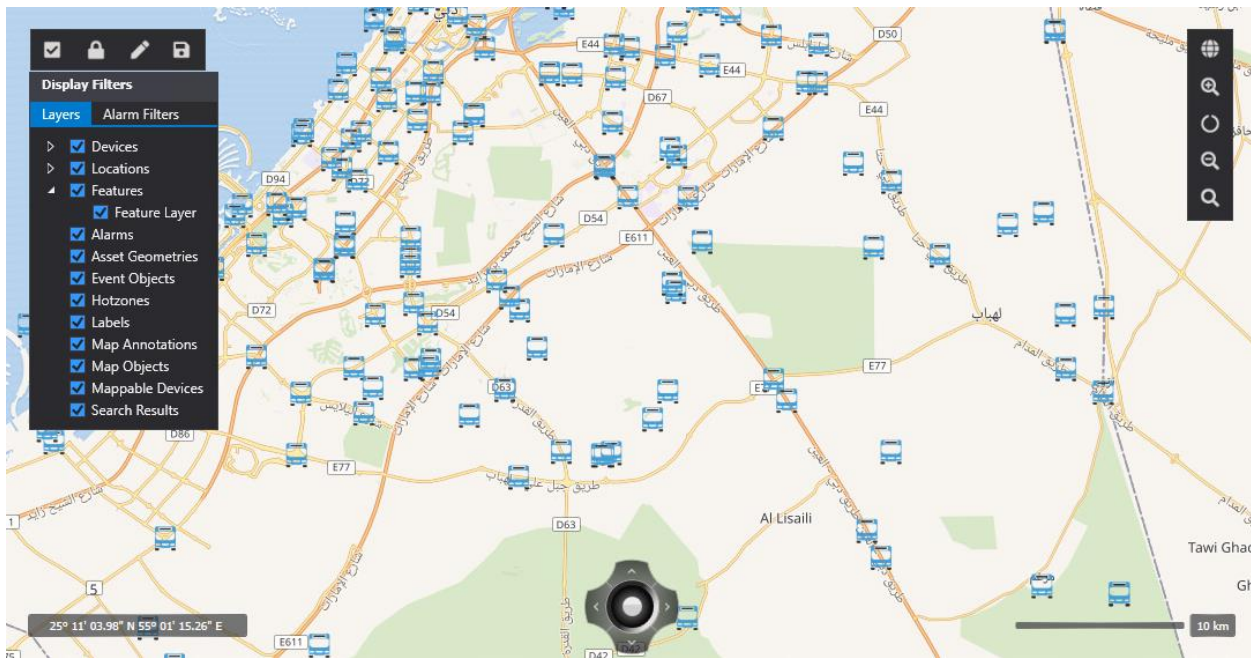
4. Select **Go**. If the source data is available and compatible with Control Center, information about the geographical features is displayed in **Layer Information**. The feature properties are displayed in **Properties**.

	<ul style="list-style-type: none"> ○ RequestIp. This option does not require any additional value as it uses the IP address of the machine performing the request.
--	--

7. Select **Dynamic Layer** if you want Control Center to automatically refresh the data in your GIS feature layer. Use this if your underlying data source changes. The **Polling Interval** specifies how many seconds Control Center waits to refresh the data. By default, the polling interval is 15 seconds but you can change this, depending on your requirements.
8. You can amend the look and feel of your feature layer when it is displayed in a map by clearing **Show feature as icon**. Use the **Line/Area Settings** to amend the look and feel of your feature layer.
 - Line Color
 - Fill Color
 - Icon
 - Icon Size
 - Line width
 - Opacity
9. The **Group Search Results By** dropdown allows you to group individual features together based on a shared property when using Map Search to search for items within a layer. For example, a bus route could be split into multiple sections but share the same route number property. Setting the route number field here would ensure that a search for 'Route 101' returned a single result and not one result for each section.
10. Select **Show Tooltip** if you want information about the feature layer to be displayed in the map. From **Properties**, in **Include in Tooltip**, select the properties that you want displayed in your tooltips for this feature layer.
11. Select **Include in Search** if you want a field to be searchable from the map search box.
12. Once you have defined your feature layer, save your changes and close **GIS Layer Manager**.
13. From System Main, open your map. Your feature layer displays.



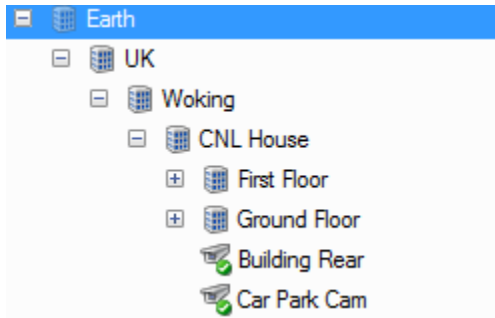
You can filter on feature layers in **Layers** and **Alarm Filter Preferences** from a map.



Sample Locations Configuration

This section details a sample location configuration in Control Center. Note how each location includes either a default Schematic Scene or Geographic Scene.

A zone is used to navigate to the UK location from the Earth location. Icons are used to navigate for other locations.

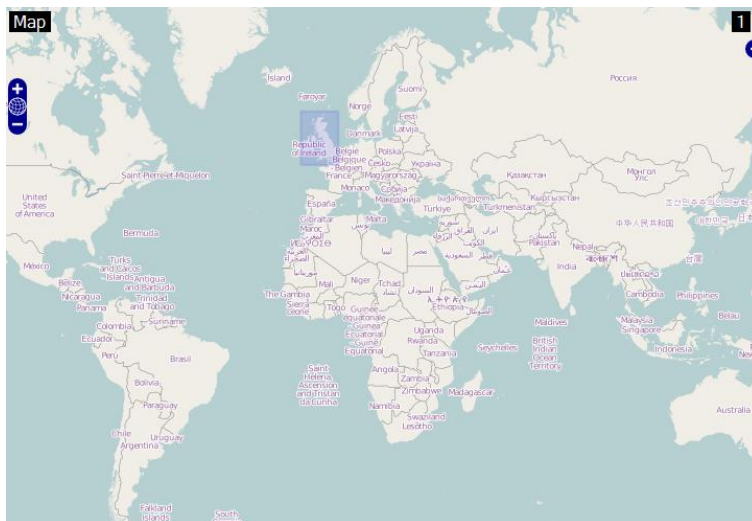


Earth

Contents

UK (Location)

Scene for Location Earth (Scene Geographic)

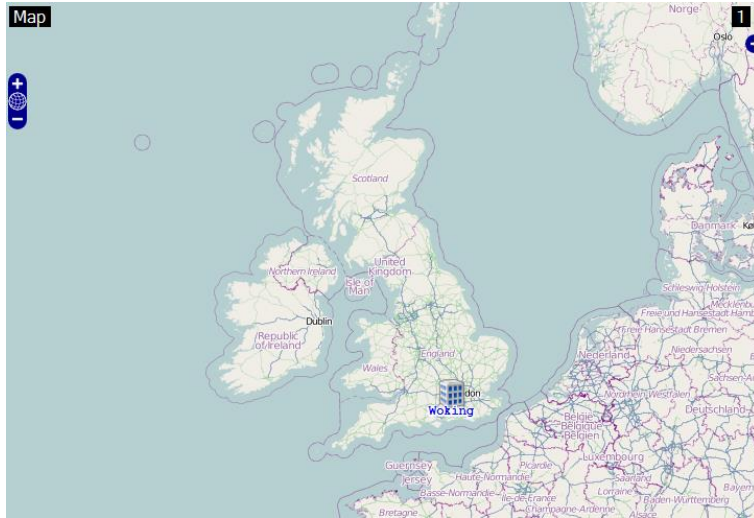


UK

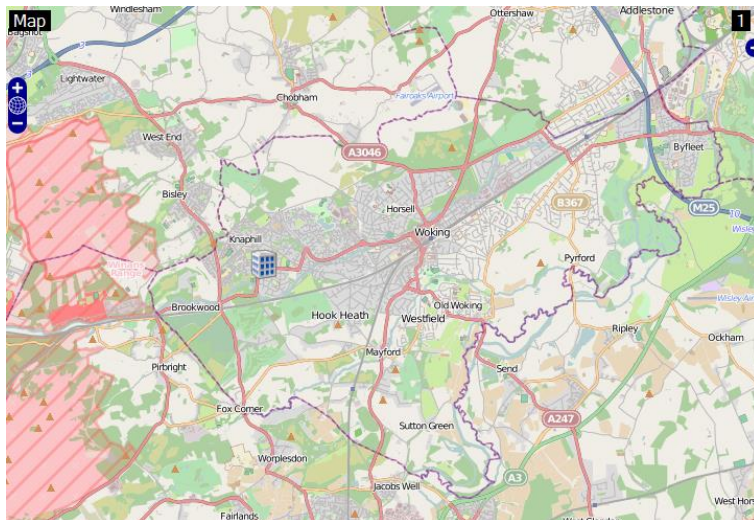
Contents

Woking (Location)

Scene for Location UK (Scene Geographic)



- Woking
- Contents
- CNL House (Location)
- Scene for Location Woking (Scene Geographic)



- CNL House
- Contents
- First Floor (Location)
- Ground Floor (Location)
- Scene for Location CNL House (Scene Schematic)
- Building Rear (Camera)
- Car Park Cam (Camera)



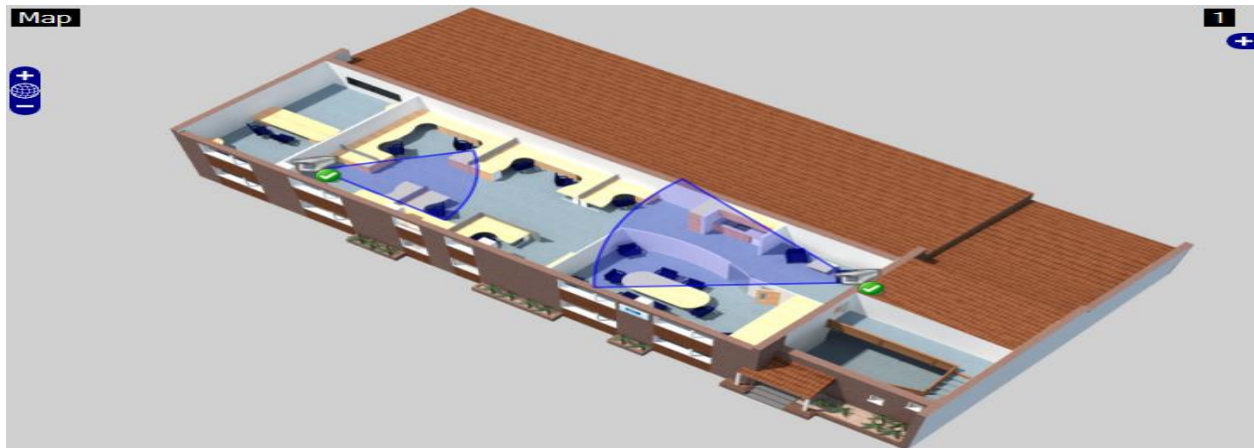
First Floor

Contents

Scene for Location First Floor (Scene Schematic)

Office Cam 6 (Camera)

Office Cam 3 (Camera)



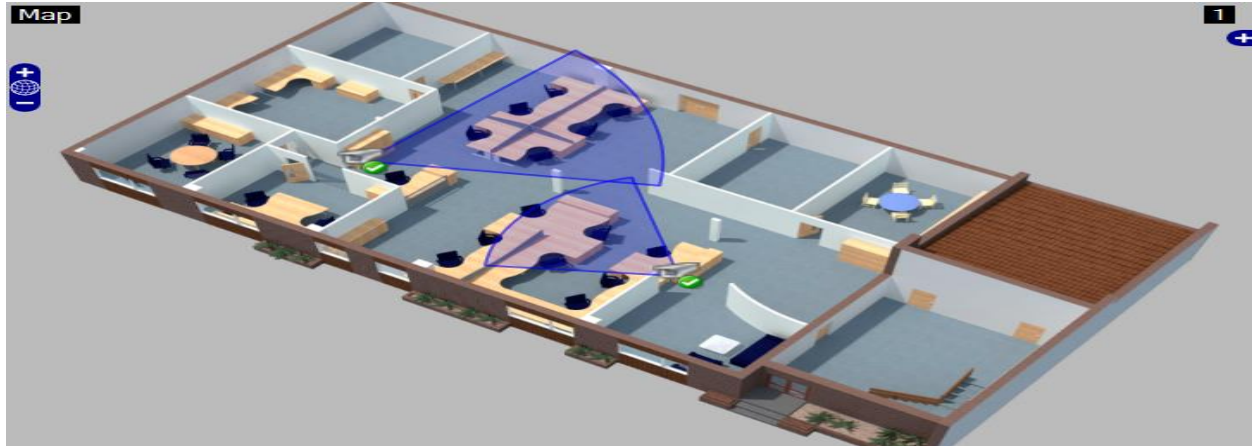
Ground Floor

Contents

Scene for Location Ground Floor (Scene Schematic)

Office Cam 2 (Camera)

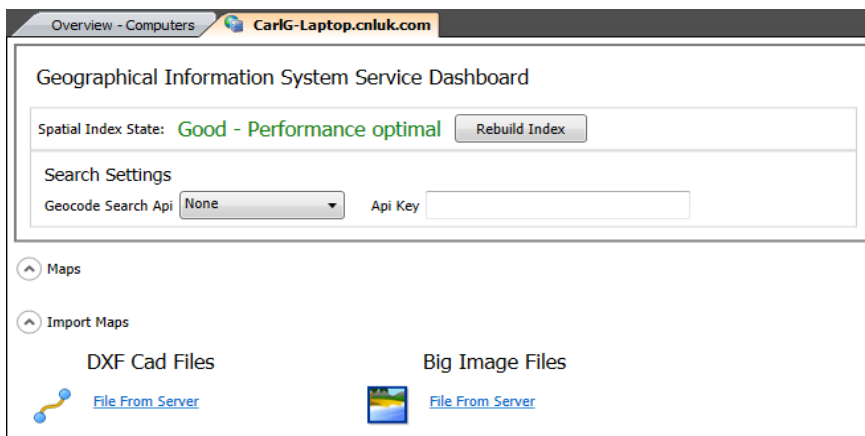
Office Cam 8 (Camera)



Geographic Information Server Manager

The Geographic Information Server Manager provides an interface to view, create, edit, and delete maps in Control Center which require the Geographic Information Service. Currently, these include CAD Files and big images. The CAD importer is used when the source map files are created in CAD. The Big images importer is used when the source images are a very high resolution and/or a large file size. Both map types use a model of tiling images to local disk and presenting to the user only the required tiles based on the selected zoom level and region of the map being viewed. This vastly improves performance and stability when working with large detailed maps.

The Geographic Information Server Manager can be accessed via the Geographic Information Server object by either double-clicking or right-clicking and selecting Geographic Information Server Manager. The Geographic Information Server Manager will then open in a new tab.



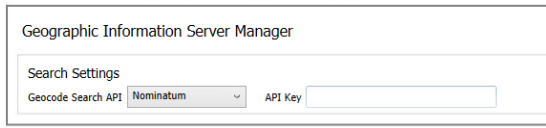
Dashboard Panel

The first section of the Geographic Information Server Manager shows a dashboard area which displays activities on the server (such as caching maps), the spatial index state

(how clean the geographic database is) and settings relevant to the server (such as, which search API to use).

Search Settings

Control Center maps support search by asset names and through connections to online search repositories. The Search Settings are used to specify the online search repository to use. Currently supported repositories are Google and Nominatum. To use an online search repository, select the Search API to use and, if using Google, specify an API key.

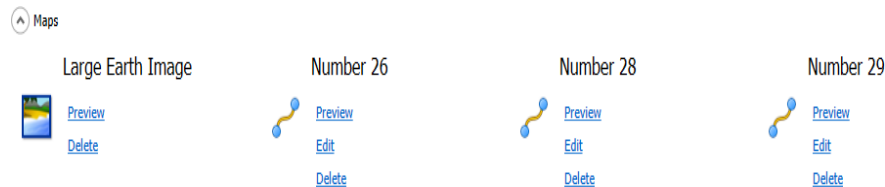


From v5.61 onwards map search is enabled by default for all scenes. To disable map search:

1. Open the **Map GUI** and click on the Design Surface.
2. In the **Property** grid, select **Hide Search Box In Map**
3. Set the property to **True**.
4. Save and close the GUI.

Maps

The Maps section of the Geographic Information Server Manager shows all imported maps. For example, you can preview, edit, and delete any available maps. See the relevant map importer sections for the available options.



About CAD Import

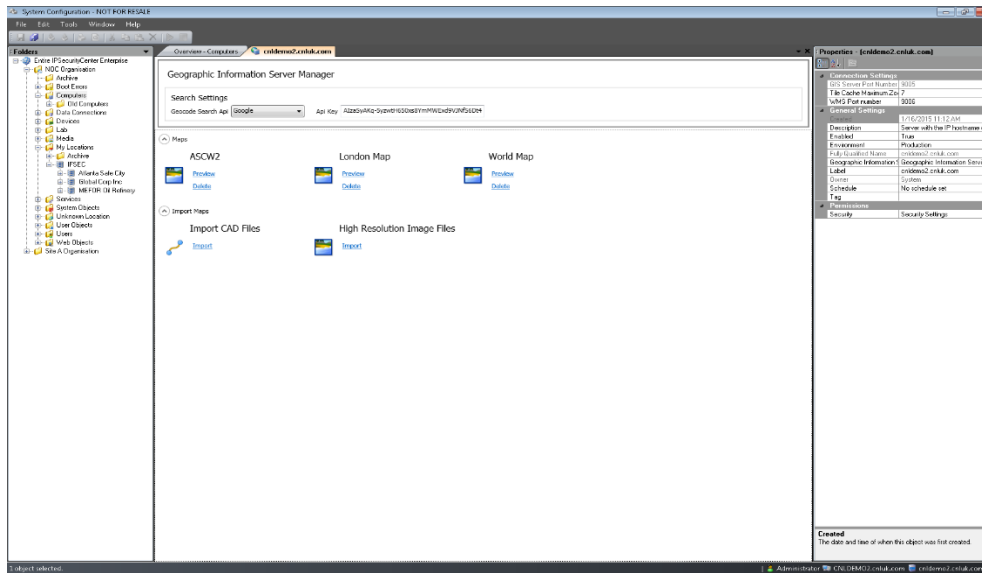
CAD files can be imported into the solution to enable displaying it to the user via a schematic scene. The process works by selecting a CAD file, selecting which layers are required and then importing the map. The import process will import the layers into the solution, so that they can be edited at a later stage, and will also create a tile cache of the map which will be used to display the maps to the end user. Additionally, data within the imported layers can be used to automatically plot Control Center assets onto the map surface.

Importing Drawings

CAD imports are managed in the Geographic Information Server Manager.

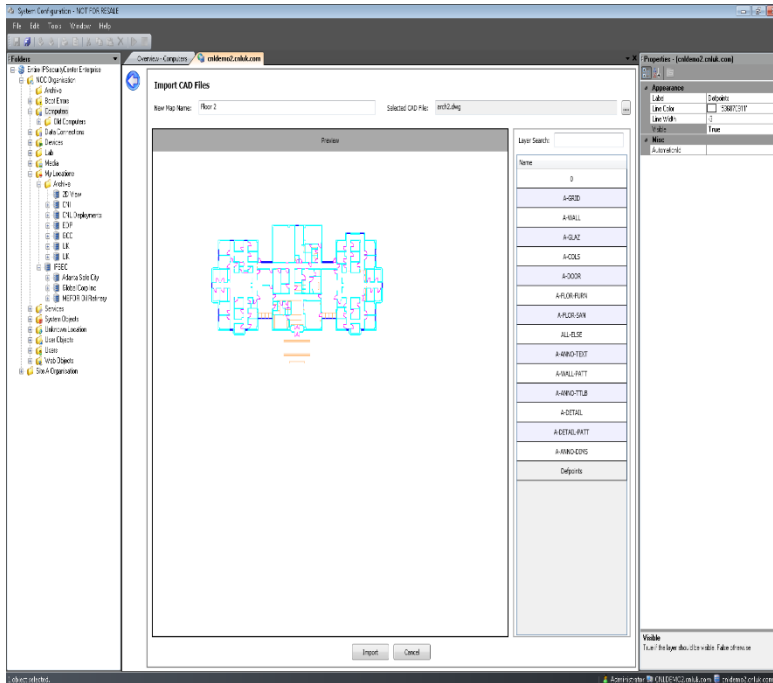
The current major version (10) of CAD .NET supports DWG versions from 2.5 up to latest 2013 inclusive. AutoCAD 2016 does not present a newer DWG format as it utilizes DWG 2013. Support for a next DWG format will be available in future major versions only.

To access the Geographic Information Server Manager, from System Configuration > Computers, double-click and select Geographic Information Server (GISM). The Geographic Information Server Manager will open in a new tab.

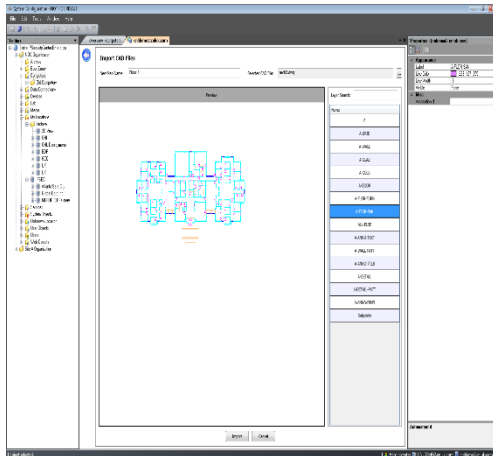


To import a CAD file:

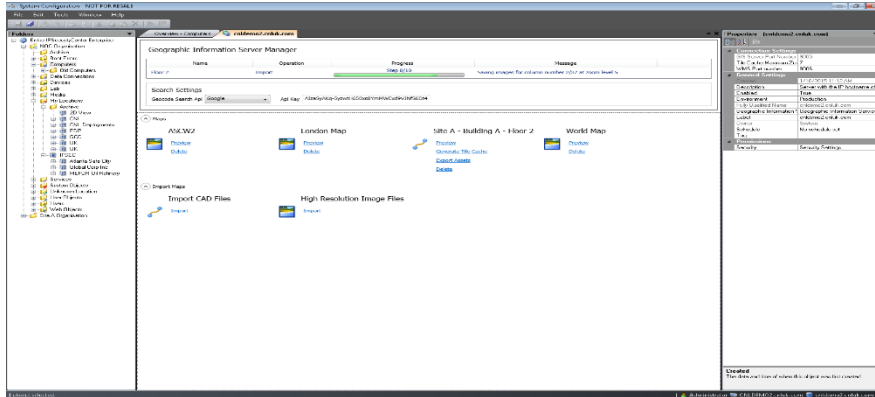
1. Click the **Import CAD Files** button. This will navigate to the CAD File importer.
2. Specify a name and select a file. Currently, CAD Import only supports .dxf and .dwg formats. This will display a preview of the drawing.



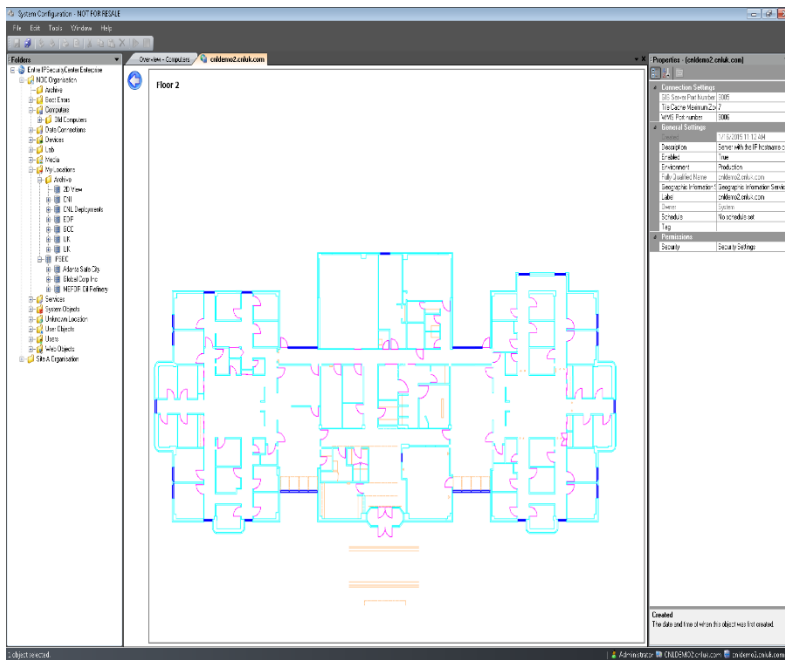
3. Select the layers to import and change the visible property in the property grid to **True** or **False**. The preview updates as layers are turned on or off depending on your selection.



4. Click **Import** to start the import of the drawing. Once the import has completed the new drawing will be available under the **Maps** section. The GISM can now be closed while the import continues and re-opened later to review progress.



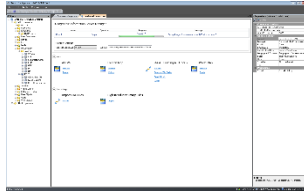
5. Once the drawing has been imported it can be previewed by clicking the preview link.



Exporting Drawing Assets

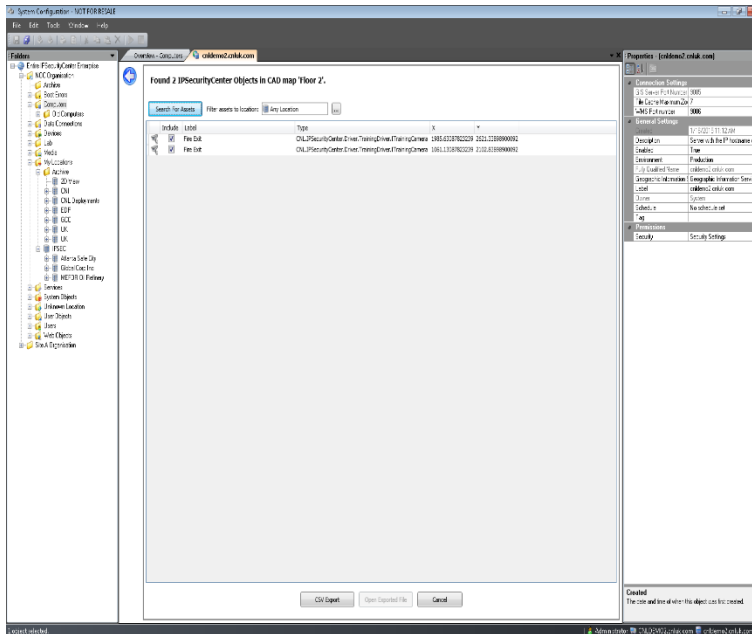
A drawing can contain information about the location of assets, for instance cameras and doors. This information can be used to automatically position assets on Control Center scenes. Control Center can search the drawing for all text strings and then attempt to match these strings with the label of all assets in Control Center.

To search and export a list of matching asset strings for a CAD map, from the **Geographic Information Server Manager** dialog, click the **Export Assets** link.



To search for assets:

1. Select the top-most Control Center location. By default, Control Center searches in all locations (my Location).
2. Click **Search for Assets** to initiate the search.



3. Any asset matches are presented in a list including their label, Control Center device type and the position in the drawing. You can also export the search results to a CSV file for further editing or importing into a scene.

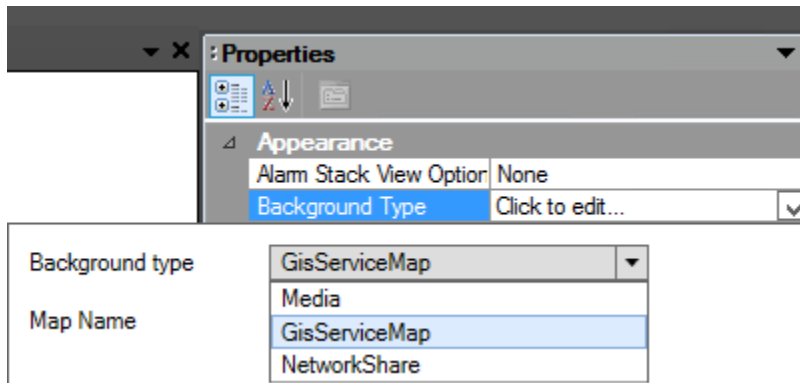
To export the Search results:

1. Click **CSV Export** to save the selected assets to a file.
2. Select the location to store the file and click **Save**. The CSV file with the matching assets has now been saved.

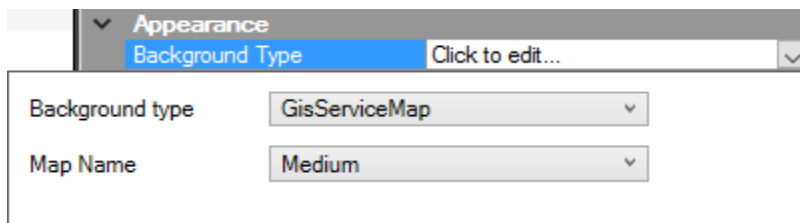
Using an Imported Drawing as a Base Map

To use a GISM drawing as a base map:

1. Create and open a **Schematic Scene**.
2. In the **Properties** pane, select the **Background Type** as **GisServiceMap**.



3. From the **Map Name** property, select the picture that you want to use.



Importing Asset Positions From a CSV File

Asset positions can be imported from a CSV file.

To import asset positions:

1. Click the **Import Assets** button along the toolbar.
2. Select the CSV file to import.



3. Once a file has been selected, a list appears showing the available assets in the file, such as assets that have already been imported and assets in the scene that are not listed in the file.

×

Import Assets

⬆ 0 assets found that are not currently on the scene

Import Icon	Label

Selected assets will be added to the scene.

⬆ 0 assets found that are already plotted on the scene

Replace Icon	Existing Asset	Imported Asset

Selected assets will be updated from the import file. Any existing customisations on the assets will be replaced with values from the import file or default values.

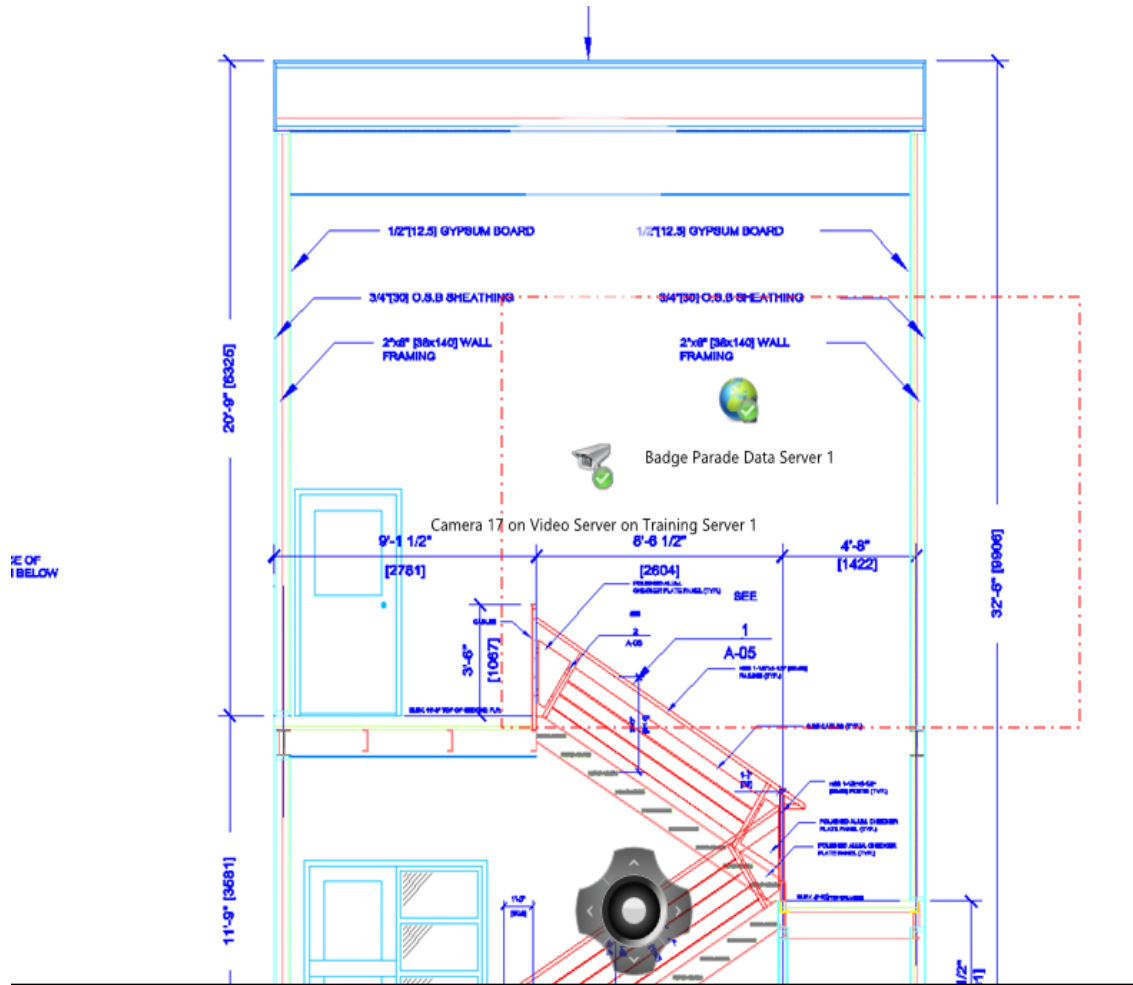
⬆ 0 assets are currently on the scene, but not present in the import file

Remove Icon	Label

Selected assets will be removed from the scene.

To import assets:

1. Select the assets to import and click **OK**. The assets appear on the map surface in the imported positions.



2. Save and close the scene. The new scene is now updated in the end-user interface.

ID	Priority	Date Created	Description	Alarm Type	Alarm Point	Location	Top Location	State	Status	Count	Last Received Event
52	3	6/20/2018 2:09:12 PM	Priority-1 Alarm on Training Server 1	Priority-1 Alarm	Training Server 1	UK	UK		Handled by Administrator	11	7/6/2018 11:17:50 AM
53	3	6/25/2018 10:16:45 AM	Test on Badge Parade Data Server 1	Test	Badge Parade Data Server 1	UK	UK		Unhandled	8	7/6/2018 11:17:50 AM

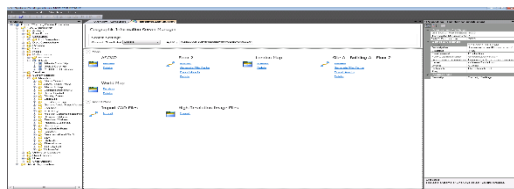
High Resolution Image File Import

The High-Resolution Image importer is similar to the CAD importer however it is much simpler and used mainly for very large images.

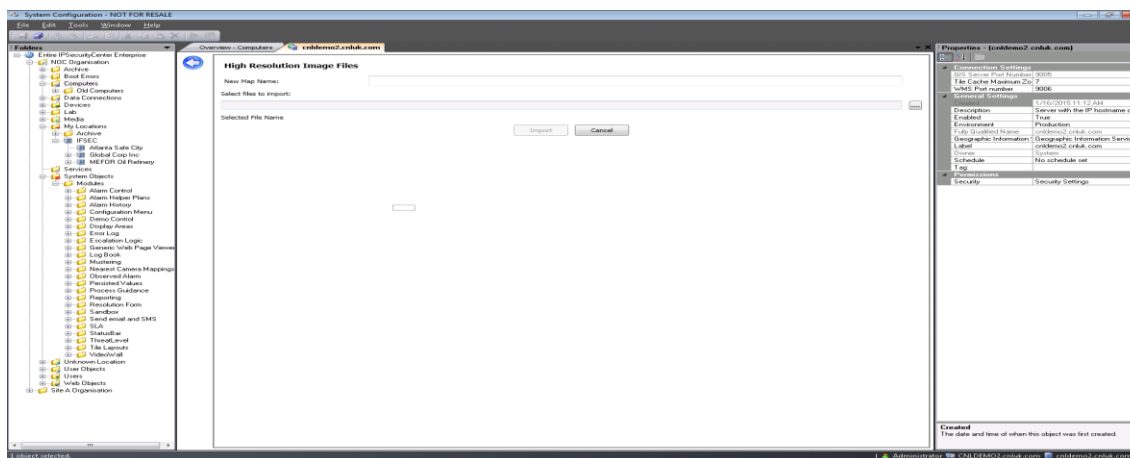
Typically, if the image is of many thousands of pixels in width or diameter, or the file size is hundreds or thousands of megabytes, then it is recommended to use the big image importer.

To import high resolution image files:

1. Double-click or right-click and select **Geographic Information Server Manager (GISM)**.
2. The **GISM** will open in a new tab.
3. Click the **High-Resolution Image Files** button in the Geographic Information Server Manager.



4. This will navigate to the **Big Image File** importer.
5. Type a name for the file, select it, and then click **Import**.



6. On clicking **Import**, the map object is created in Control Center and the Control Center GIS Service begins the process of creating the tile cache. The progress of the import can be seen in the dashboard area of the Geographic Information Server Manager.

Geographical Information System Service Dashboard

Name	Operation	Progress	Message
Large Earth Image	Import	Step 5/10	Saving images for line number 4/8 at zoom level 3

Spatial Index State: Good - Performance optimal [Rebuild Index](#)

Search Settings

Geocode Search Api: None

- The imported map will be shown in the **Maps** area of the GISM. You can select to preview, generate the tile cache, or delete the map.

^ Maps

Large Earth Image



[Preview](#)

[Generate Tile Cache](#)

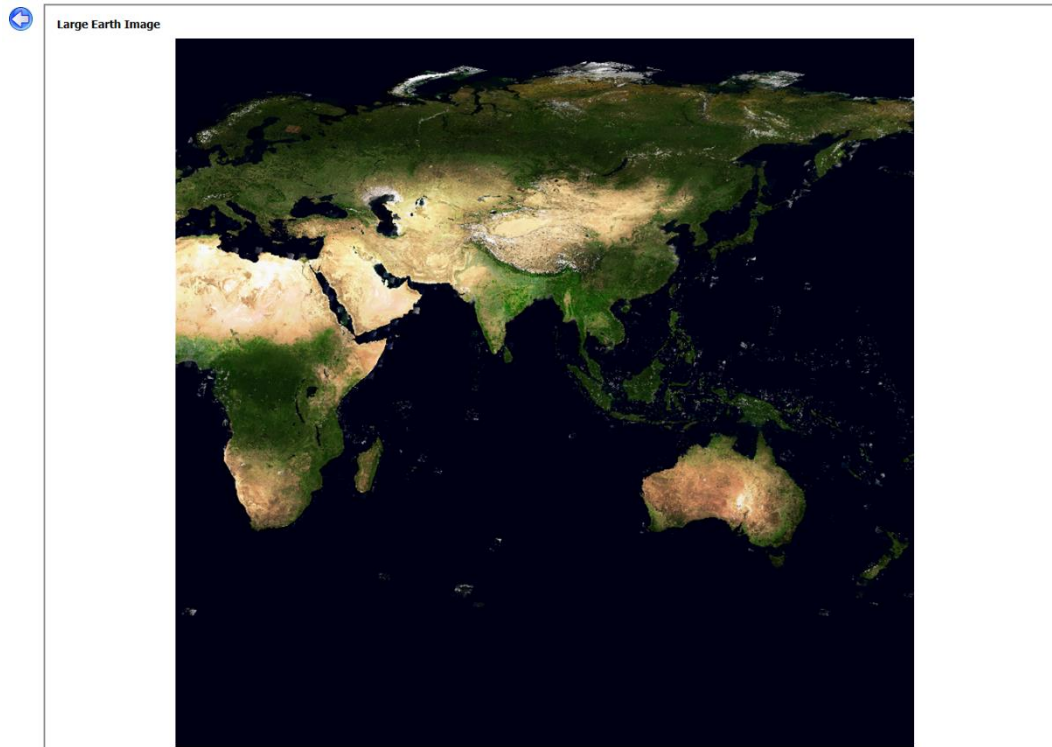
[Delete](#)

Preview

Clicking Preview will show a preview of the imported big image map based on the tile cache created. The same view is available when viewing the map in a scene.

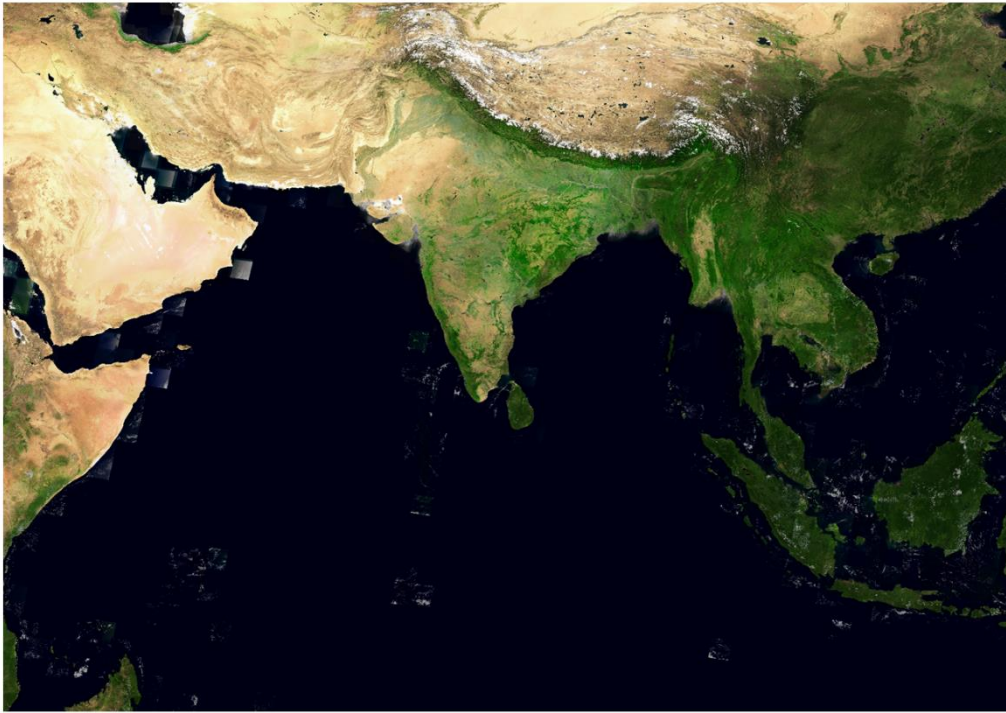
To navigate back to the Geographic Information Server Manager, click the Back button on the top-left corner.

The following image shows a 1.5 GB image imported using a tile cache, which otherwise would have been impossible to load directly into a Schematic scene.



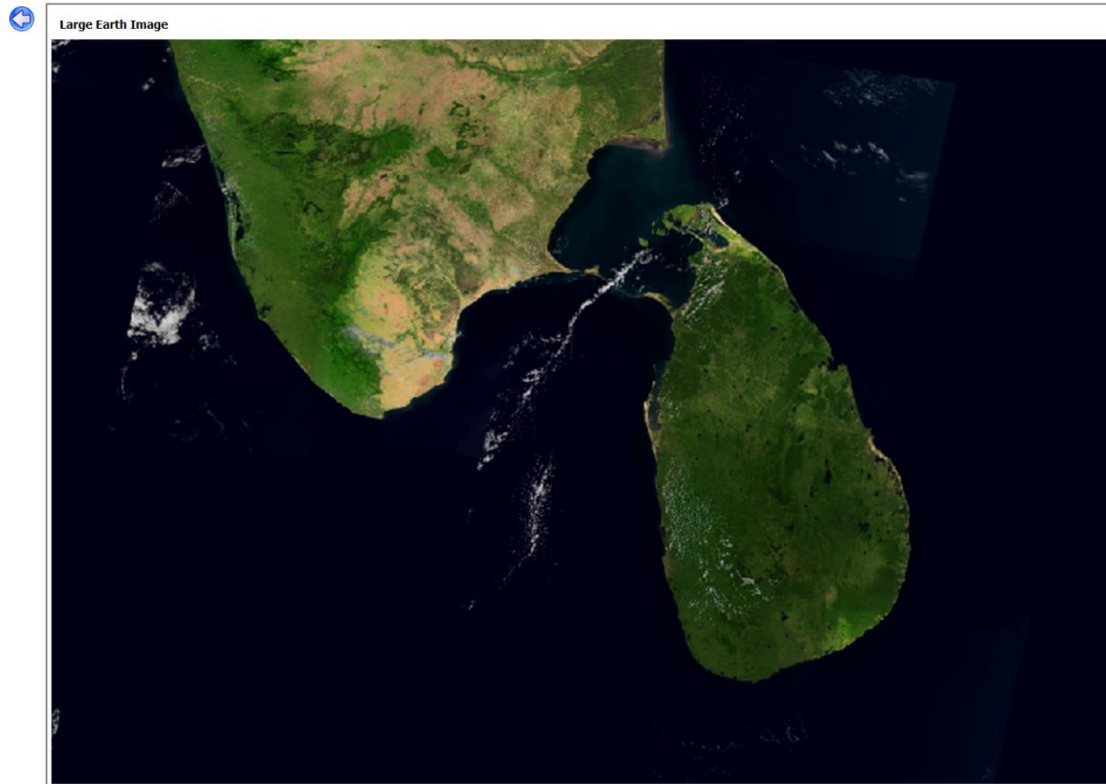


Large Earth Image



Large Earth Image

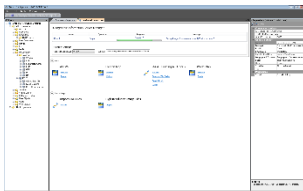




Recreating Tile Cache

The GISM creates a cache of map image tiles on the GIS server machine. If the Control Center database is restored on a new server, it is required to re-create the Tile Cache. This can also be done if the Tile Cache for any reason is corrupt.

To re-create the Tile Cache, open the GISM and select [Generate Tile Cache](#) link under the map to be re-created.



Deleting High Resolution Image Files

To delete a high-resolution image file, select the big image that you wish to delete and click the **Delete** link. A confirmation message appears confirming the delete action.

Warnings

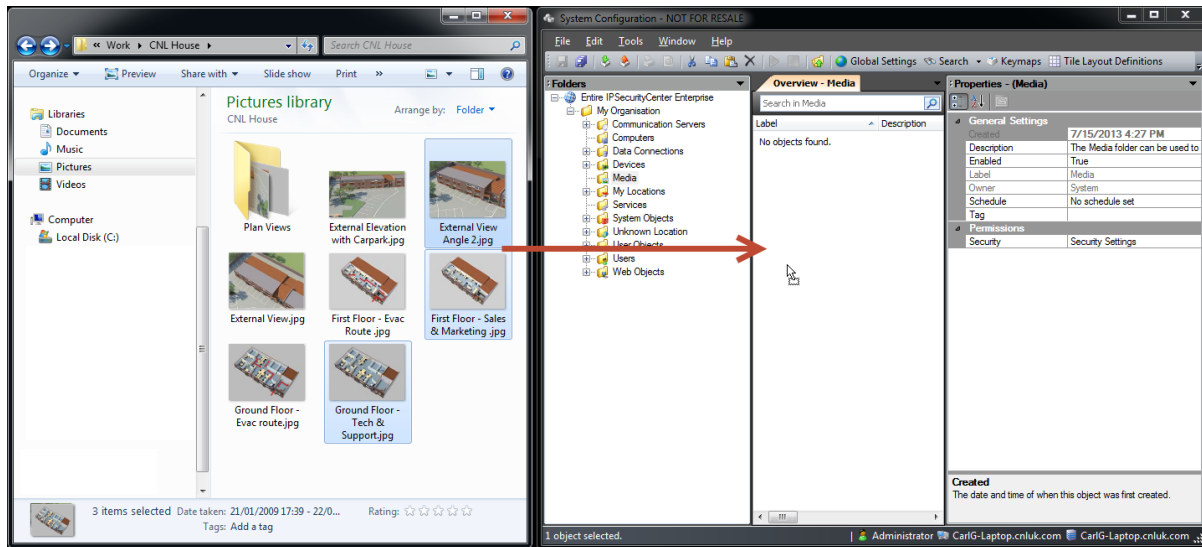
Write access is required to the source image folder when importing large images. The Geographic Information Server will temporarily place files in this folder during import.

Transparent PNG files are not supported. The background of the image must be set to white before importing.

Importing Media Objects

You can import media files as media objects in Control Center as a prerequisite to creating Schematic scenes.

To import a media into Control Center Client, simply drag and drop the file to the Media folder.



The selected files are then added into the solution as media objects and can then be used with schematic scenes.

Media

- External View Angle 2.jpg
- First Floor - Sales & Marketing .jpg
- Ground Floor - Tech & Support.jpg

Adding a Location with Schematic Scene

Locations that need schematic images such as floor plans, can be added with a corresponding schematic scene.

To add a new location with a schematic scene:

1. Right-click in any folder or location, select **New** and then click **Location**.
2. Specify a label for the location and then press the **Enter** key. A dialog appears prompting to create a new scene or to create a location only.
3. Click **Create a Schematic Scene**.

Create a Schematic Scene

Creates a Schematic Scene for the new location.



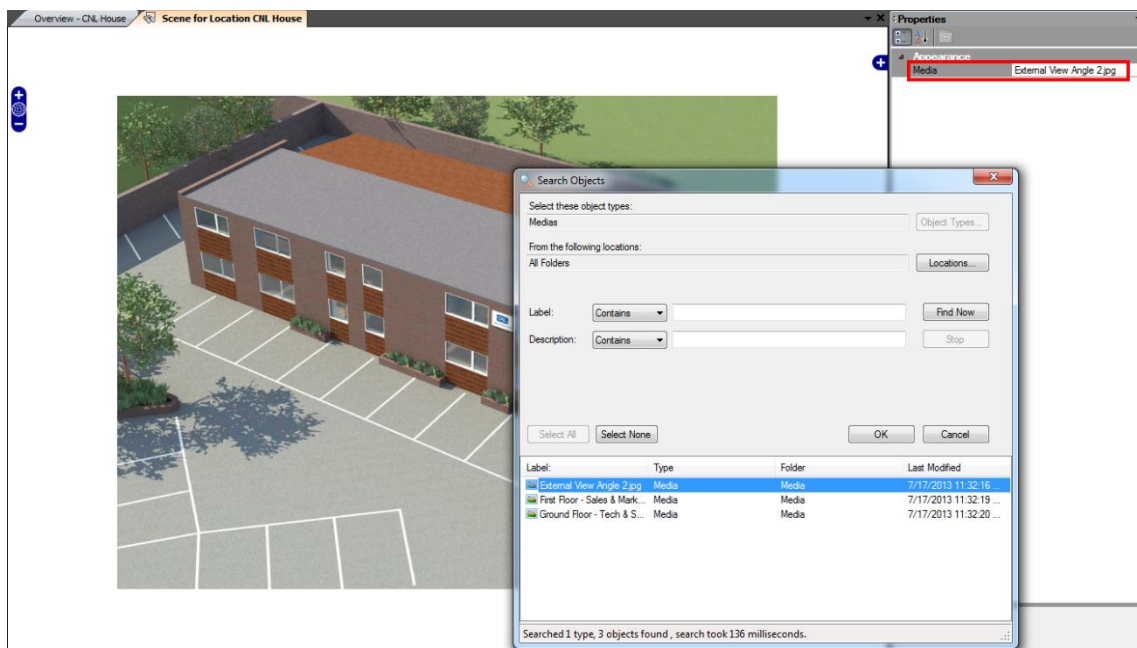
4. A prompt appears asking to edit the scene. Click **No** to proceed.
5. Continue to create as many locations and scenes as required or simply proceed to edit the scene.

Editing a Schematic Scene

A schematic scene offers a similar editing experience to geographic scenes. The only difference is that instead of specifying layers for the map surface, you specify a media file. The following steps assume that at least one media object has been created or imported in the solution which can be used as the map for the scene.

To edit a schematic scene:

1. From **My Locations**, navigate to the schematic scene to be edited and double-click to open the scene editor.
2. Edit the **Media** property and search for a media object.



3. Zoom and position the map based on the map view required for the location.
4. Click any location or asset in the System Explorer control on the left and then click on the map surface to plot an icon.



5. Click **Save** to persist the map position and the plotted icons, then exit the editor.

You can update properties for multiple assets at the same time by selecting multiple objects before changing the properties in the property grid. To select multiple assets, hold down the CTRL key while clicking on the assets to be selected. However, you cannot move or delete multiple selected assets.

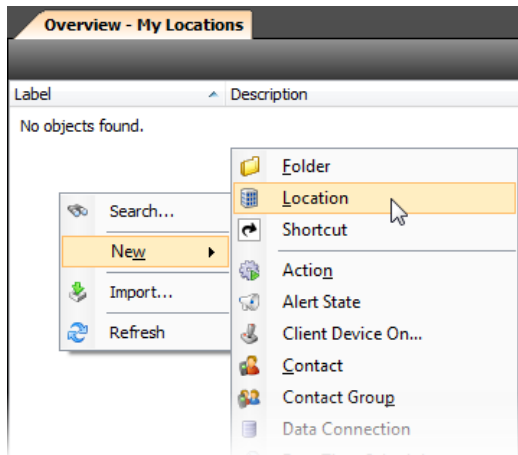
Adding a Location with Geographic Scene

You must at least have added one base layer into the solution to create a schematic scene. A base layer is used as a background map such as OSM and Google Maps, however it cannot include KML files.

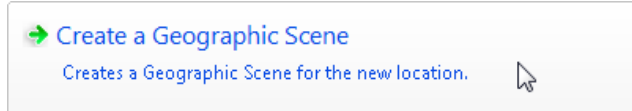
The following steps detail how to add a location along with a corresponding geographic scene. You can specify the existing layers to be used within the scene. The corresponding scene and the associated layers appear when providing the SharpMap GUI control with a location.

To add a location with geographic scene:

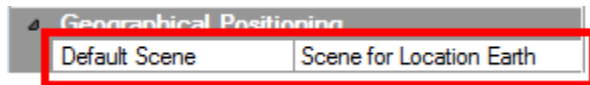
1. Right-click on any folder or Location in System Configuration and select **New> Location**



2. Specify a label for the location and then press the **Enter** key. A dialog appears prompting to create a new scene or to create a location only.
3. Click **Create a Geographic Scene**.



4. A prompt appears asking to edit the scene. Click **No** as the scene will be configured in the section [Editing a Geographic Scene](#).
5. The association between the location and the scene can be viewed in the property grid under the **Default Scene** property of the location.



6. Continue to create as many locations and scenes as required or simply proceed to edit the scene.

Editing a Geographic Scene

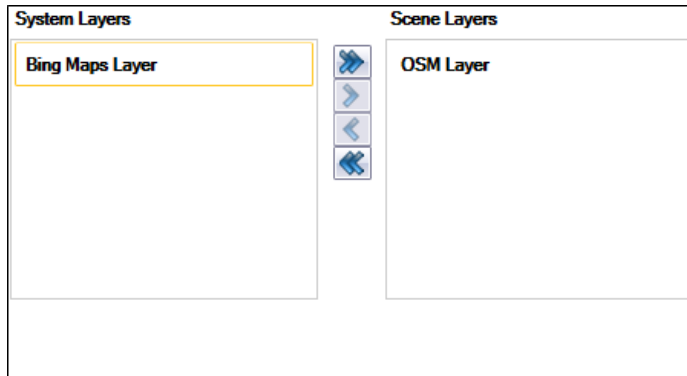
Control Center enables you to edit a Geographic scene to define the GIS layers to be used and to plot assets into the map surface. This requires that the solution is first populated with the different locations and assets (cameras, doors, and so on) to be plotted onto the map before editing the scene.


Follow these steps to edit a geographic scene, define the GIS layers to use, and plot icons for other locations. These steps assume that multiple locations have been created and at least one base GIS layer has been created.

In this example, a hot zone is plotted to allow you to navigate between locations.

1. From **My Locations**, select the geographic scene to be edited and double-click to open the **Scene** editor.

2. Edit the **GIS Layers** property and specify the required layers for the scene. Specify at least one base layer to act as the map surface, for example, **OSM Layer**.



3. Zoom and position the map based on the map view required for the location. Alternatively, click **Layers** to edit the zoom position. For more information on the **Entity Layers** dialog, see [Configuring Visibility Range, Zoom Levels and Clustering](#).
4. To create a hot zone, select  from the toolbar. Hot zones enable you to navigate between locations.
5. From the drop-down list, select **Hot Zone**.
6. Search for an object to associate with the location. In this example, the UK location has been selected.
7. Set the properties on the hot zone as follows and position accordingly on the map:
 - **Custom Size** = True
 - **Height** = 2000000
 - **Opacity** = 0.1
 - **Shape** = Rectangle_tall
 - **Width** = 700000



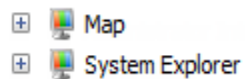
8. Click **Save** to persist the map position and the plotted icons, then close the editor. You can also use the mouse wheel to zoom the map. Alternatively, hold down the **Shift** key, and use the mouse to drag out an area on the map to zoom to.

How to Show Scenes

With locations and scenes configured in the solution, the logic can now be added to show the scenes when the you select a location from the System Explorer control.

This logic is configured when you install Control Center, which can be changed, if required. You must configure this logic in older solutions.

Graphical User Interface



You can configure the System Explorer control to Map GUI for a location to show the scene associated with the location.

To configure System Explorer to Map GUI to show the scene associated with the location:

These steps assume that a blank 1-way tile layout is available in the solution. If this is not available, simply create a new Tile Layout anywhere in the solution called Blank 1x and edit the layout to be 1-way.

1. Go to the **System Configuration > System Objects** folder.
2. Double-click the **System Explorer** GUI and edit it.
3. Select **System Explorer** on the design surface.
4. Edit the **Base Location** property and specify the location to act as the top-most location in the tree of locations.

5. Edit the **Types to Show** property to specify any other objects to show within each location in the tree, for example, **Devices** and **Placeholders**.
6. Handle the **Location Selected** event by dropping down the **Events** drop-down at the top of the GUI editor and selecting the **Location Selected** event. A new event page will be created for the event with event specific variables detailing items such as the location which was selected (Selected_Location).
7. Create two variables to be used to show the map GUI:
 - o A page variable called **MapTile** with type **Tile Layout**. Set the **Special Properties > Tile Prototype** property as the **Blank 1x Tile Layout**.
 - o A page variable called **Map** with type **GUI**. Set the **Special Properties > Graphical User Interface** property as the Map GUI.
8. Drag and drop the **Script** shape on the **Event Pages** editor to configure the GUI variable with the selected location variable using the following script:
 My.PageVariables.Map.sharpMapGISMap1.GotoLocation(My.PageVariables.Selected_Location)
9. Drag and drop the **Configure Tile Layout** shape setting.
10. Select the **Tile Variable** property to show the **MapTile** variable and the **Actions** property to place the **Map** variable in tile 1.

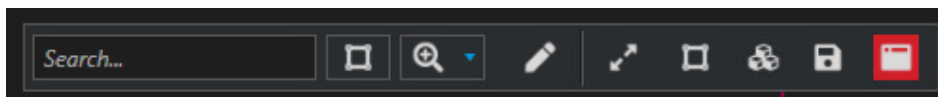
Tile Number	Action	Data
Tile 1	Gui	Map (Variable)

11. Add a **Display Tile Layout** shape and set the following properties.
 - o **Update Tile layout** - True
 - o **Display Area** - System Main (Static)
 - o **Target Objects** - Current Generic Client (Variable)
 - o **Tile Layout Variable** - MapTile
12. Add a **Finish** shape, then save and close the GUI.
13. Upon saving the GUI, the updated version will be pushed out to all currently logged-in clients. Ensure that the logic has been configured correctly by selecting a location in the System Explorer. When selecting a location, the Map GUI should be shown detailing the scene associated with the selected location.


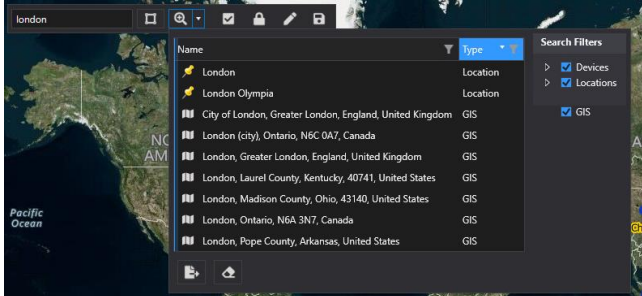
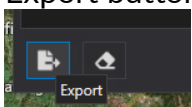

Toolbar Displayed on the Global Map


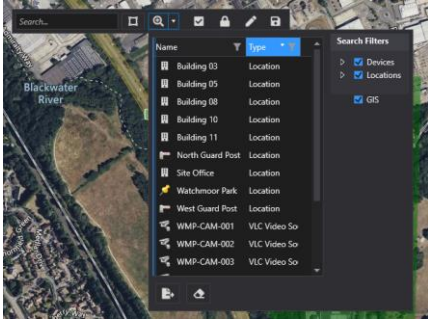

There are two toolbars displayed on the global map.

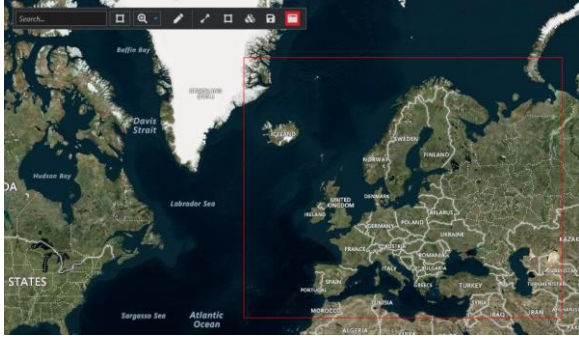

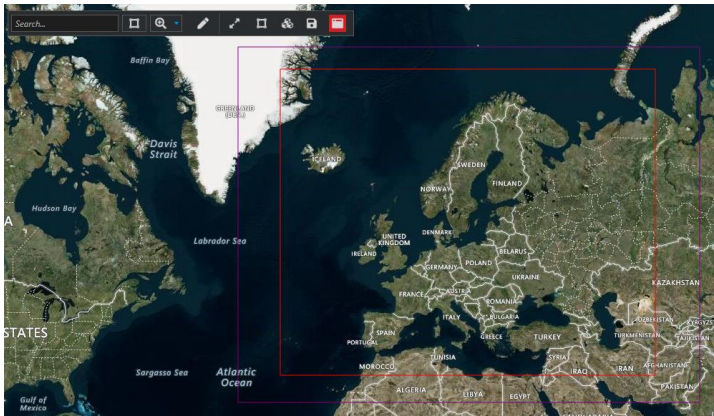
From this toolbar you can select actions you can perform on a map.



The following table describes the actions you can perform from the toolbar in the global map.

Name	Description
Search Box	<p>You can search for assets, locations, supported addon layers and external GIS results by entering text into this box and pressing the Search button .</p>  <p>From the search results screen, clicking a result will pan and zoom to that item. Using the Search Filters you can remove unwanted results, and you can export results to CSV using the Export button.</p>  <p>Search results are highlighted on the map with a pin icon. You can return to the search results screen by using the dropdown arrow to the right of the search icon.</p> <p>Pressing the Clear Search button will remove the search results and map pins.</p>
Area Search	<p>The Area search button allows you to draw a shape on the map to return assets, locations, and supported addon layers within the shape.</p> <p>This can be combined with the Search Box to search for text within the drawn area.</p> <p>To perform an area search:</p> <ol style="list-style-type: none"> 1. Click the boundary icon next to the Search box. 

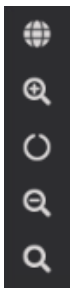
	<p>2. Click on the map to place points. When more than two points are placed this will create a polygon between the points.</p>  <p>3. Click the boundary icon again, or press the search icon, to see the search results.</p>  <p>4.</p>
<p>Draw Figures and labels on maps</p>	<p>You can add lines, text and shapes to your maps. See Using Map Annotations.</p>
<p>Set Minimum Visible Map Area</p>	<p>The Set Minimum Visible Map area in the Scene editor of the Client (not Legacy Client) enables you to set the area of the map as close as possible to the view an end user would see.</p> <p>When displayed in the end-user GUI, the map extents and zoom level can be set to ensure that the entire marked area is visible at the maximum possible zoom level. Depending on the aspect ratio of the end-user GUI parts of the map beyond the marked area will also be displayed.</p> <p>To set the minimum visible map area:</p> <ol style="list-style-type: none"> 1. Click the Set Minimum Visible Map area  icon. The icon will be highlighted. 2. Select the area of map to be configured by holding down the shift key while dragging the mouse button to select the area you want to cover:

	 <p>3. The area that has been set is marked in the Scene editor as a rectangle with a dotted red outline, however it does not show up in the end-user interface.</p>
<p>Set Map Pan Boundaries</p>	<p>Panning on a map is an action of dragging the map to move to a location without changing the level of scaling as opposed to the zooming action which changes the scaling.</p> <p>Setting a map pan boundary will help the administrator to define the area on the map within which the user/operator can pan. This feature is particularly useful in scenes with larger images or maps where the user can easily lose focus in an attempt to get to a desired location while panning the map.</p> <ol style="list-style-type: none"> 1. Click on the set map pan boundary icon  on the toolbar. 2. Select an area of map by holding down the shift key while dragging the mouse button to select the area you want to allow panning.  <ol style="list-style-type: none"> 3. Save the scene. <p>When the pan boundary is set, the Minimum Zoom Level of the map will be changed to the level that displays the whole pan</p>

	<p>boundary. This is so the user cannot zoom outside the pan boundary. The Minimum Zoom Level can however be changed to a different value if desired.</p> <p>Key points to note:</p> <ul style="list-style-type: none"> • The pan boundary does not apply on the scene editor. You need view the scene on the main screen to see the pan boundary set on the map. • The pan boundary is similar to the set minimum visible area functionality. • On a fresh install of Control Center version 5.10.2 all new scenes will have, both minimum visible area and pan boundary set to the whole map area as the default. For all the existing scenes, the pan boundary will need to be set. • Always define the minimum visible area inside the pan boundary. If the minimum visible area is larger than or outside of the pan boundary, the area outside the pan boundary will not be visible in the map. • Pan/Zoom to location on selection will not have any effect if the location selected is plotted outside the pan boundary on the map. • Zoom to Max Extent on Load will not take any effect if the zoom level is set lower than the minimum zoom level as it would be referring to places outside of the pan boundary.
Import Assets From CSV File	<p>Use Import Assets on the toolbar to import asset positions and style information from a CSV file. The Import Assets and Save Template buttons are now displayed on the toolbar that is available in the Scene editor when editing either geographic or schematic scenes.</p> <ol style="list-style-type: none"> 1. Click the Import Assets icon from the toolbar. A dialog to locate the CSV file opens. 2. Select the CSV file that you want to import and click OK. Once a file has been selected, a list appears showing the available assets in the file, such as assets that have already been imported and assets in the scene that are not listed in the file. The user can then decide how the data in the import file is used to update the assets on the scene.

Save Asset Import Template	<p>Use Save Asset Import template to save asset positions into a template in the form of a CSV file.</p> <ol style="list-style-type: none"> 1. Click the Save Asset Import template icon on the toolbar. A dialog to save the .CSV file opens. 2. Provide a name for the .CSV file and click Save. The new asset import template is saved for importing into a scene. Provide a name for the .CSV file, for example, assetpositions.csv and click Save. The new asset import template is saved with headers and blank comma separated fields for importing into a scene. 3. To use the .CSV template, enter the values for the following mandatory fields by copying from an external file or by manually entering the values: <ul style="list-style-type: none"> ○ ID – The unique identifier of a device from Control Center. ○ Label – The label of the device. ○ X – The longitude position of the plotted device. ○ Y – The latitude position of the plotted device. <pre> ObjectIdentifier,Custom Label,X,Y,IconName,HideIcon,IconSize,Icon Visibility,Rotation,Use Custom Icon,Visible Object Search Radius,Viewsh 57E7866A-CBD4-4F51-AA0A-5E22AC348EF, Drone 1, -0.187928 ,51.505490,..... AE0995AC-09F8-4B29-8B45-7D022AC48EE, Drone 2, -0.187988 ,51.505587,..... 9A2F9671-C74B-43E3-BB89-CE69896A7E44, Drone 3, -0.188401,51.504806,..... 549C75C4-E8E2-4F14-A2C2-F128B894C11, Drone 4, -0.187998 ,51.504943,..... </pre> <ol style="list-style-type: none"> 4. ID, X, and Y are the only mandatory properties that must be filled. Other values can be left blank. When you have added the assets to the template file, save it as a CSV file.
Enabling/Disabling Clustering	<p>When zooming in and out on a geographical or schematic scenes, you can cluster cameras together for clarity. See Using Clustering.</p>

You can use this toolbar to navigate around your map.



The following table describes how to navigate round your map using the map navigation toolbar.

Name	Description
Toggle Mini Map	Select the Mini Map icon to display a mini map of your global map. Move the global map until you find the area of your global map that you want to display in your map. You can move your global map around until you find the area of the global map you want to display in your map.
Zoom In	Zooms the current displayed map based on the selection made.
Reset Zoom and Position	If you have zoomed in or out of your map, you can reset your map to its original state.
Zoom Out	Zooms out of the current map based on the selection made.
Zoom to Max Extents	Zoom out to the maximum extent available for your global map.

Configuring Map Navigation Control

You can configure whether you want the Map Navigation control to be displayed on your maps. The Map Navigation control is visible by default.



You can disable the Map Navigation control by setting the **Hide Navigation Control** property to **False** in the **SharpMap** control.

Layers

Use the Layers option to set the zoom settings in the Entity Layers dialog to perform the following:

- Make sure the map is not cluttered when you zoom out.
- Adjust the zoom levels at which the labels should appear for a scene. To do this, click on the map surface and then select the **Layers** property in the property grid.
- Adjust the visible range for the labels layer using the slider.

Displaying Trail Paths on Map Surface

To display trail paths on a map surface:

1. Configure the **Trail Point** layer.

2. Display the default location in the Display Area.
3. View the Scene. The trail paths are displayed on the scene.
4. Zoom the map in and out to see the trail paths. In addition, right-clicking on a trackable object provides the following options:
 - **Get Nearest Cameras**– Displays the nearest camera devices from the selected point. Note: This feature only works if you have configured the Map GUI with Get Nearest Cameras event.
 - **Hide Trail (TrackId)** – Hides the trail path for the selected tracking object. However, the icon for the object will still be displayed.
 - **Hide all trails**–Hides all trail paths for all tracking objects on the scene. However, the icons for the objects will still be displayed.
 - **Show Trail**– Displays the selected trail for the selected object.
 - **Show all Trails**– Displays the trails for all geo-aware objects on the scene.
5. The trail itself is made up of trail segments, where a segment is shown as a line between two trail points. Hovering over a trail segment shows the start and end time of the segment, and the time difference between the two trail points. For example:


From 8:48:39 AM
 To 8:48:40 AM
 (1.059 seconds)


Asset Geometry Linked to a Device

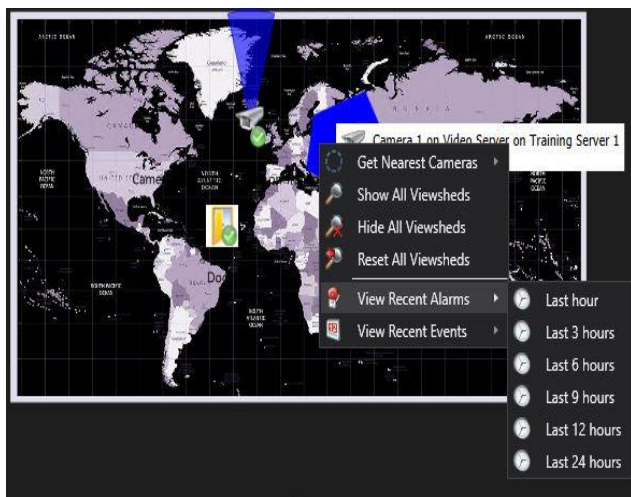
The asset geometry can be defined for a scene and linked to a device or door in the system configuration window. This will allow the user to view context menu for that particular device in the defined area. Only one device can be linked to a polygon or line at any given time.

Configuring Asset Geometry

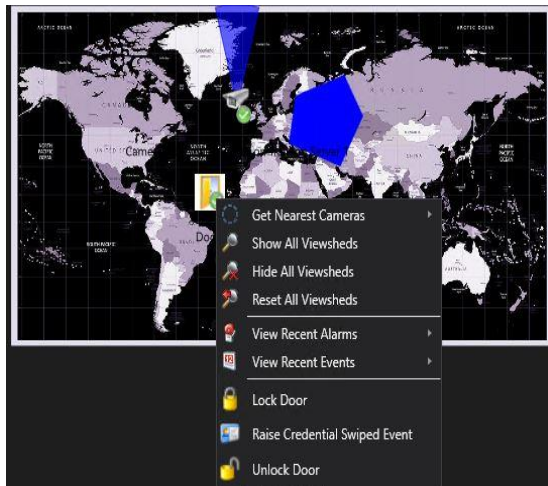
To configure asset geometry for a particular location, do the following:

1. Go to **System Configuration** and create a location object under **My Locations**.
2. Go to the location created and create a scene.
3. Double click on the **Scene** object to open it.
4. Plot at least one camera and door on the map.
5. Select  from the tool bar.
6. From the drop-down list, select **Label/Line/Polygon** or **Hot Zone**, depending on your requirements.

7. Select the map where you want to place the asset geometry.
8. Do the following:
 - o For **Labels**, edit the text of the label in the Label property. Depending on your requirements, you can save the settings and close the scene window, at this point.
 - o For **Lines** and **Polygons**, select the map again where you want the next part of the line or polygon to be. Repeat this step until you have finished creating your line or polygon. Select  again. A search window appears for you to choose the device you want to link to. Select the device and click **OK**.
 - o For **Hot Zones**, a search window appears for you to choose the device you want to link to. Select the device and click **OK**.
9. Save the settings and close the scene window.
10. Go to the **Main** display and select the location for which the asset geometry was defined.



11. Right click on the asset geometry to view the device context menu linked to it.

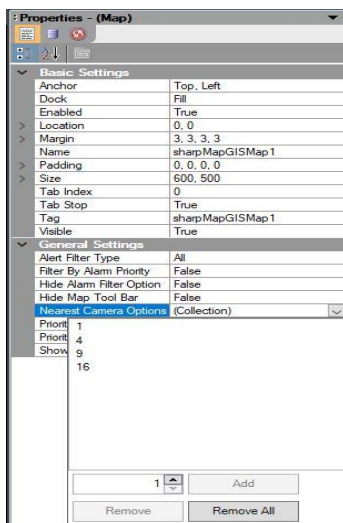


Only one device can be linked to the line/polygon at any given time.

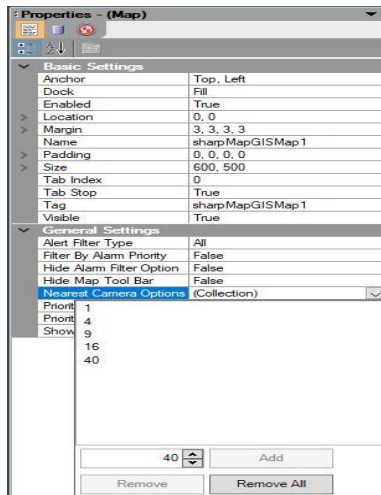
Configuring Get Nearest Cameras

You can configure the number of cameras that can be made available in a selected location on a Schematic or Geographic map as follows:

1. Go to **System Configuration > System Objects**.
2. Go to the **Design Surface** tab of the **Map** object selected.
3. Click on the **Nearest camera** options to see the existing list.



4. Enter the count of cameras you wish to add and click on the **Add** button.



5. Save the settings.
6. You can now right-click the **System Map > Get Nearest Cameras** and view the new configuration.



Configuring Visibility Range, Zoom Levels and Clustering

The zoom level is a value representing the magnification of a map/image representing the scene. Every time you move the mouse wheel forward to zoom in, the magnification of image is increased proportional to the mouse wheel movement.

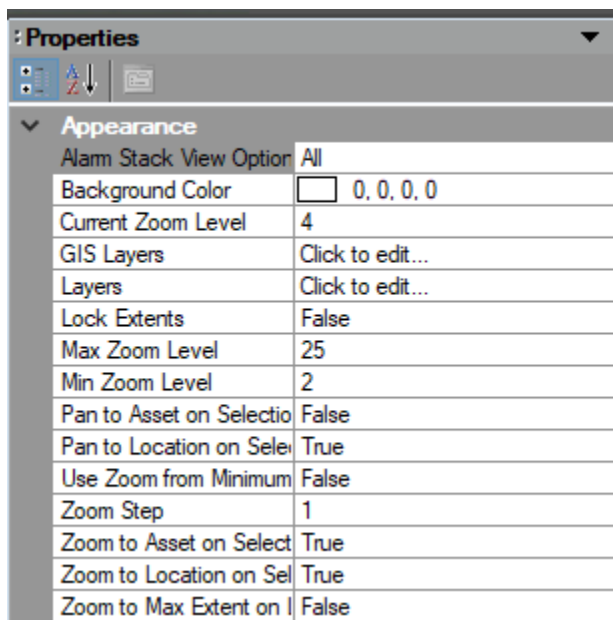
Different asset and location types appear in different layers on the map surface. You can set the visibility range and zoom levels to show or hide the assets on the map. Visibility range is set by using the sliders on the Entity Layers dialog and Zoom levels are configured using the Min Zoom level and Max Zoom Level property in the property pane of the scene editor. The granularity of zoom levels can be set using the Zoom Step property.

This helps the user to navigate on large drawings or maps without spanning too much far or near on the screen.

Setting Zoom Level for a Scene

Zoom level helps the user to focus on the assets plotted on the map by zooming in to have a closer view or zooming out to have an broader view of the scene. By setting the zoom level, the administrator can limit the users from spanning too much far or far too near on the scene. The zoom level properties can be set in the property pane of the scene editor. To configure the zoom level:

1. Go to **System Configuration > My organization > My Locations** and select the scene for any location listed under this folder
2. Double click on the scene object to open the scene editor.
3. **Property** pane is shown on the right, in which the zoom level configurations can be set as shown in the figure below.



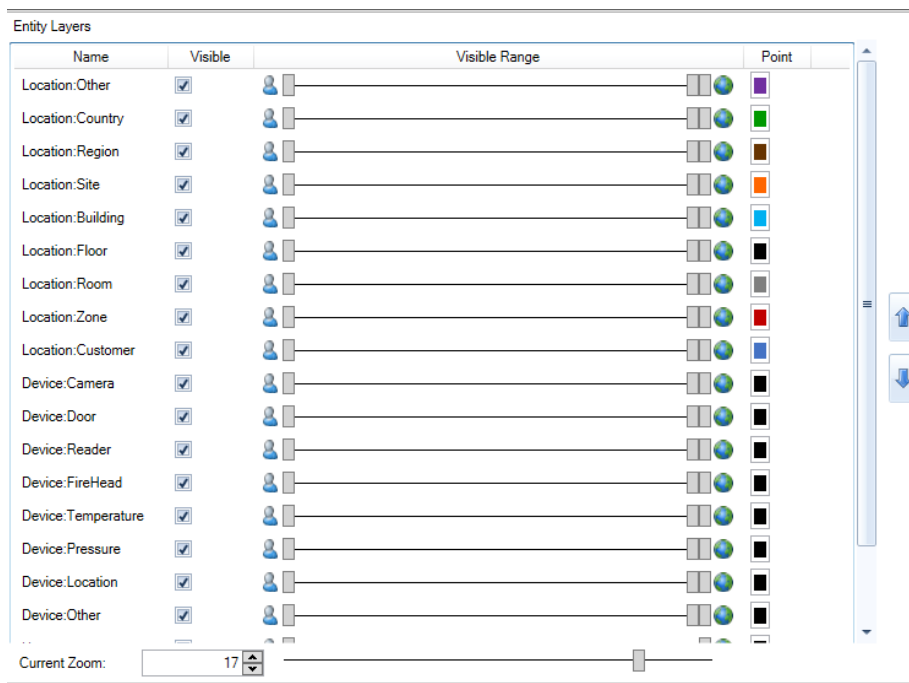
Three properties help the user to configure the zoom levels as mentioned below:

- **Max Zoom Level:** Defines how far you can zoom in to a particular location on a map or CAD image. The default value is either 20 or 30 depending on the type of the scene background selected.
- **Min Zoom Level:** Defines how far you can zoom out of the map/image. The default value is always set to one. The user can configure the minimum zoom level to any number greater than 1 but **MUST** be lesser than the Max Zoom level. If the Min Zoom value is greater than the Max Zoom level, the value will automatically default itself to the previously saved value.
- **Zoom Step:** Controls the zoom in/out granularity. The default value is 1, meaning a zoom level of 2 changes to 3 with one click. For example, setting this to 0.2 would mean that the zoom level changes from 2 to 2.2 with each click.

- A fourth property, **Current Zoom Level** indicates the current zoom level of the scene. A zoom value can be entered here to take the current zoom to the desired level. If the current zoom level is set greater than the Max Zoom level, then the value will default itself to the Max value. Similarly, if the Current Zoom level is set to lesser than the min zoom level it will default itself to the Min Zoom value.

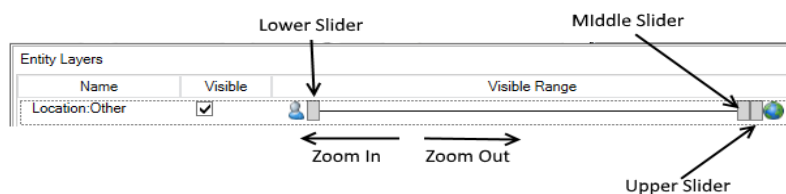
Setting Visibility Range for a Scene

To set the visible range for a layer, and the current zoom settings can be configured using the layers dialog. The Entity Layers Dialog allows the commissioning user to set the visibility of Location Types, Location Icons, Point Colors for Locations or Devices, and the option to preview the zoom level for the current scene. You can move the sliders to define the range when the layer should be visible.

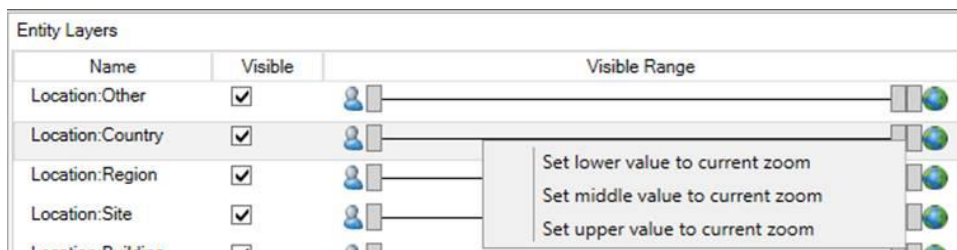


Visible Range Controller

You can plot assets as icons or points on a 2D Scene. In the Entity Layers dialog, you can specify a range of zoom levels where the icon for the asset is replaced by a colored point on the screen.



- **Setting Visible** range – The visible range for the scene appears as a horizontal line where the human icon on the left represents the most zoomed-in setting that the scene supports. The globe icon on the right-hand side represents the furthest zoomed-out extent that the scene will support. The actual numerical values for these extents will vary by the type of the scene (GIS or Schematic) and by the size in pixels of the image itself.
- **Setting Current Zoom** levels – You can set a zoom level to a value more than the maximum supported by the sliders, however the upper slider values should not exceed the maximum range for the scene. In addition, when setting the value for sliders, you can right-click the visible range control for the entity to set the sliders to the current zoom level.



If the zoom level is below or above the low/high visibility bar, then the layer is not visible.

Using the Entity Layers Dialog

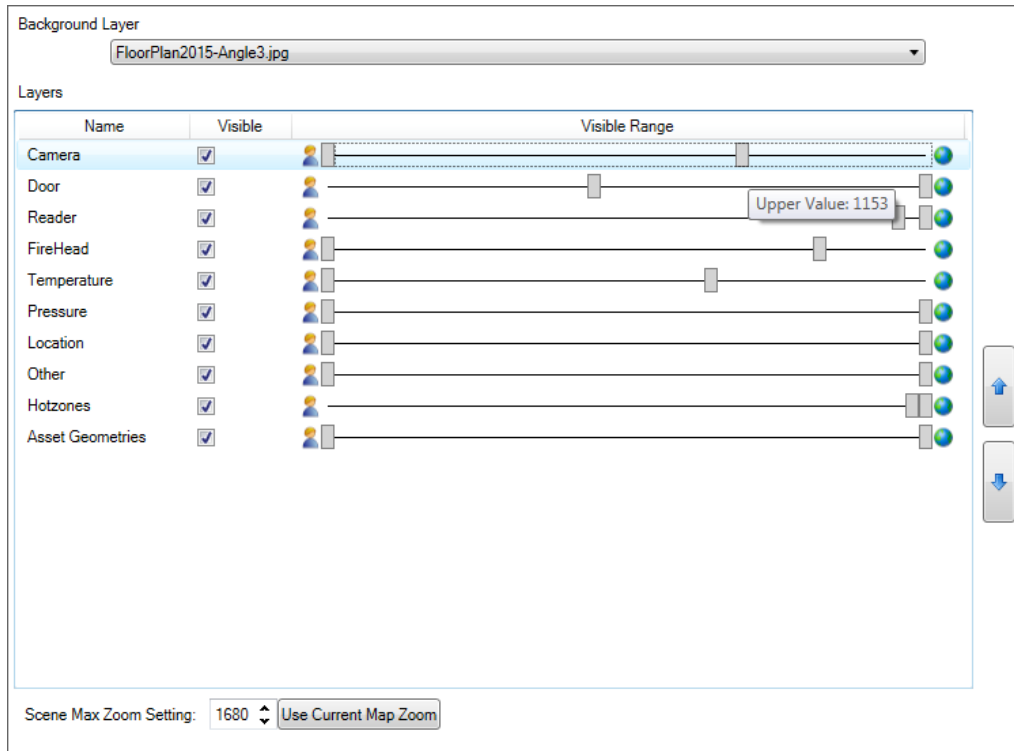
- To access the **Entity Layers** dialog, open the scene for editing and click the **Layers** property.
- To close the dialog, click outside the area of the dialog box.

The Entity Layer dialog is divided into the following sections:

- **Entity Layers Controller**
- **Overlay Layer Controller**
- **Background Layer Controller**

Using the **Entity Layers** dialog, you can control the following aspects of how plotted items are displayed on the scene:

- Whether a specific Location or Device Type is visible on the scene. The Visible check box next to the name of each Entity Type controls. The check box indicates whether the selected entity will be visible on the scene. By default, a new scene has all Location Types, Device Types, and other Entity Types set to be visible.



- To make a layer invisible, clear the Visible check box in the Layers dialog.
- The range of zoom levels, where:
 - Icon for the Location Type or Device Type appears: the range between the Left and Middle Slider Controls.
 - A colored point appears for the Location Type or Device Type instead of the icon: the range between the Middle and Right Slider Controls.
 - No icon or colored point appears: the range below the Left Slider and above the Right Slider.
 - Hotzones, Asset Geometries, Labels, and Mappable Devices appear or are hidden from the user.
- The colors used to indicate which Location Type or Device Type are on the map.
 - The Color Selectors for Hotzones, Asset Geometries, Labels and Mappable Devices are not functional currently.

Hotzones, Asset Geometries, Labels, and Mappable Devices do not have a colored point representation, therefore only two sliders appear.

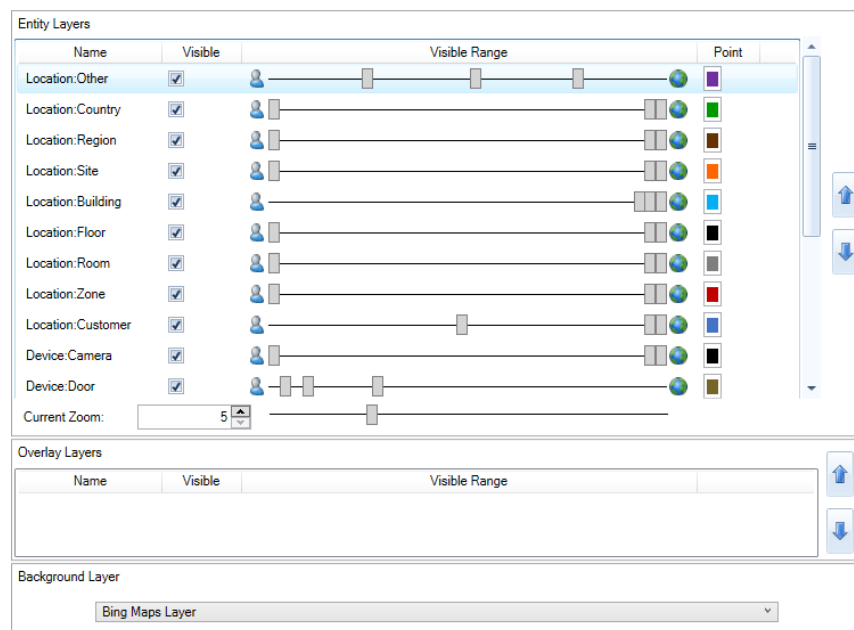
- The z-order in which each type of entity is drawn on the screen, that is, when entities overlap each other, which is displayed on top.

GIS Scenes

For a GIS scene, the Current Zoom range is established between 1 and Max Zoom Level. To correctly set up the Entity Visibility, adjust the current zoom of the map using any of the following controls: text entry value, up/down control.

The slider instantly adjusts the view on the screen. The new zoom value is applied to the scene as soon as you click away from the control.

The Current Zoom Controller value assists with visualizing the placement of the Visible Range Sliders for the various Entity types.



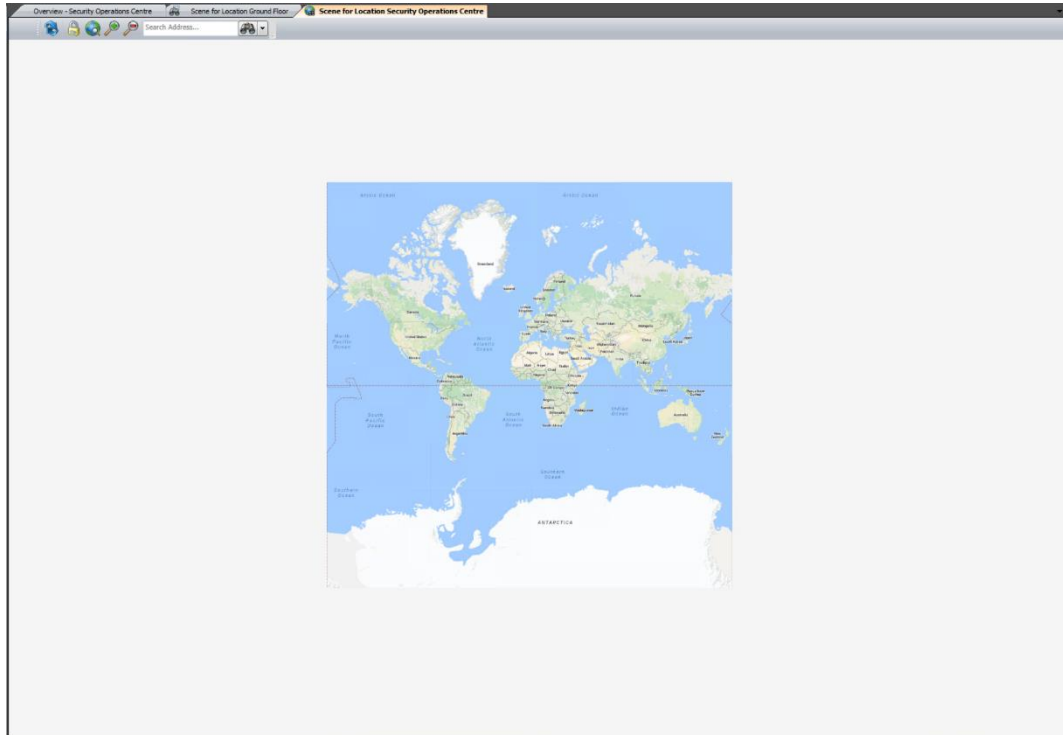
Current Zoom Range – GIS Scenes

As the size and aspect ratio screen of the visible area for a Scene may differ from system to system, Control Center enables you to display the Map scenes in the target display area such that the largest dimension in pixels on the scene fits to the appropriate dimension on the target display.

Depending on the aspect ratio and size of the target display area, you can customize the map to display more horizontal or vertical map area on the main display area. The level of detail and the area of interest as configured in the scene is always retained. However, when presenting the scene, you can zoom independently of the initial setting. You can also use the Lock Extents property on the Scene to prevent the user from zooming in or out from the Scene as it initially loads.

The value shown in the Current Zoom control is calculated based on the current zoom level of the underlying scene. As you zoom out past the extent of the width of the earth,

the Layers Dialog will display the current zoom level based on the actual calculated number of meters to be shown on the screen below the associated Layers dialog.



The Current Zoom value is the value that the screen can accommodate from the left edge to the right edge of the screen. This value is defined between the Minimum and Maximum Zoom values in order to retain the focus within the range specified.

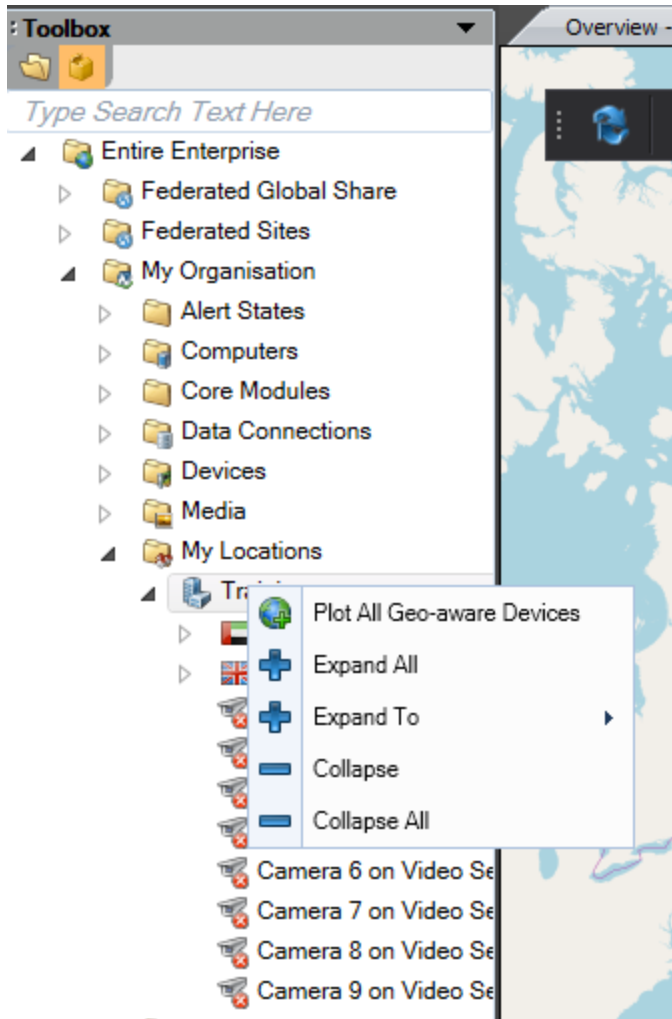
You can save the currently selected zoom level to the scene in Layers dialog. In addition, you can restrict zooming out from the boundaries of the image or map surface that make up the scene.

Automatic Positioning of Geo-aware Devices

Only applies to geographic scenes.

An Control Center device can be Geo-aware. This means the device has a geographical position stored in **Longitude/Latitude**. The position is visible in the **X** and **Y** properties visible in the property grid when selecting the device. If you have Geo-aware devices, you can now automatically plot them on your map using the **Plot All Geo-aware Devices** option. This means you do not have to drag and drop your devices individually to your map.

From **System Configuration**, right-click on your location folder and select **Plot All Geo-aware Devices**.



Schematic Scenes

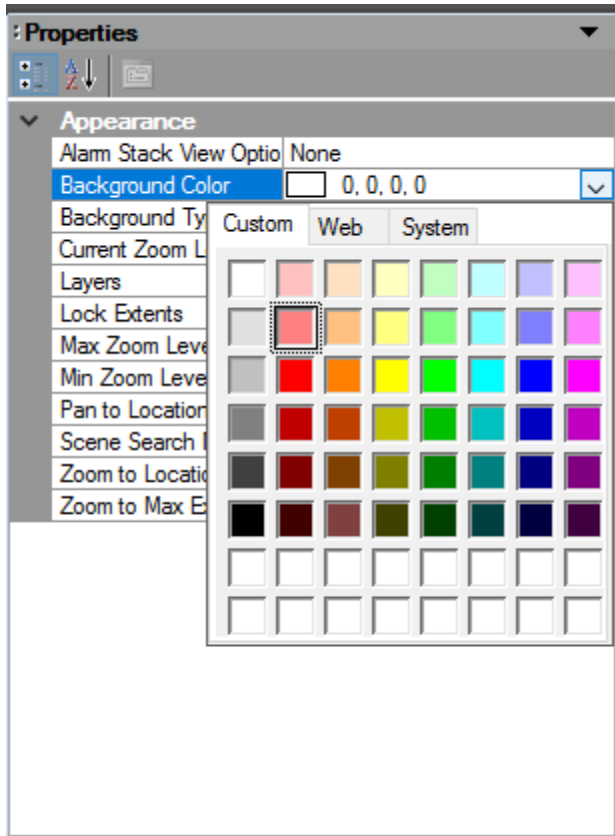
The Visible Range Controller for Schematic scenes works the same as GIS Scenes. Currently, Control Center allows scales between 1 and 5000px similar to the method used for GIS Scene with pixels instead of meters. For images where both dimensions of the image are smaller than 5000px, the dialog box will allow the user to accurately locate and manage the position of plotted assets.

Currently, there is a known issue that limits the sliders on a schematic scene to 1px to 5000px range, which makes it challenging to accurately position the visible range markers on very high-resolution images. This issue will be addressed in a future release.

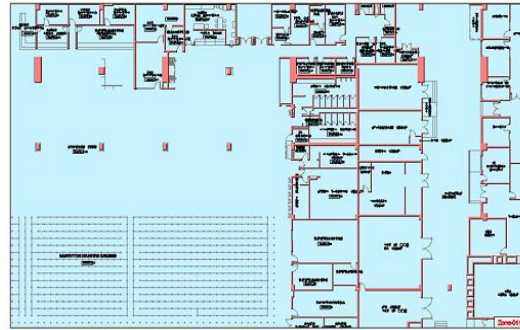
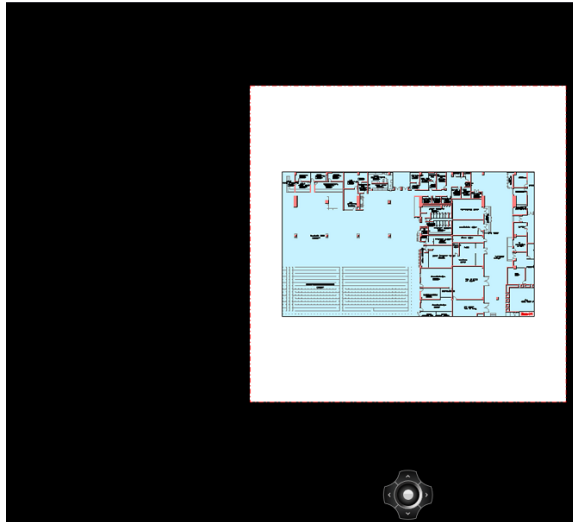
This issue affects all Schematic scenes including those based on Media objects or served by the built-in Geographic Information Service Manager.

Defining Background Color for the Scenes

The Background Color property, available in the scene editor, allows you to change the background color of the CAD/Media image to blend with the background color of the scene.



When the user clicks on the background color property of the scene editor, a color palette is displayed. A suitable color can be chosen and saved for the scene. It can always be rolled back to the default color by selecting the transparent option under Web tab in the color palette. The difference is illustrated below.



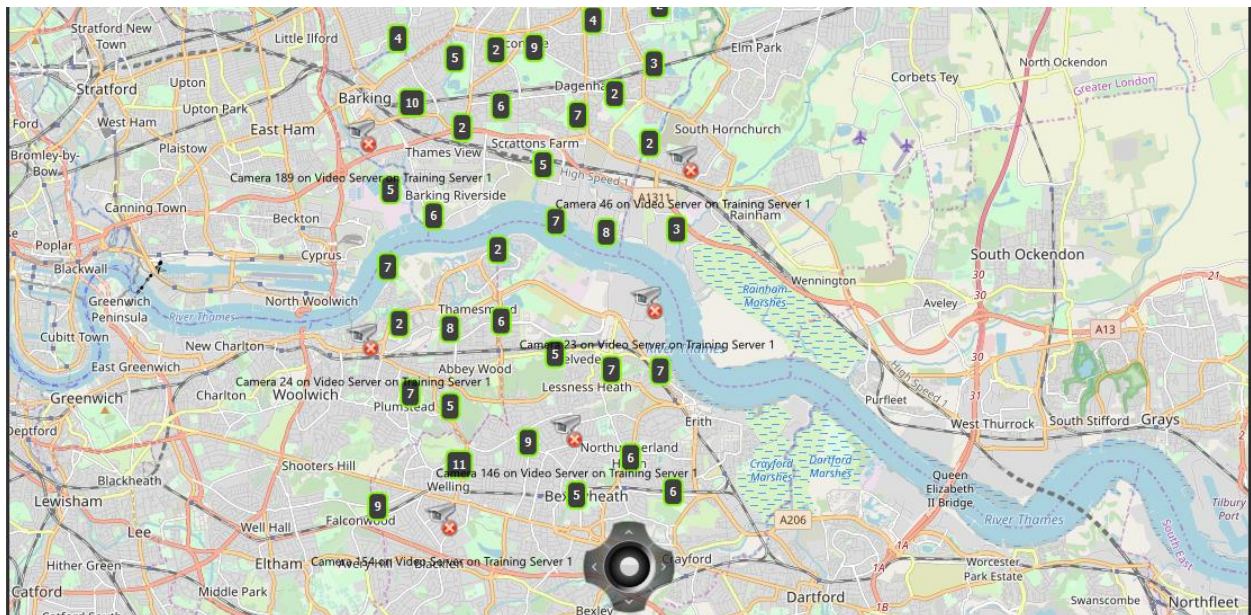
Using Clustering

When zooming in and out on geographical or schematic scenes, cameras are clustered together for clarity.

When you are zoomed in to the maximum zoom level, cameras are not clustered.

Select a cluster to display all the individual cameras within that cluster. If you select an individual camera, Control Center automatically zooms into that camera on the map.


When clustering is enabled, right-clicking a cluster only works for the first camera in the cluster. For example, you can only view the alarm history for the first camera in the cluster.



In the Map GUI, clustering is disabled by default. To enable clustering in the Map GUI:

1. Go to **System Configuration > Entire Organization > My Organization**.
2. Select **System Objects**. The **Overview** tab displays.
3. From **Graphical User Interface**, double-click **Map** to open the editor.
4. Select the **Design Surface** tab to display the properties and set **Enable Clustering to True**.
5. Reload the map, for example, by logging off and on again.

By default, clustering is enabled in the Scene Editor. You can turn clustering on and off in the Scene Editor, depending on your requirements.

1. Go to **System Configuration > My Organization > My Location**.
2. Select the location whose map you want to view. The **Overview** tab displays.
3. Double-click the scene you want to edit to open the scene editor.
4. Select  from the tool bar.

Configuring System Explorer to Display a Map

You can configure System Explorer to display a map of your choice.

To configure system explorer to display a map of your choice:

1. From the **System Configuration > System Objects** folder, double-click the System Explorer GUI and edit it.
2. Select the **guiSystemExplorer1** control from the drop-down list and update the following properties:
 - **Base location** – Select the location to appear as the top-most location in the tree of locations in System Explorer. See [Configuring a Location to appear as base location](#).
 - **Types to show** – Select devices and placeholders.
3. Select the **Location Selected** event in the **Events** drop-down list. The **Event** page opens.
4. Create a new variable called map and assign the map GUI to it.
5. From the **Basic Shapes** pallet, drag and drop a **Script** shape to the editor and add the following script:

```
My.PageVariables>.Map.sharpMapGISMap1.GotoLocation(My.PageVariables.Selected_Location)
```

6. From the **User Interface Shapes** palette, add a **Display Object** shape to the VRP and configure the following properties:
 - **Display Area** – System Main
 - **Show Objects** – GUI variable

- **Target Objects** – Current Generic Client variable
7. Add **Finish** shapes and save the System Explorer GUI.

Configuring Snapshots in Maps

You can take a snapshot of a map in Control Center, in the same way that you can take a snapshot of a video. This is useful if you want to send this snapshot to a third party or if the snapshot is required for reference, in another company's system, for example.

In **Enterprise Settings** there are options that allow you to configure how Control Center uses snapshots. To configure these options,

1. Go to **System > System Configuration**.
2. Select **Global Settings**.
3. From **Global Settings**, select **Enterprise Settings**.
4. Navigate to the snapshot options, as shown below:

Add Snapshot Information	<input type="checkbox"/>
Auto-enable PTZ Behavior	<input checked="" type="checkbox"/>
Enable Location Quotas	<input type="checkbox"/>
Enable Snapshot Editing	<input checked="" type="checkbox"/>
Snapshot Image format	Native
Snapshot Information Date-Time format	
Snapshot Information use client Local Time	<input type="checkbox"/>
Video Snapshot Path	%userprofile%\Documents\VIPSecurityCenter Snapshots

The following table describes how to configure the snapshot options.

Option	Description
Add Snapshot Information	Adds snapshot information to your snapshot. See Taking Snapshots From Maps
Auto-enable PTZ behavior	Only applies to snapshots taken of video.
Enable Location Quotas	Only applies to snapshots taken of video.
Enable Snapshot Editing	Enables you to edit your snapshot. See Taking Snapshots From Maps
Snapshot Image Format	Select one of the following: <ul style="list-style-type: none"> • Native • JPEG

	<ul style="list-style-type: none"> • PNG • BMP
Snapshot Information Date-Time format	See Snapshot Time Zone
Snapshot Information use client Local Time	See Snapshot Time Zone
Video Snapshot Path	Allows you to specify where to store your snapshots.

Get Viewing Objects for Object

Control Center includes a method to find cameras that can view a specific asset. This can for instance be used to locate nearby cameras to a door which has been forced. The functionality is available through a new response plan shape called Get Viewing Objects for Object.

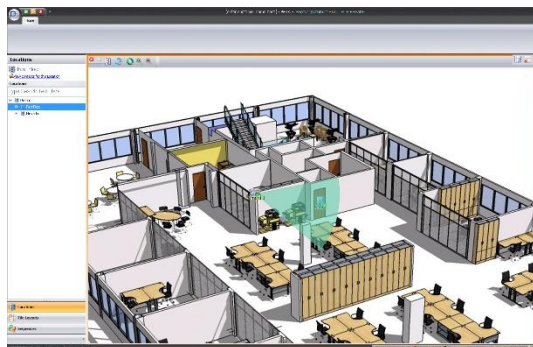
Before the shape can return any result, the assets must be plotted on a map and configured to detect viewing objects.

The following two methods can be used to detect viewing objects:

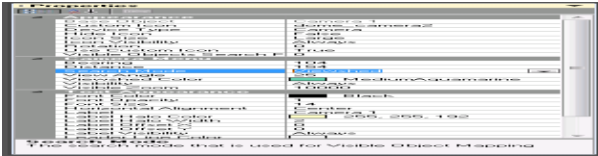
- **Viewshed**– This method returns all cameras within the view of a camera that covers the selected asset.
- **Radius** – This method returns all cameras within a specified radius of the selected asset.

To configure the logic:

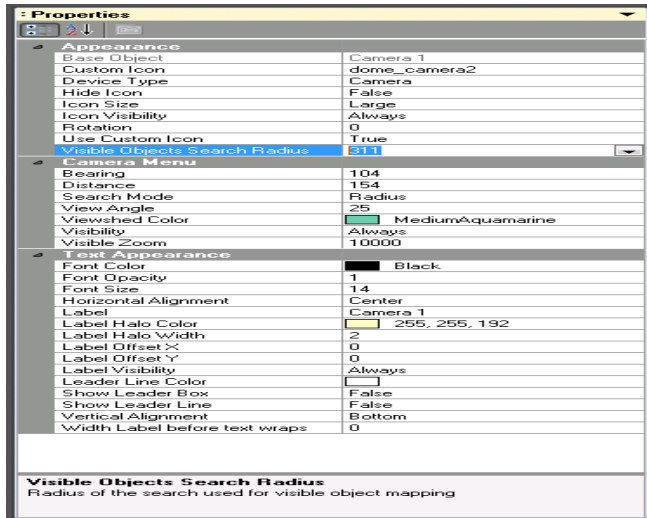
1. Double-click and open the **Scene** editor and plot an alarm point (a door in this example) and at least one camera.



2. Select the door asset to view its properties in the property grid.
3. Select **Search Mode**.

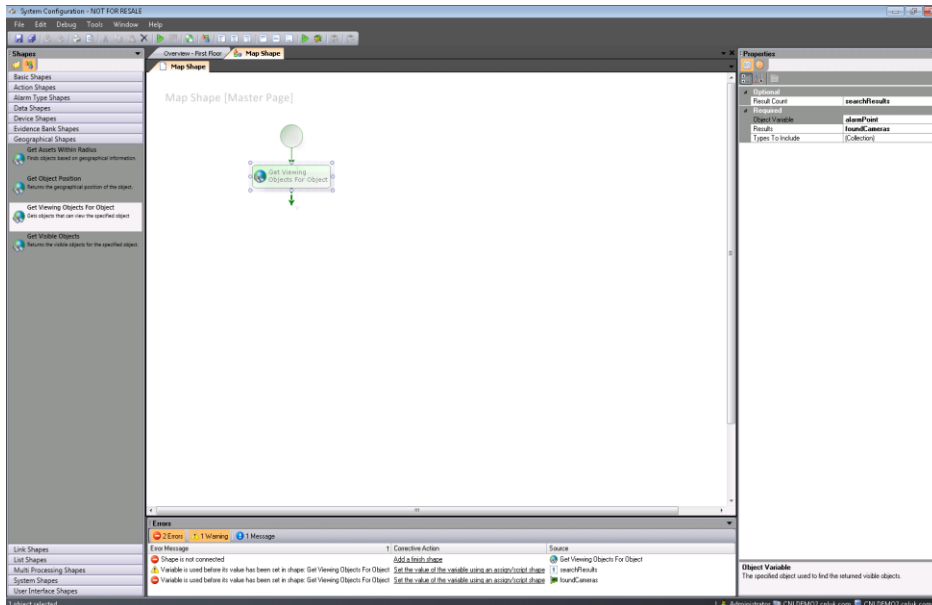


4. If the **Radius Search Mode** is used, specify the **Visible Object Search Radius**.

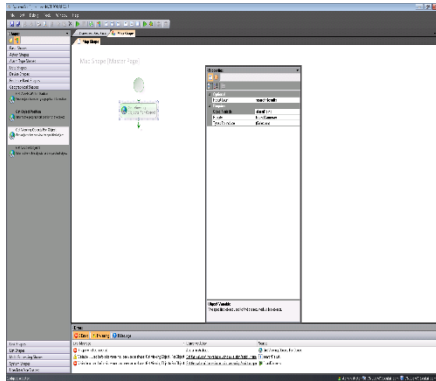


Radius on Schematic scenes is measured in pixels.

5. Save the scene. Create a response plan and add an **Object** variable. Make the variable Required.
6. Create a device variable and make it a **Basic List**.
7. Add a **Get Viewing Objects for Object** shape to the response plan.



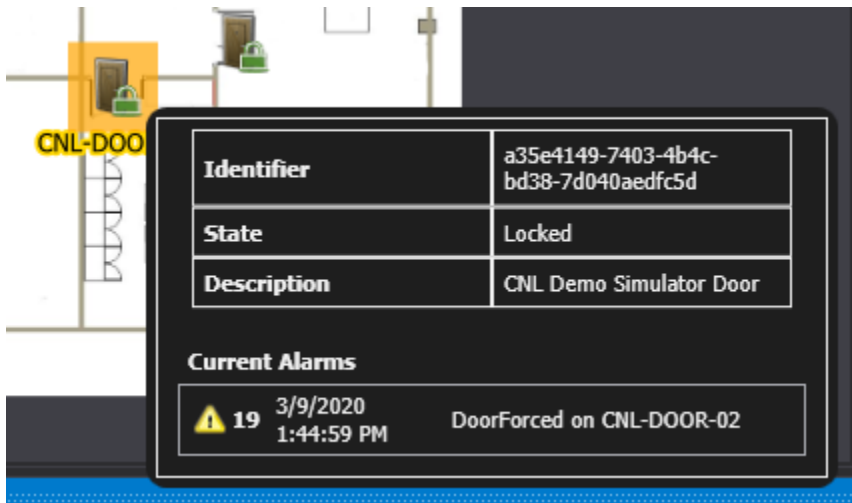
8. Select the shape to view its properties.



- 9. Set the **Object** variable to be the object passed into the response plan. Set the **Results** to point to the list of devices.
- 10. Optionally, create a **Whole Number** variable and set the **Result Count** to be the results variable.
- 11. Select the **Type To Include**. Only devices of the specified types will be returned by the shape.
- 12. The shape will return the cameras that are located within the view of the asset (door). To expand on this feature, utilize the **User Interface** shapes to display the cameras to the user.

Displaying Information About Objects on Maps

When hovering over an object on a map, you can configure Control Center to display information about that object in a tool tip. For example, the object’s status, alarms and location.



Tooltip annotations are created by default upon a new installation or upgrade of Control Center for:

- Device
- Location

The default tooltip displays:

- Label
- Description
- Extra State Info

You can configure the default tooltip template (or add a new one) from **System > System Configuration > Enterprise Settings > Global Settings > UI Configuration**. See [Enabling IPSecurityCenter Client Access to Tooltip Templates](#).

If you have configured your tooltip to display the Current Alarms property, the tooltip displays information about the latest 3 alarms for the object.

Note:

- You can only apply one tooltip at a time.
- If there is no value for a particular property, then the property is not displayed in the tooltip, even if that property has been configured to display in the tooltip template.
- If you have configured any theming for your Control Center client, then the tooltip uses the theming you have defined.
- If you have configured your tooltip to display the Extra State Information property then, if the Control Center Connection Service is not available, then the tooltip displays a message that informs the user that the Control Center Connection Service is not available.
- If no tooltip is configured, then nothing is displayed.

Configuring Map Object Interaction

You can add logic to the Map GUI to determine what happens when a user clicks or double-clicks a map object such as an icon or a feature. The following events are available:

Event	Available Metadata (Variables)
Asset Double Clicked	Selected Object
HotZone Double Clicked	Selected Object
Base Object Geometry Double Clicked	Selected Object

Event Object Double Clicked	Selected Object
Trail Clicked	Selected Object Track ID
Trail Double Clicked	Selected Object Track ID
Get Nearest Cameras Clicked	Camera Count Scene X Y
Slew to Cue Clicked	Slew to Cue Camera Track ID
Feature Clicked	AlarmID FeatureId FeatureLayerName
Feature Double Clicked	AlarmID FeatureId FeatureLayerName

The following steps detail how, for example, to set up logic to change the selected location on the System Explorer when the user double-clicks a location.

To configure asset interaction on maps:

1. Go to the **System Configuration > System Objects** folder and double-click the **Map GUI** to edit it.
2. Select the **SharpMap** control on the design surface.
3. Handle the **Asset Double-clicked** event by dropping down the **Events** drop-down list at the top of the GUI editor and selecting the **Asset Double-clicked** event.

A new event page will be created for the event with event specific variables detailing items such as the selected object.

As the selected object can be one of many different types, logic must be added into the event page to check if the selected object is a location.

4. Add a new page variable called **SelectedLocation** with the type location.

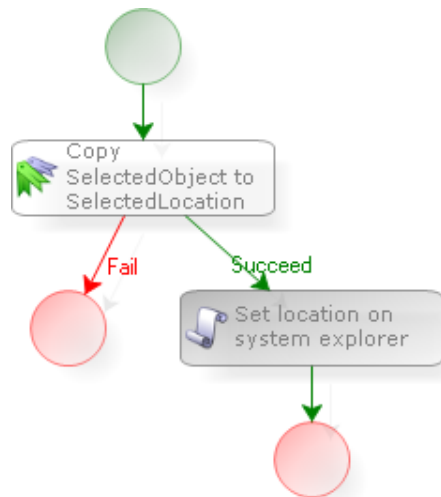
5. Add a **Copy Variable** shape and set the properties as follows:
 - **Source Variable** - SelectedObject
 - **Target Variable** - SelectedLocation

If successful, the shape will populate the SelectedLocation variable with the location held in the **SelectedObject** variable and then take the **Succeed** route otherwise **Fail** route will be taken which indicate that the **SelectedObject** references something other than a location

6. Add the **Finish** shape to the **Fail** route.
7. Add the **Script** shape to the Succeed route with the following script:

```
My.SystemVariables.[System Explorer].guiSystemExplorer1.[Current Location] =
My.PageVariables.SelectedLocation
```

8. Add the **Finish** shape to the script shape.




9. Save the GUI and select a new location from the System Explorer to show the updated map and then click an icon representing a location. The selected location of the System Explorer should be updated and in turn show the corresponding scene.

Tooltips

Creating a Tooltip Template

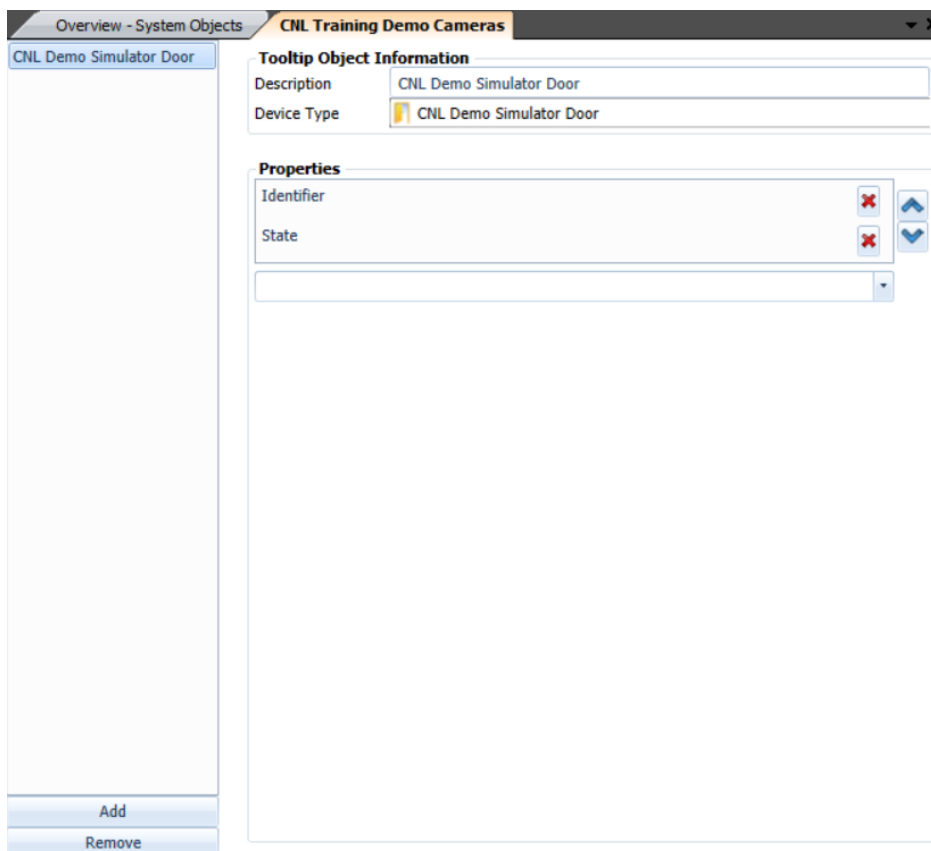
To do this:

1. Go to **System Configuration > Entire Enterprise > My Organization**.
2. Select **System Objects**. The **Overview** tab displays.
3. Right-click in the **Overview** tab and select **New > Tooltip Template**.
4. Enter a name for your tooltip template.

5. Double-click your tooltip template to configure it. The tooltip template tab displays.
6. Optionally, enter a description for your tooltip template.
7. From **Object Type**, select  to display the **Objects Type** dialog.

Repeat this step for each object type you want to configure a tooltip template for.

8. Select the devices that you want to provide tooltips for.
9. Select **OK** to close the **Objects Type** dialog.
10. From the **Properties** drop-down list, select a property that you want to display in the tooltip and press **Enter** to add that property to the **Properties** box. Repeat this step for all the properties you want to display in the tooltip. For information about the properties available for each object, see [Devices Section](#).
11. Use the arrows next to the **Properties** box to configure the order that you want the properties to display.
12. Use the **Add** and **Remove** buttons to add and remove tooltip templates, depending on your requirements.



You cannot remove the default **Tooltip Template**.

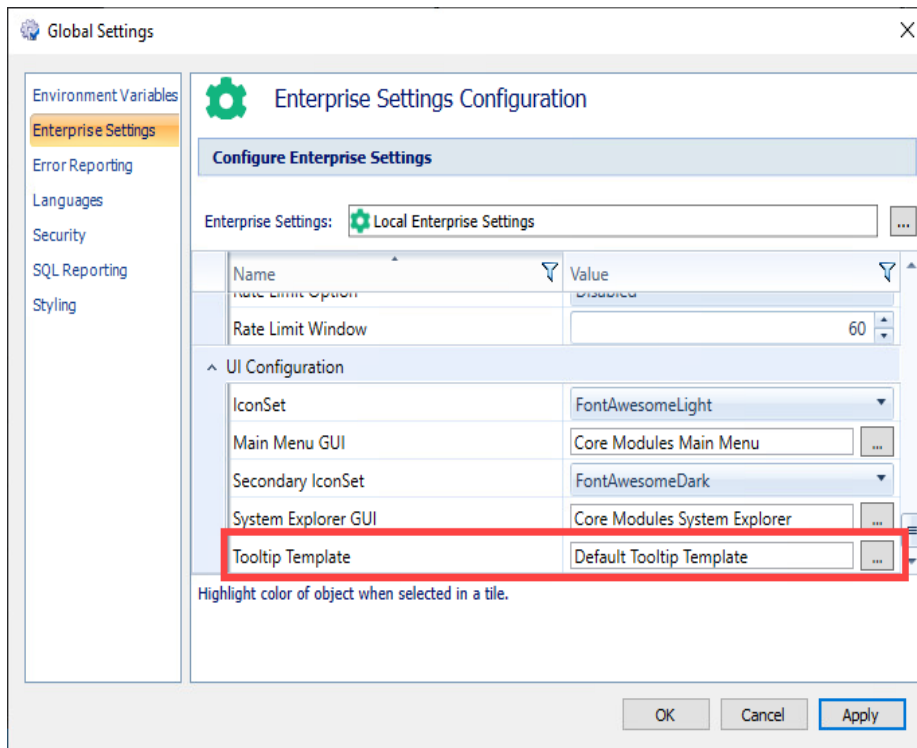
13. Save and close the tooltip template tab.
14. Enable your tooltip template in Global Settings, see [Enabling IPSecurityCenter Client Access to Tooltip Templates](#).
15. Log off and on again to apply the changes. When you hover over your object, your tooltip is displayed.

Enabling Control Center Client Access to Tooltip Templates

Only one tooltip template object can be applied at a time.

To enable your Control Center client access to tooltip templates:

1. From **System Configuration**, select **Global Settings > Enterprise Settings**.
2. Navigate to **UI Configuration**.
3. From **Tooltip Template**, select . The **Search Object** window displays.
4. Select **Find Now**. The available tooltip templates display.
5. Select the tooltip template that you want to grant access to and select **Apply**.



Configuring Permissions to Tooltips

You must have read access to a tooltip template object to see the tooltip template in Control Center. If you want to create a tooltip template object, you must have write permissions to tooltip templates.

You can restrict who has access to this feature using the Tooltip Template type permission. See [Type Permissions](#) for more information.

Map Shapes

Both schematic scenes and geographic scenes can be modified by the user to represent other objects in the system and to illustrate useful information to other users.

Depending on the type of shape, these are either added at runtime through the end-user interface or at design time in the system configuration window.

The following table lists the different objects types available and their associated functionality.

Shape Type	Availability	Description
Icon	System Configuration	Used to plot icons into the map surface to represent assets such as cameras or doors. Icons include a label for the associated object.
Hot Zone	System Configuration	Provides a circle, square or rectangle to represent any object in the system. This is typically used to draw an area on the map to represent a location to allow the user to navigate between locations.
Asset Geometry	System Configuration	Provides the ability to draw lines and polygons onto the map surface to represent objects in the system. This provides similar capabilities to a hot zone and would typically be used to draw a fence or more complex area with multiple points.
Map Labels	System Configuration	Provides the ability to add static labels to maps. The labels keep their size regardless of the zoom level.

Icons

Icons can be added to the map surface to represent system objects. These will typically be used to represent cameras and doors.



You can customize an icon's properties to determine its appearance and behavior:

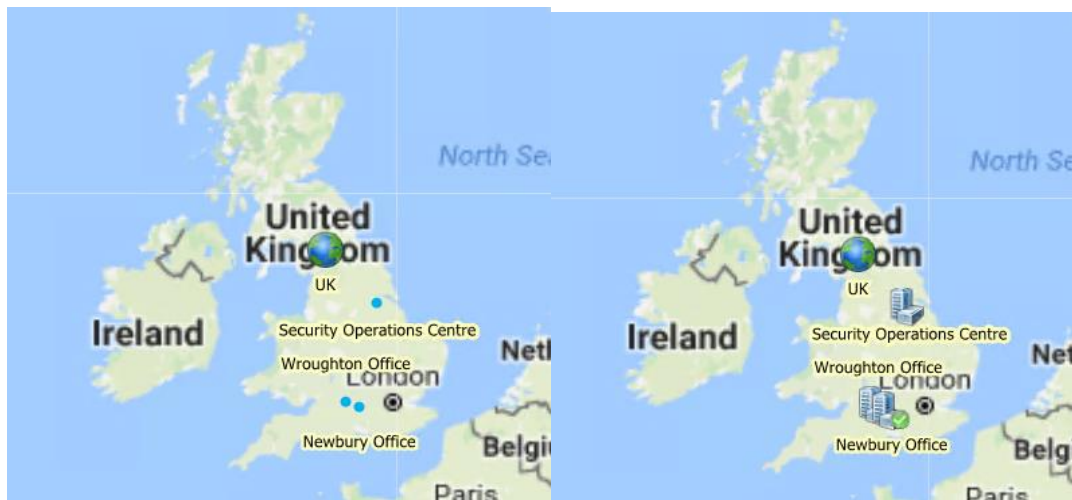
Custom Icon	Provides the ability to select a custom icon.
Device Type	Determines the type of object the icon represents. This property will be set automatically when adding the icon.
Hide Icon	Provides the ability to hide an icon. The icon will become visible if an Alert State is applied to it.
Icon Size	Determines the size of the icon on the map.
Icon Visibility	Determines the icon visibility on the map.
Rotation	Determines the rotation of the icon. By default, this is set to zero which indicates no rotation.
Use Custom Icon	Specifies if a custom icon should be used as specified in the Custom Icon property.
Visible Object Search Radius	Determines the radius in which to search for nearest assets when the Visible Object Search Mode property is set to Radius. For geographic scenes, the value will determine meters, for schematic scenes, the value will determine pixels.
Bearing	The bearing of the Viewshed property, which is the direction at which the camera is pointing in degrees (Latitude & Longitude). Where, 0 is north, 90 is east, 180 is south and 270 is west.

Distance	The distance of the Viewshed. On Geographical maps, this is 50 by default and on Schematic maps, it is set to 144, which can be changed.
Opacity	The opacity of the Viewshed on a scale of 0 to 1.
Search Mode	Determines the method by which to search for visible objects. This can be based on either the Viewshed or Radius.
View Angle	The width of the Viewshed in degrees on both sides from the center of the bearing. For example, if bearing is 90 and the view angle is 10, the view shed will cover an area of 20 degrees, which is 10 on each side of the bearing.
Viewshed Color	The color of the Viewshed, if applicable.
Visibility	The visibility of the Viewshed, if applicable.
Visible Zoom	The zoom level at which the Viewshed becomes visible, if applicable.
Font (Color, Opacity, Size)	The font properties of the asset label.
Horizontal Alignment	The horizontal alignment for the asset label. The options are: Left, Center, Right.
Label	The Label is pre-populated by the selected object but can be customized.
Label Halo (Color, Width)	The Label Halo creates an area of different color around the characters in a label to provide better visibility.
Label Offset	Determines the Offset of the asset label.
Label Visibility	Determines the Visibility of the asset label.
Leader Line Color	If the label is offset from the asset using the Offset properties, a leader line can connect the label with the asset. The Line Color property determines the color of the line.
Show Leader Line	If the label is offset from the asset using the Offset properties, a leader line can connect the label with the asset.

Show Leader Box	Determines if a line shall be painted around the label for greater visibility.
Vertical Alignment	Determines the vertical alignment of the label.
Width Label before text wraps	Determines if label text should be wrapped if longer than the specified width.

Location Dots

When visualizing multiple locations on a fixed size map, you can reduce the fixed size icon to a point on the map to control the zoom level point at which the transition occurs. Comparison of Location Dots (Left) with Location Icons (Right) is shown below.



The above figure illustrates the challenges of visualizing multiple sites close to each other on a map scene. The image on the right shows that the icons for Wroughton Office and Newbury Office overlap each other, and it is unclear where they are located.

As the icons are presented with an absolute size, the visibility deteriorates the further out of the map you zoom, and the map appears smaller, even though each icon stays the same size.

When the icon is replaced by a colored dot at the selected zoom point of the map, it improves the visualization of locations on the map especially where a large geographic area is covered.







Locations are assigned a color based upon the Location Type commissioned for that Location. This setting is available within the Location Property Grid and consists of a pre-defined list of Location Types.




Properties - (Security Operations Centre)

Address 2	
Address 3	
Country	
County	
Postal Code	
Postal Town	
Time Zone	
Contact	
Fax Number	
Internal Dialing Number	
Phone Number	
Radio Channel	
Details	
Default GUI	
Live Video Schedule	24 x 7 Allow
Location ID	
Location Type	Building
Manned Location	Other
Max Concurrent Connect	Country
Max Concurrent Exports	Region
Max Export Duration	Site
Max Export Filesize	Building
SLA Time	Floor
Video Export Schedule	Room
Video Playback Schedule	Zone
	Customer
General Settings	
Created	9/13/2016 2:34 PM

For each of the defined Location Types, Control Center specifies a default color to be used as the point color for that location on a map.

The following table lists the default colors for location types.

Location Type	Color	RGB / Hex
Other		113,51,155 / #71339B
Country		0,154,0 / #009A00
Region		102,51,0 / #663300
Site		255,102,0 / #FF6600
Building		0,176,240 / #00B0F0
Floor		0,0,0 / #000000

Room		127,127,127 / #7F7F7F
Zone		192,0,0 / #C00000
Customer		68,114,196 / #4472C4

The list of Location Types and the default colors for each type are not currently editable by users or commissioning engineers.

On a scene-by-scene basis, the user can change which colors are used for the Location Types using the Entity Layers Dialog on the scene.

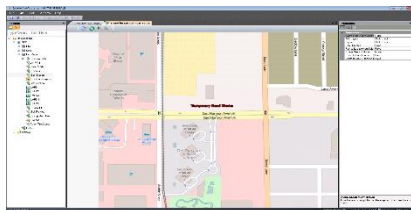
Alerting Location dots

When a Location is displayed as a Location dot, Alert States continue to be displayed against the Location. However, if the Location that is displayed as a Location dot, the Alert State Property icon is ignored while the Location is displayed as a dot. If the user returns to a zoom level where the icon for the Location would be displayed, the Alert State icon will appear. Note that this applies to Alarm Alert States and Manual Alert States.



Map Labels

You can add labels to a scene to add more descriptions to a map or floor plan.

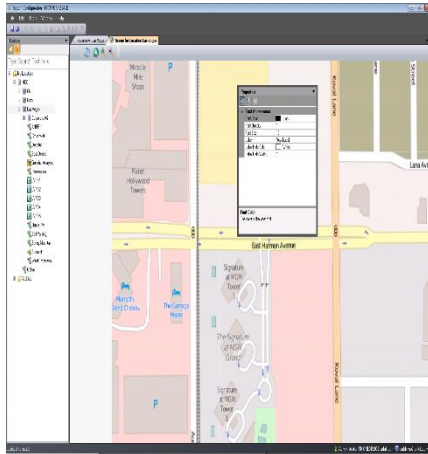


You can add a label in the same way as a Hot Zone or an Asset Geometry.

To add a Label, right-click on the scene and click **New > Label**.



Once a label is added, it can be configured using the properties in the property grid.



A label will persist its size through the zoom levels. That is, regardless of the zoom level, the label will always be of the same size.

In addition, the zoom feature in the Entity Layers dialog can be used to:

- Make sure the map is not cluttered when you zoom out.
- Adjust the zoom levels at which the labels should appear for a scene. To do this, click on the map surface and then select the Layers property in the property grid.
- Adjust the visible range for the labels layer using the slider.

Entity Types

Activate the Entity Layers Dialog

Entity Layers

Name	Visible	Visible Range	Point
Location:Other	<input checked="" type="checkbox"/>		Color selector for each location type on this scene
Location:Country	<input checked="" type="checkbox"/>		
Location:Region	<input checked="" type="checkbox"/>		
Location:Site	<input checked="" type="checkbox"/>		
Location:Building	<input checked="" type="checkbox"/>		
Location:Floor	<input checked="" type="checkbox"/>		
Location:Room	<input checked="" type="checkbox"/>		
Location:Zone	<input checked="" type="checkbox"/>		
Location:Customer	<input checked="" type="checkbox"/>		
Device:Camera	<input checked="" type="checkbox"/>		
Device:Door	<input checked="" type="checkbox"/>		
Device:Encoder	<input type="checkbox"/>		

Current Zoom: 634066.1

Zoom Controller

Overlay Layers

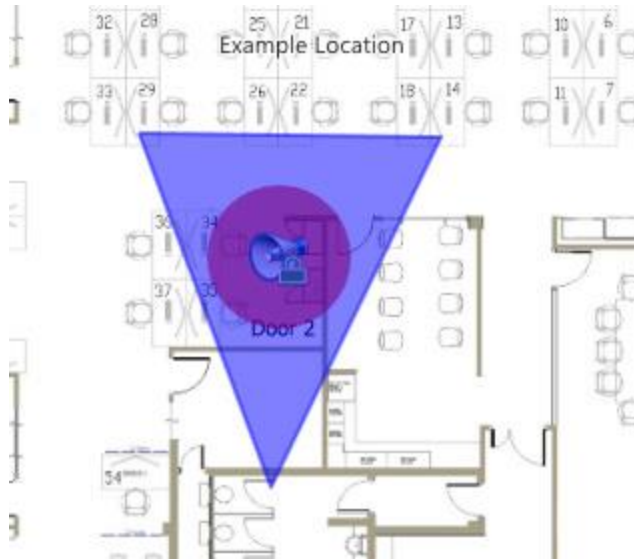
Name	Visible	Visible Range

Background Layer

OSM Layer

Using Map Annotations

You can draw shapes and add labels to geographic and schematic scenes in Control Center. Map annotations can be added from the map GUI and can be filtered on or off via the map filters. Map annotations are included in the map search results.



This is useful if you need to share a map with others in your organization and you want to highlight specific areas and provide more information about areas of interest on the map, like an oil spill, for example.

Map annotations are created on the scene and represented as an object in System Configuration in the same folder as the scene where you created the map annotation.

Note:

- In a federated system, you can see map annotations that have been created on remote sites. However, you cannot publish map annotations to remote sites.
- If you have created a map annotation, the map annotation is displayed on all Control Center clients connected to your Control Center server.
- By default, map annotations will appear above scene editor drawn shapes and lines but below assets and objects. This can be adjusted using Layer Configuration in the scene editor.


Map Annotation Permissions

You can use map annotations if you have, both:

- Permission to the map you want to add an annotation to.
- The Map Annotation type permission. See [Type Permissions](#) for more information.


Adding Annotations to Maps

To add an annotation to a map:

1. Go to the map GUI.
2. Select  from the toolbar.
3. From the drop-down list, select the type of annotation you want to create from the following options:
 1. **Label**
 2. **Line**
 3. **Polygon**
 4. **Rectangle**
 5. **Circle**
 6. **Cone**
4. Select the map where you want to place the annotation.

For **Label**, **Rectangle**, **Circle**, or **Cone** annotations this should be the center of the annotation.

For **Line** or **Polygon** annotations this should be the start of the annotation.

5. If you are creating a **Label** annotation, edit the text.
6. If you are creating a **Line** or **Polygon** annotation, select the map again where you want the next part of the line or polygon to be.
7. Select  to confirm the annotation.
8. Change the label for the annotation in the Map Annotation Properties window.
9. Select **Save** to save the shape.

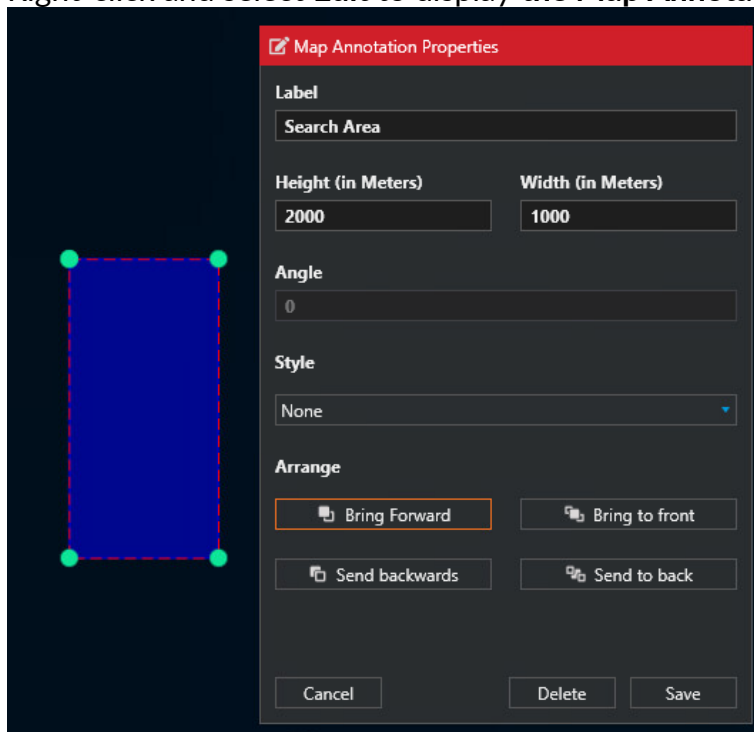
NOTE: You cannot adjust the rotation of the annotation while adding it. To change the rotation, follow the steps described in the Editing Map Annotations section below.

Editing Map Annotations

To edit an annotation on a map:

1. Go to the map GUI.
2. Select the map annotation you want to edit.


- Right-click and select **Edit** to display the **Map Annotation Properties** window:



While the Map Annotation Properties window is open you can:

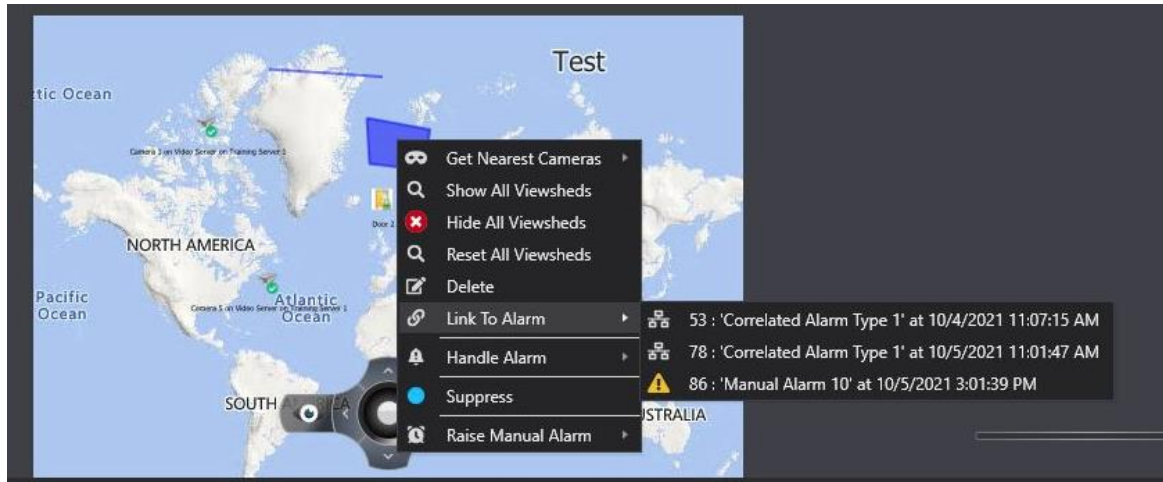
- Move the annotation around the map by clicking and dragging it.
- Change the **Label**
- Adjust the size and shape of the annotation by clicking and dragging any of the green dots, or by changing the **Height**, **Width**, and **Diameter** properties.

NOTE: You cannot change the number of points on an existing Line or Polygon annotation. If you need to make such changes, you must delete the existing annotation and add a new line or polygon to the map.

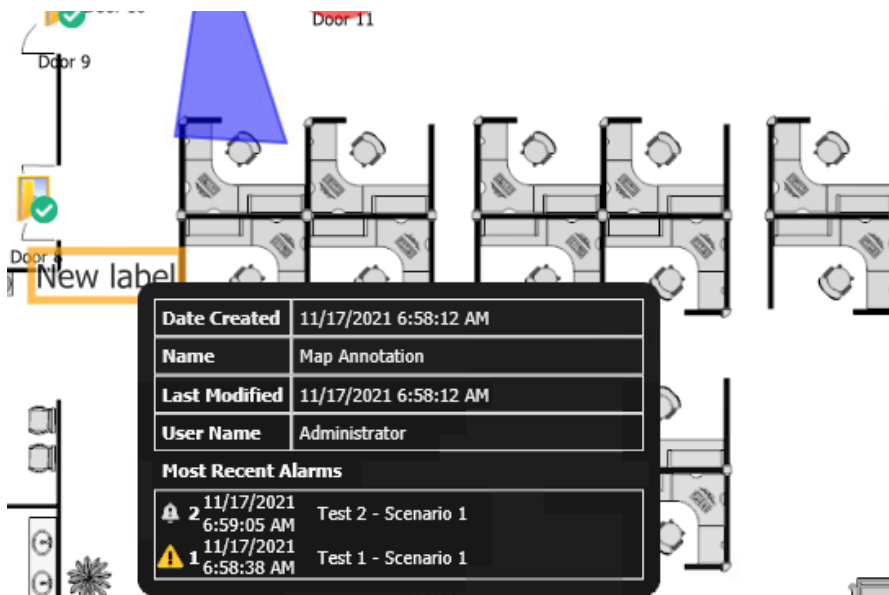
- Adjust the angle of the annotation by clicking the rotate icon  and moving the mouse. To fix the new angle, click the map outside of the annotation.
 - Assign a pre-configured **Style** to change the appearance of the annotation. See [Object Style Templates](#) for details on how to create a new style.
 - Arrange the position of the annotation within the map layers using the **Bring Forward** and **Send backwards** buttons.
 - Delete the shape using the **Delete** button.
- Select **Save** to save the changes made to the annotation.

Linking Alarms to Map Annotations

You can link alarms to map annotations. This is useful if you have an ongoing alarm, and you want to draw attention to the area affected by the alarm for others in your organization.



When an alarm is linked to a map annotation, the alarm details are displayed in a tooltip. The last 3 alarms raised on any object, device or annotation are displayed. A maximum of 3 alarms are displayed. The alarms you have access to depends on your alarm permissions. See [Type Permissions](#).



You can handle an alarm from a linked annotation. See [Handling Alarms](#).

Deleting Annotations from Maps

To delete an annotation from a map:

5. Go to the map GUI.
6. Select the annotation you want to delete.
7. Right-click and select **Delete**.

Show or Hide Viewsheds

You can show or hide device coverage area by showing and hiding the coverage area for one or more devices.

The context menu supports a universal option for viewshed display on all 2D schematic and GIS scenes. The context menu shows the following options, in addition to the appropriate operator actions and the context menu controls that appear when you right-click on a 2D scene.



The context menu options change, depending on the actions you select. For example, if you select **Hide a Viewshed** and the viewshed is hidden, then **Show Viewshed** context menu option appears.

Note that the default state of the viewshed visibility will not change from how it has been set in the properties for a scene. That is, when the scene is opened and closed and then re-opened, the viewshed visibility reverts to the commissioned defaults.

Get Nearest Cameras

You can get the nearest cameras mapped on scenes using the **Get Nearest Cameras** option in the context menu. For a schematic scene, the calculation is based on simple geometric distance from the point clicked on the map. In a GIS scene, an absolute distance can be calculated based on the distance units for the map.


Taking Snapshots From Maps

You can take a snapshot of a map in Control Center, in the same way that you can take a snapshot of a video. (See [Snapshots From Video](#)). This is useful if you want to send a snapshot to a third party or if the snapshot is required in another company's system, for example.

As well as taking a snapshot, you can also change the snapshots appearance. For example, you can highlight areas of the map, add text, resize the snapshot or add effects.


The snapshot can be:

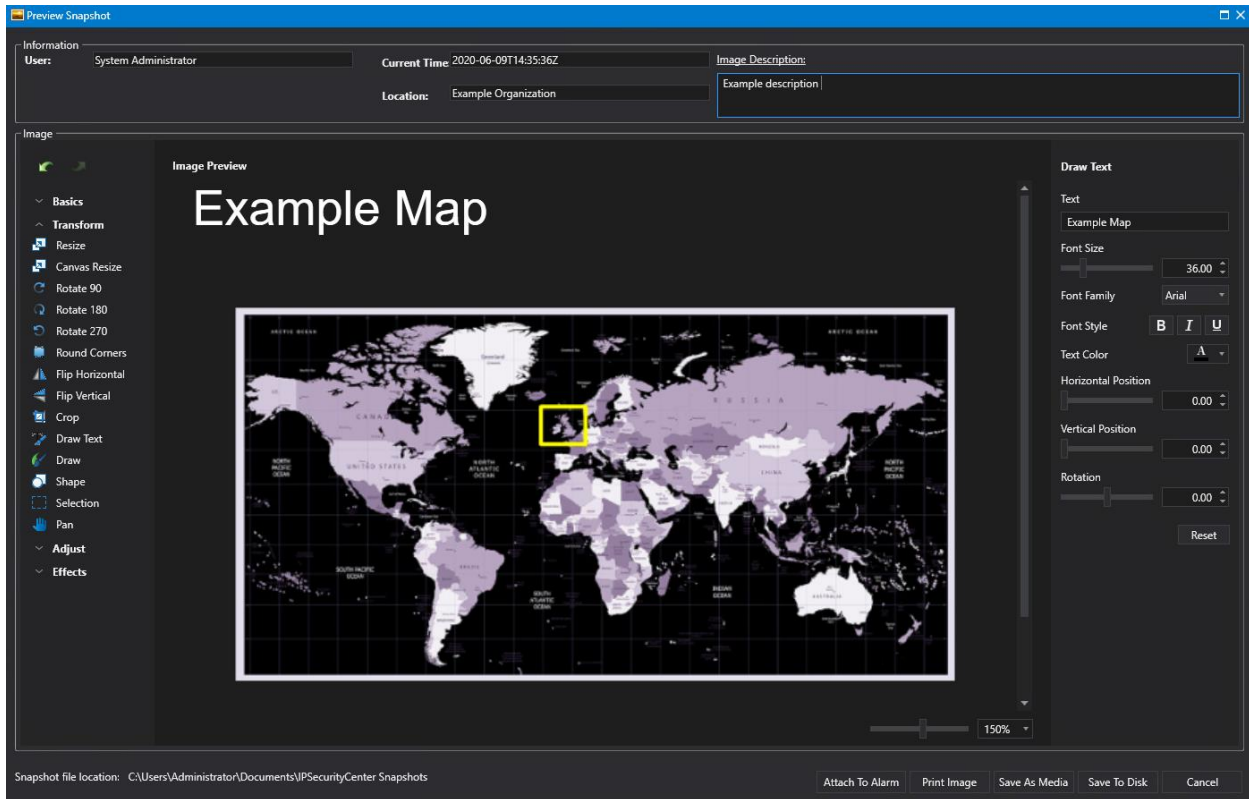
- saved to disk
- saved as a media file in Control Center
- attached to an alarm

The options that are available to you when you select , depend on how your Control Center Administrator has configured how snapshots can be used in Control Center. This means that you may not have some of the options described below. See [Configuring Snapshots in Maps](#).

To take a snapshot from a map:



1. From **System Main**, select . The **Preview Snapshot** dialog displays. The **Information** panel displays:
 - **Username** of the user who created the snapshot
 - **Current Time** the snapshot was created
 - **Location** in Control Center where the snapshot was taken.
2. Optionally, add an **Image Description** for the snapshot.
3. Use the tools in the **Image** panel, to make any changes required to the snapshot.



4. Select **Snapshot File Location** to browse to the location where you want to save the file.
5. Select one of the following:

Option	Description
<p>Attach to Alarm</p>	<p>Attach the snapshot to the alarm that is currently being handled. Attach to Alarm is only available if you are handling an alarm in Control Center.</p> <p>The snapshot is saved in the System Configuration > System Objects > Alarm Media folder. In a federated system, once the snapshot is saved as a media object, you can publish it to other sites in your federated system, if required.</p> <p>If you have process guidance configured, you will see Map Snapshot or Camera Snapshot in the alarm activity grid when you are completing the alarm resolution form.</p> <p>Notes:</p>

	<ul style="list-style-type: none"> ○ You can attach multiple images to the same alarm as long as the alarm is in a handled state by your current user. ○ You cannot have more than one alarm handled by the same user in Control Center. ○ The snapshot is saved to the [Alarms].[AlarmActivity] table in the Control Center database.
Print Image	Print the snapshot.
Save As Media	<p>Save the snapshot as a media object in Control Center</p> <p>. When a snapshot is saved as a media object, it is stored in System Configuration > User Objects > Snapshots folder. For federated node sites, snapshots stored with the user objects folder are federated to any configured hub.</p>
Save to Disk	<p>Save the snapshot to the location you specified in Snapshot File Location</p> <p>. See Configuring Snapshots in Maps</p> <p>.</p>
Cancel	Close the Snapshot Preview dialog without saving the snapshot.

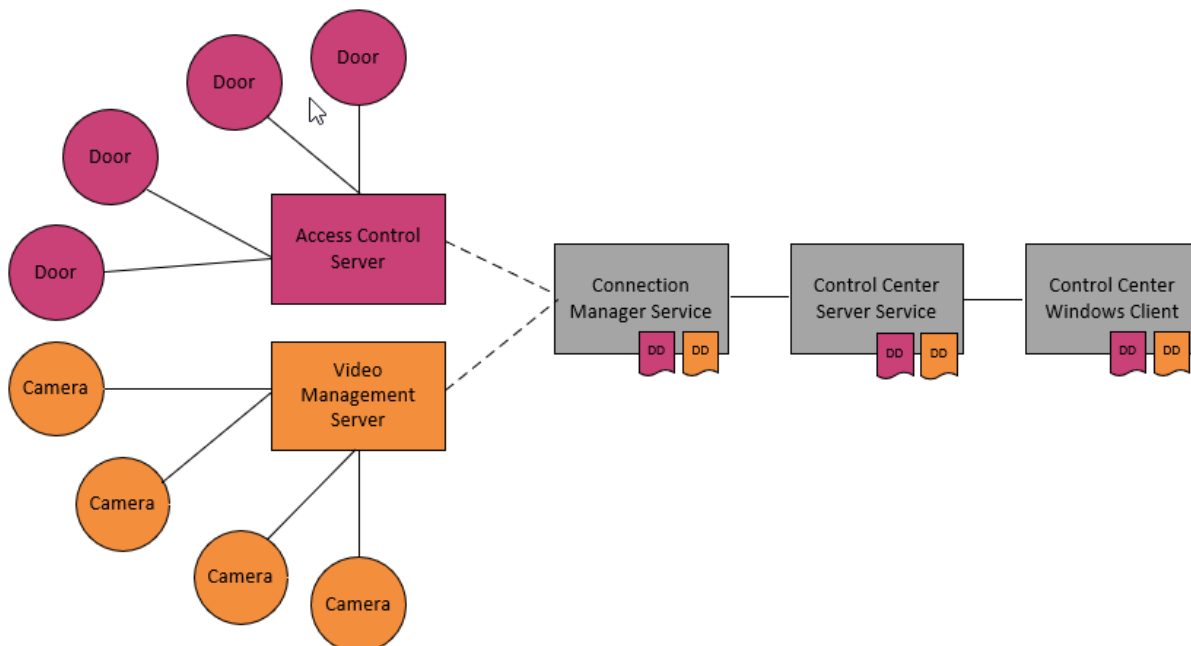
Devices & Extensions

Devices in Control Center are used to represent physical systems as objects within the solution. Objects added to represent devices can then be used through the solution to provide interaction with the available devices.

For example, a device might be added into the solution to represent a video management server and then multiple connected devices can be added to represent the cameras. The cameras can then be represented on the available maps as icons, dragged out to view video, controlled by the user to view recorded video, used in a video export job to archive recorded video to disk, etc.

As well as user interaction, logic within the solution can also be configured to interact with the available devices. For example, the Alarm Types service could be configured to create an alarm when an event is received from a device, or a response plan could be configured to automatically PTZ a camera when a user handles an alarm.

Connectivity to the available sub-systems is achieved using different Control Center components with the addition of device connector packages which are written specifically for the different types of devices to be connected.



Understanding Device Connectivity

Devices are used in Control Center to represent physical systems inside Control Center. Each type of device which is connected to Control Center requires a specific device connector written to encapsulate functionality exposed in the manufacturer SDK. The

Control Center device connector then enables a device of that type to be added and configured in Control Center.

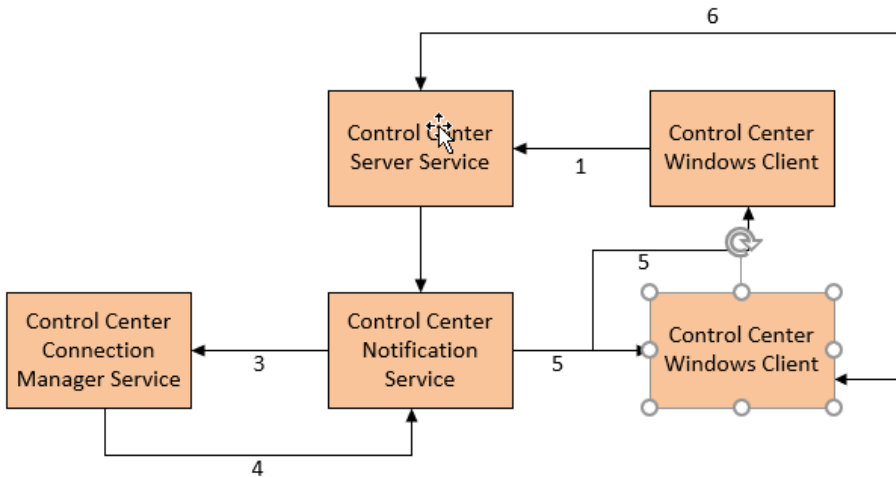
The following diagram shows how communication to the various sub-systems is achieved using a series of Control Center components with the inclusion of device connectors for the relevant sub-systems (marked as DD for device connector).

Using the device connector, the Connection Manager communicates with the different sub-systems which, in turn, communicate back to the Control Center Server which, then, communicates with the Control Center Clients.

Device Connector Loading Process

Before a device is added into a solution, the corresponding device connector must first be installed using the System Configuration window.

The diagram below details the process for installing device connectors into a Control Center solution.



1. The device connector is installed using in **Connectors & Extensions** in **System Configuration** window. The connector package is then sent to the Server service.
2. The Server service receives and loads the newly installed device connector and then informs the Notification service of the update.
3. The Notification service then notifies the Connection Manager that a new device connector is available for download.
4. Once the Connection Manager has downloaded the new device connector, it instructs the Notification service that the new connector is loaded and ready for use.
5. The Notification service then notifies all clients in the solution that a new connector has been loaded.
6. Any clients without a copy of the new device connector then download the new connector from the Server service.

Connectors also support specifying custom state change event times as well as other events to support reporting of sub-system time in Alarms and Alarm reporting.

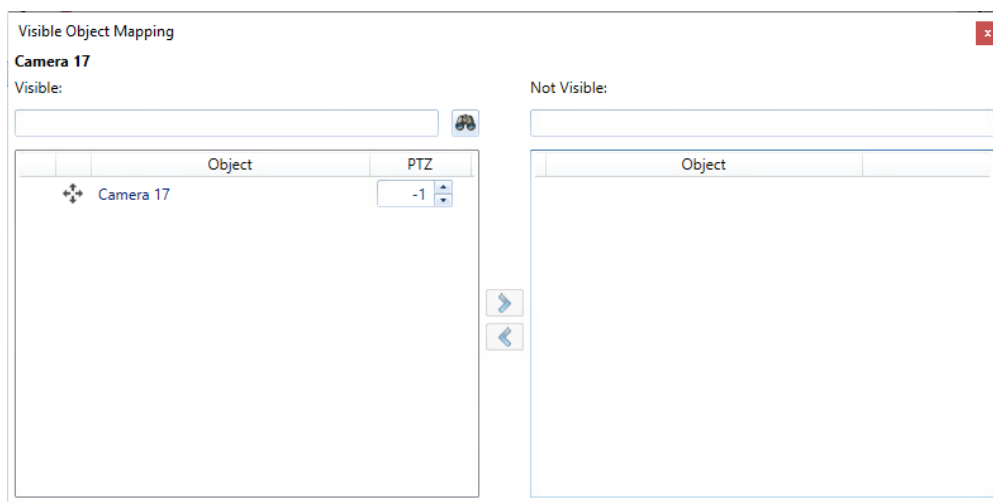
PTZ Presets and Visible Object Mapping

You can set PTZ Preset values for a device using the Visible Objects Mapping dialog. Presets refer to the preset camera configurations of PTZ cameras. PTZ (pan, tilt, and zoom) reflects the movement options of a camera. Using the Visible Object Mapping

dialog, you can configure the objects that should be visible from a camera device on a scene.

To edit the PTZ Preset value:

1. From the **System Configuration** window, select the device or location for which you want to edit the PTZ Preset value for.
2. In the **Properties** section, click the **Visible Objects** button. The **Visible Object Mapping** dialog appears.
3. In the **Visible** section, click the binoculars to search for visible objects. The search results with the available objects.



4. Select the object for which you want to reassign the PTZ value and edit it. For example, the above figure shows that to view Door 11, Camera 4 on Video Server on Training Server should use PTZ Preset 4.

The PTZ column supports integers as well as the value -1 to indicate that the camera cannot be moved to any PTZ preset value. This can be used for devices that do not support PTZ.

Alternatively, you can also use the Get Viewing Objects for Object shape to retrieve a list of objects that are viewable by the selected device including the PTZ preset value corresponding to each device.

Permissions-aware PTZ Pre-set

In Control Center, administrators can apply security permissions to PTZ Preset settings so that users have permission only to interact with resources in single or multiple groups. That is, you can allow control over which users are able to create and save new PTZ Presets on cameras that support PTZ. The PTZ permissions can be defined at a folder level or an individual device level. When the permissions are defined at the folder level, all devices that are part of the selected folder hierarchy will follow the same permissions.

In addition, administrators can specify which users can save the new PTZ presets and the cameras the user cannot recall PTZ presets. By default, all users can create new PTZ presets set on a device.

Configuring PTZ User Permissions

You configure PTZ User Permissions in System Configuration either at the folder level or device level.

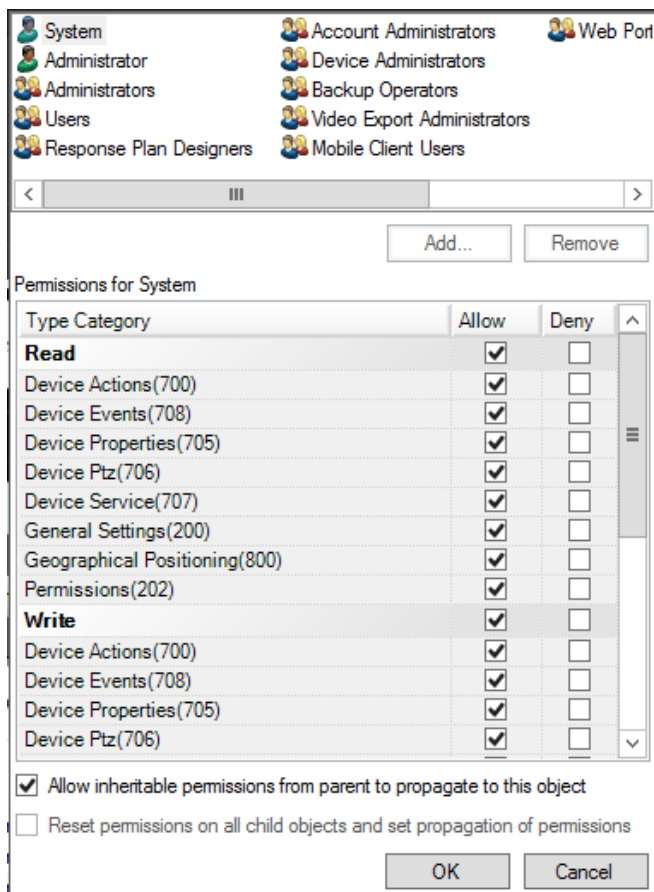
Prerequisites:

Before configuring the PTZ permissions, ensure that:

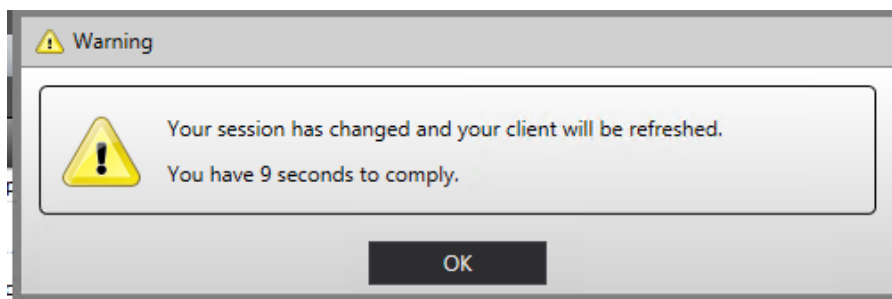
- A PTZ camera is configured and displayed on a tile layout.
- The device supports PTZ and preset.
- The PTZ and Preset settings are enabled, that is, set to True in Properties.
- The Allow Tile menu option is enabled for the display area from Setup Display.
- At least a few users and user groups are defined in the system.

To configure PTZ user Read and Write permissions:

1. In **System Configuration**, select a device. The **Device Details** window appears.
2. From **Properties**, click **Security Settings**. The **Security Settings** dialog appears.



3. If already checked, clear the **Allow inheritable permissions** from parent to propagate to this object check box to make changes to the read and write permissions.
4. In the **Permissions** for the system > **Read** section, scroll down to the Device PTZ option and select it.
5. In the **Write** permissions of the system section, scroll down to select the DevicePTZ option and select it.
6. A warning message displaying the Time Count is displayed. Click **OK** or wait for 20 seconds. The window disappears, and the changes take effect.



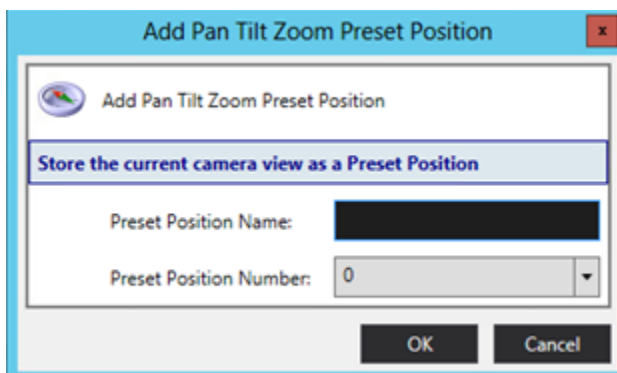
7. Navigate to the tile windows where the PTZ camera is being displayed. Notice the new options on the toolbar that appears.



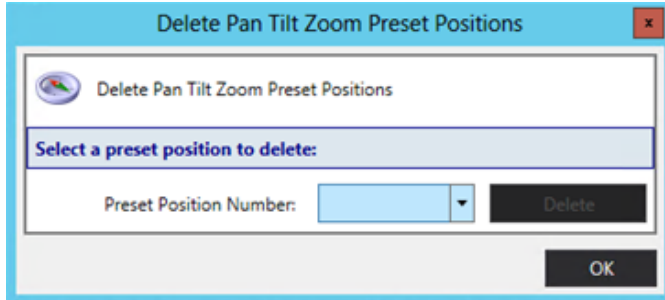
8. Click on the **Preset** icon to populate the options. Note that these options will not be populated if you set the PTZ permissions to read-only for a user in the Security Settings dialog.



9. Click **Set Preset**. A new dialog box appears to select the predefined PTZ Preset position for the selected device.



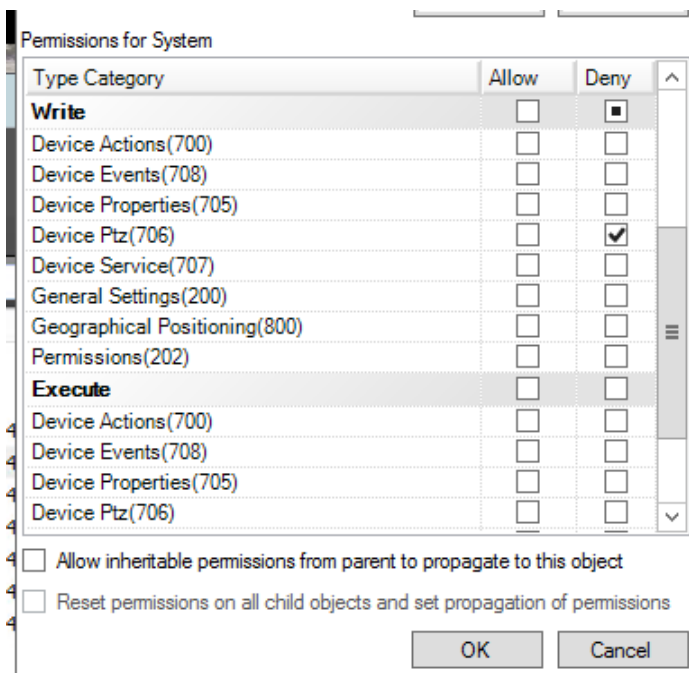
10. Specify the Preset Position Name and **Preset Position Number**.
11. Click **OK**. The new preset should appear in the list of Presets.
12. To delete a preset, select the **Delete Preset** option from the toolbar that appears.



13. Select the **Preset Position Number** that you wish to delete from the drop-down list and click OK.

To deny user permissions for a PTZ camera:

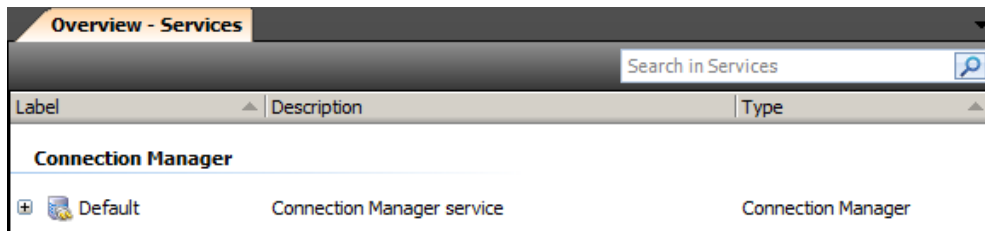
1. In **System Configuration**, select a device. The **Device Details** window appears.
2. From **Properties**, click **Security Settings**. The **Security Settings** dialog appears.
3. If already checked, clear the **Allow inheritable permissions** from parent to propagate to this object check box to make changes to the read and write permissions.
4. In the **Permissions** for the **System** > **Write** permissions section, scroll down to the **Device PTZ** option and select **Deny**.



5. Click **OK**. The changes are applied to the PTZ settings in the tile layout.
6. Check the **Tile layout** and notice the Set Preset and **Delete Preset** options do not appear anymore.

Loading Connection Managers

The Control Center Connection Managers are automatically loaded into the Services folder when the service is started. The installer will configure the Connection Manager with the location of the Control Center Server. Once both the Connection Manager and Server services are running, the Connection will automatically add a record for itself as shown below.

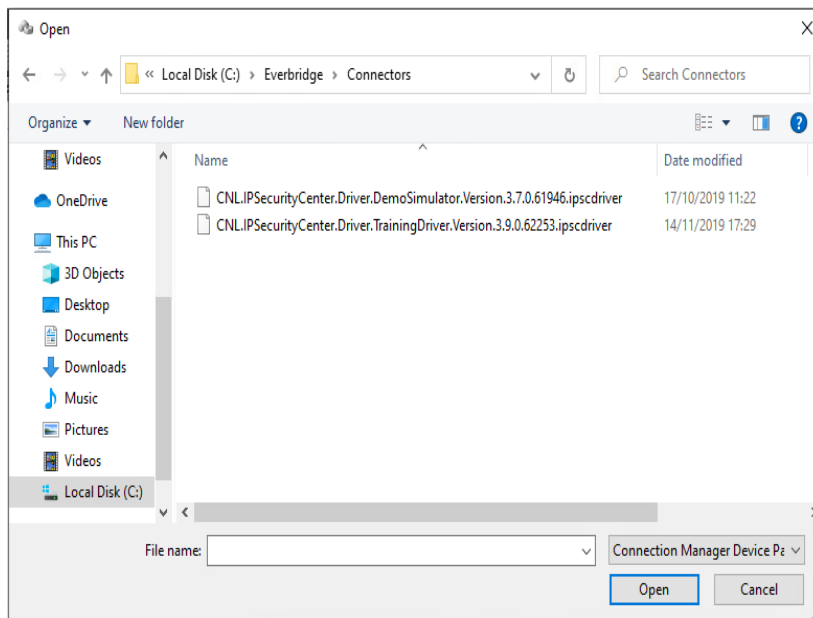


Installing a Device Connector

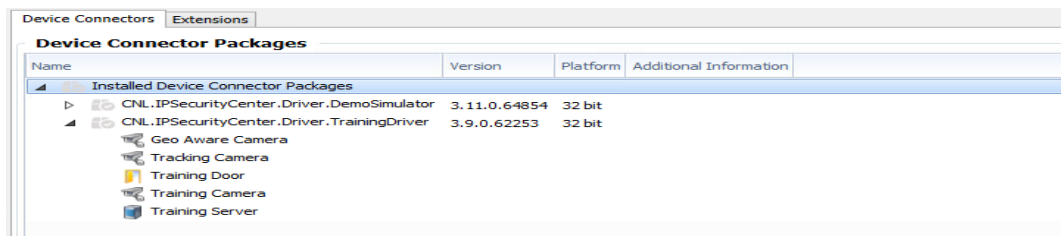
Device connectors can be loaded into a solution using **Connectors & Extensions in System Configuration**.

To load a single device connector:

1. Open the **System Configuration** window and on the toolbar, click **Connectors & Extensions**.
2. Click **Install**.
3. Navigate to the .ipscdriver file and then click **Open**. The device connector is loaded and then shown within **Device Connectors**.



- Expanding the connector package shows the different types of devices available within the package; for example, the *TrainingVideoServer* package contains information for both the Training Server and the Training Camera.



Adding Devices

Once the Connection Manager is running and the device connector is loaded, a device can be added into the solution. Typically, the parent device for example, a video management server (VMS)) is added first, which then automatically adds all the child devices (for example, all cameras connected to the VMS).

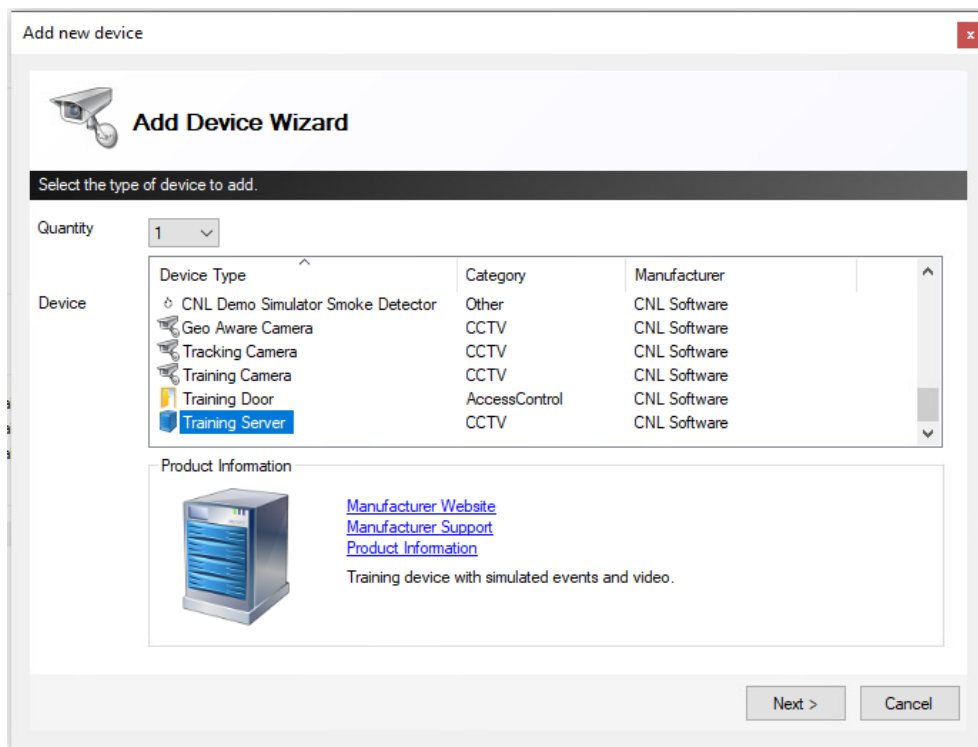
Devices can be added via the context menu or via a connection manager. All devices must be associated with a Connection Manager, therefore when adding a device using the context menu a connection manager must be specified.

To add a single device (using training server as an example):

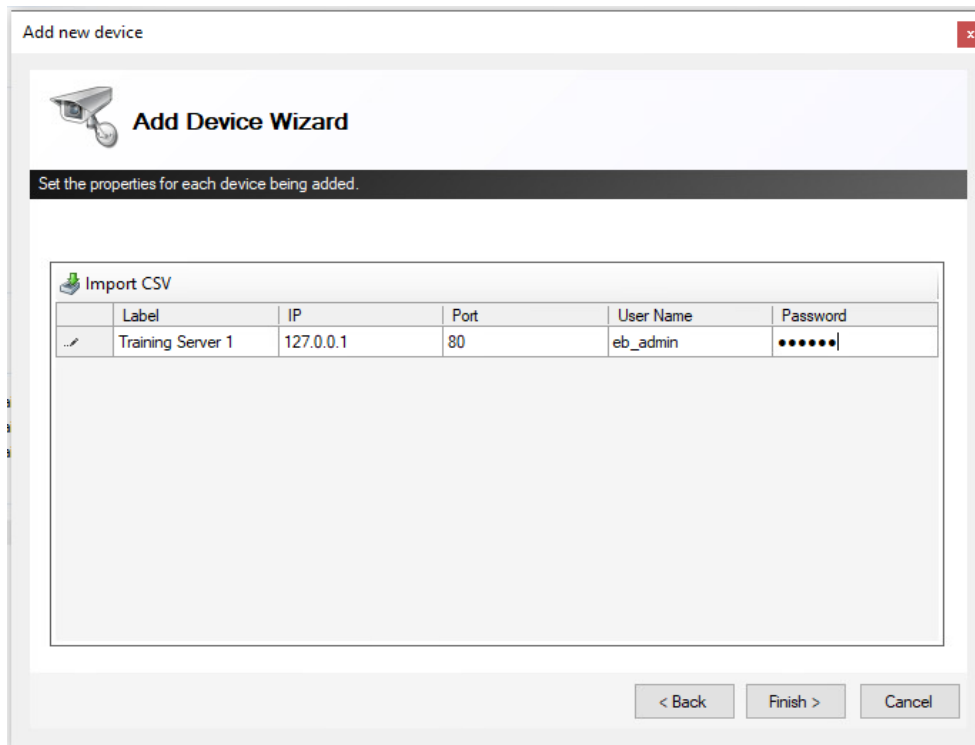
- Open the **System Configuration** window.
- Open the **Add Device Wizard** using one of the following methods:

The **Add Device Wizard** appears.

- In the **Overview** pane, right-click a **Connection Manager** and click **Add Device**.
 - Right-click anywhere in the **Overview – System Objects** tab and click **New > Device On > Connection Manager**.
- Click **Start** to continue.
 - On the **Select the type of device to add** page, select the **Training Server** device type and then click **Next** to continue.



5. Enter the details for the device, then click **Finish** to add the device. In the following example, the connection details are taken from the training server RDIN , however these details would differ from user to user.



6. Enable the device by setting the **Enabled property** to **True** in the property grid or by right-clicking the device and clicking **Enable**. This will initialize the device and add any connected devices.

You can also enable and rename the devices, if required.

Devices must always be enabled for it to raise events. Care must be taken to enable all devices that needs to be monitored by the Control Center, as disabled devices do not raise any events.

Training Camera

- + Camera 1 on Video Server on Training Server 1
- + Camera 2 on Video Server on Training Server 1
- + Camera 3 on Video Server on Training Server 1
- + Camera 4 on Video Server on Training Server 1
- + Camera 5 on Video Server on Training Server 1
- + Camera 6 on Video Server on Training Server 1
- + Camera 7 on Video Server on Training Server 1
- + Camera 8 on Video Server on Training Server 1
- + Camera 9 on Video Server on Training Server 1

Training Server

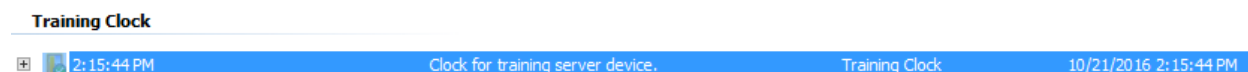
- + Training Server 1

Folders should be used to contain related objects to provide a logical system structure. Create the required folders for new devices and drag the newly created devices into them.

Device Connector Control of Device Label

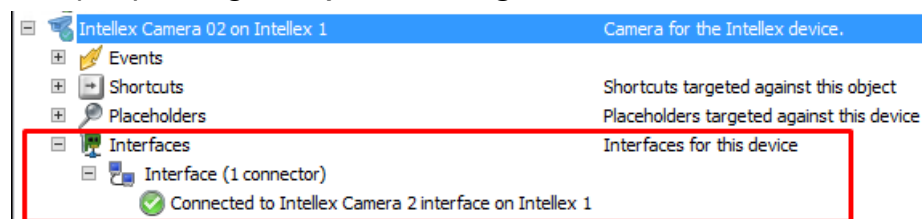
From DDK 3.1 onwards, the underlying sub-system allows changing of the label on a device in Control Center. This also prevents the users from modifying the device label in Control Center.

To test this feature, use the device called Training Clock in the Training Server Device Connector.



Ability to Determine a Parent Device

You can determine the parent object to which the camera or any other device belongs to, by expanding the **System Configuration > Device Name > Interfaces** section.



Connector Version Compatibility

From Control Center 5.2 onwards, connectors compiled for DDK 3.0 and DDK 3.1 co-exist on a single system. This functionality is supported such that connectors compiled against an earlier version of the DDK can co-exist with connectors compiled against a later version.

This support is limited to situations where the major versions of the DDKs are the same. For example, DDK 3.1 and DDK 3.0 connectors will work, but DDK 3.1 and DDK 2.4 connectors will not work.

Viewing Extensions

In **Connector & Extensions**, you can view the different extensions currently installed within Control Center. An **Extensions** tab allows you to determine what extensions are supported within Control Center and distinguish between the extensions that contain proprietary software developed by a third-party. For example, if a third party extension is being used in Control Center, it lists the name of the vendor in the details section.

1. Open the **System Configuration** window and on the toolbar, click **Connectors & Extensions**. The **Device Connectors** page appears.

- Click the **Extensions** tab. The extensions are displayed along with the package and type information. The **Extensions** section also lists any additional dependencies below the extension type.

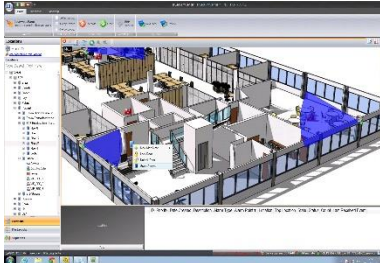
Device Connectors		Extensions		
Extensions				
Name	Version	Author	Additional Information	
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; align-items: center;"> ▲ Installed Extensions </div> <div style="margin-left: 20px;"> <p>By Extension Package</p> <ul style="list-style-type: none"> ▶ Client Themes 5.31.0.0 CNL Software Ltd ▶ Dashboards 5.31.0.0 CNL Software Ltd ▶ DataSourcesBuiltIn 5.31.0.0 CNL Software Ltd ▶ HotKeys 5.31.0.0 CNL Software Ltd ▶ InfoView 5.31.0.0 CNL Software Ltd ▶ InfoView 5.31.0.0 CNL Software Ltd ▶ Instant Messenger 2.13.0.0 CNL Software Ltd ▶ MobileClient 5.31.0.0 CNL Software Ltd ▶ Object Style Template 5.31.0.0 CNL Software Ltd ▶ SiteReferences 5.31.0.0 CNL Software Ltd ▶ System 5.31.0.0 CNL Software Ltd ▶ Themed Controls 5.31.0.0 CNL Software Ltd ▶ TimeBarAlarms 5.31.0.0 CNL Software Ltd ▶ TimebarEvents 5.31.0.0 CNL Software Ltd ▶ TimeBarVideoExport 5.31.0.0 CNL Software Ltd ▶ TimeBarVideoLoop 5.31.0.0 CNL Software Ltd ▶ TypePermissions 5.31.0.0 CNL Software Ltd ▶ WindowsClientTemplate 5.31.0.0 CNL Software Ltd <p>By Extension Type</p> <ul style="list-style-type: none"> ▶ Add-on Object ▶ Add-on Property Extender ▶ Add-on User Interface ▶ Client Action ▶ Client Manager ▶ Data Source ▶ Data Source Designer ▶ GUI Plugin ▶ User Interface Designer ▶ Video Extension </div> </div>				

The same dialog is used for installing and configuring device connectors in Control Center.

Operator Actions

Asset types can expose pre-configured actions. For instance, a door asset might have a function to provide access.

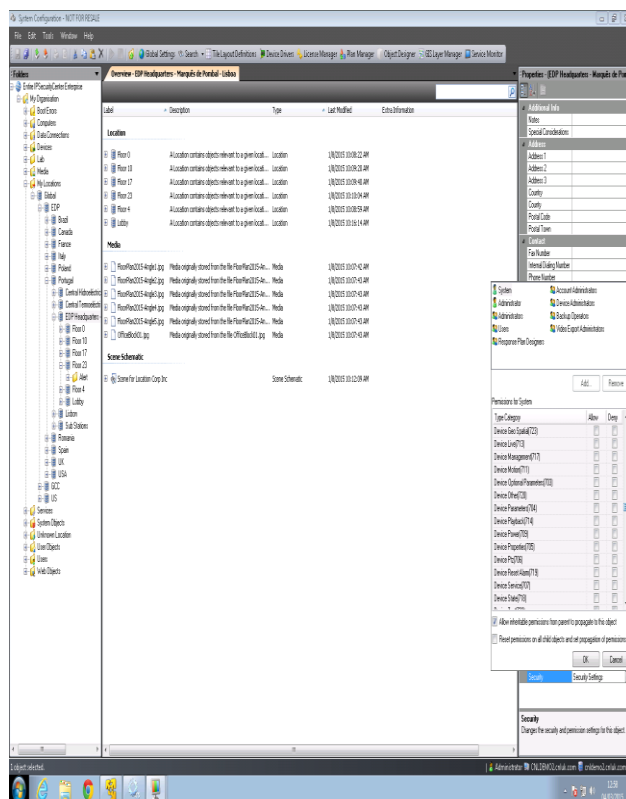
To access Operator actions, right-click an asset on the map surface or alternatively, in System Explorer, right-click a device and select the Operator actions.



The options available in the Operator Actions are determined by the connector configured in the system. Refer to the respective connector documentation to find out what the available Operator Actions for the selected connector are.

Setting Permissions on Operator Actions

Permissions can be used to restrict which users and groups can execute specific actions. To set permissions for Operator Actions, select the Location where the asset resides and then **Properties**> **Security**.



Radar and Video Monitoring System

The Radar and video monitoring system is an integrated feature offered by Control Center to receive and display Radar information such as tracks, geofences, long range video and associated data within the application. It is an easy to use solution for receiving Radar information and displaying it on the map and processing the events that are being generated, to create alarms. Control Center is ideal for taking information from any Radar Subsystem and connected cameras for representing and processing within the Control Center which makes it suitable for use in distributed architectures.

The geofences and tracks from the Radar device can be displayed in a multi layered map interface and the video feed from the connected cameras can be displayed on single display window or a tiled layout to be able to monitor multiple tracks at the same time. Any camera can be chosen to be displayed on the tile layout for a live feed or can be played back from the recording for monitoring purposes.

In addition to displaying the tracks on a map, you can also classify the tracks by various criteria. By default, three classifications Friend, Foe and Unknown are made available within Control Center when you create a Trail point Layer. Additional classifications can also be created by the administrator.

Geofences, which are a virtual perimeter of the actual geographic boundary, can also be represented on the map. Geofences can be predefined on a map in a connected

subsystem that can then be imported to be used within the Control Center. Furthermore, alarms can be created from events that gets triggered when an object encroaches certain defined areas.

A Slew to Cue functionality has also been implemented that allows the target object to be selected and automatically followed using the nearest camera available.

Radar Architecture and Functioning

The architecture diagram shown below is a visual representation of how the Radar and Video monitoring system works seamlessly within Control Center.

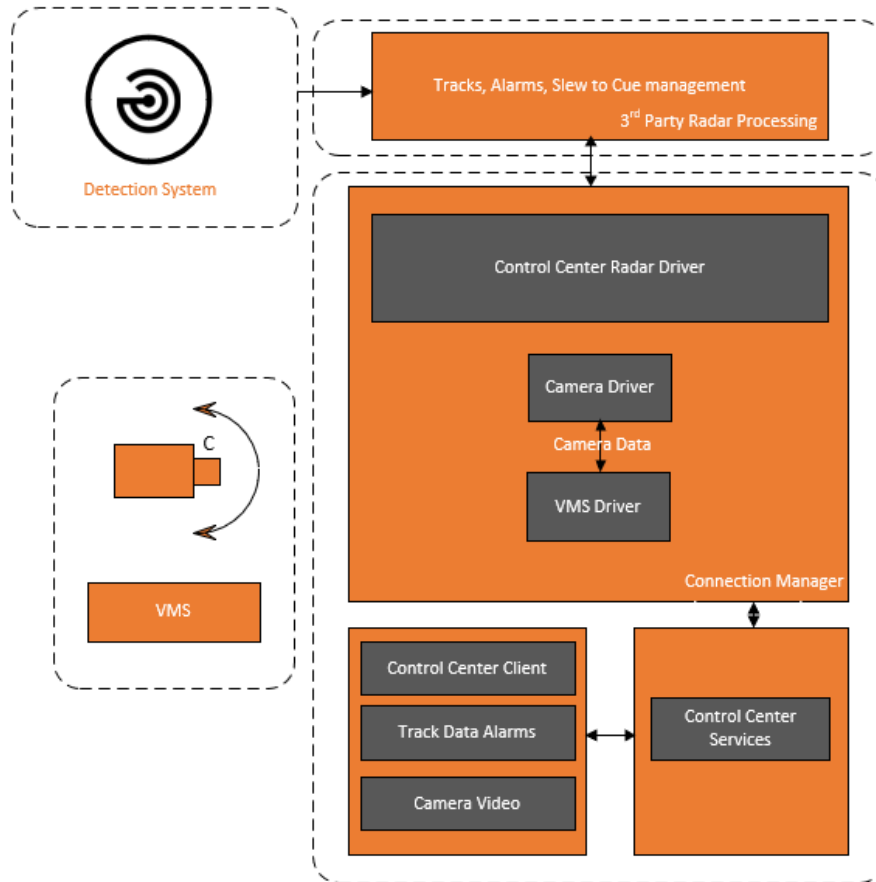
The Radar subsystem consists of one or more Radar devices which feed the radar information to the Radar Server. The data received is sent to the third-party Radar processor which then shares the information with the Connection Manager of Control Center to filter out the events triggered by the third-party processing unit.

Control Center Radar connector extracts the track and geofences information to be plotted on the map within the client application.

The third-party interface must be a passable platform which allows the user to create geofences and export it to be used within Control Center. It also needs to correlate with the track information received from the Radar device and trigger events which is then directed down into Control Center for creation of necessary alarms. The events that can be configured for various scenarios are as shown in the example below:

- Object Entering or Leaving the Geofence; for instance, when an object enters or leaves a defined area.
- Object Loitering around the Geofence; when an object has not remained in the actual perimeter of the geofence far too long.
- Object Approaching the Geofence; an object is moving in the direction of the geofence and is about to enter it.
- Device state changed: This event is raised when the online state of the device changes
- Crossed: The track has crossed the geofence area before the radar scan the area again.

When configurations are changed in the third party interface, the information is passed on to the Control Center Radar Connector and successively to Control Center to be used within the application.



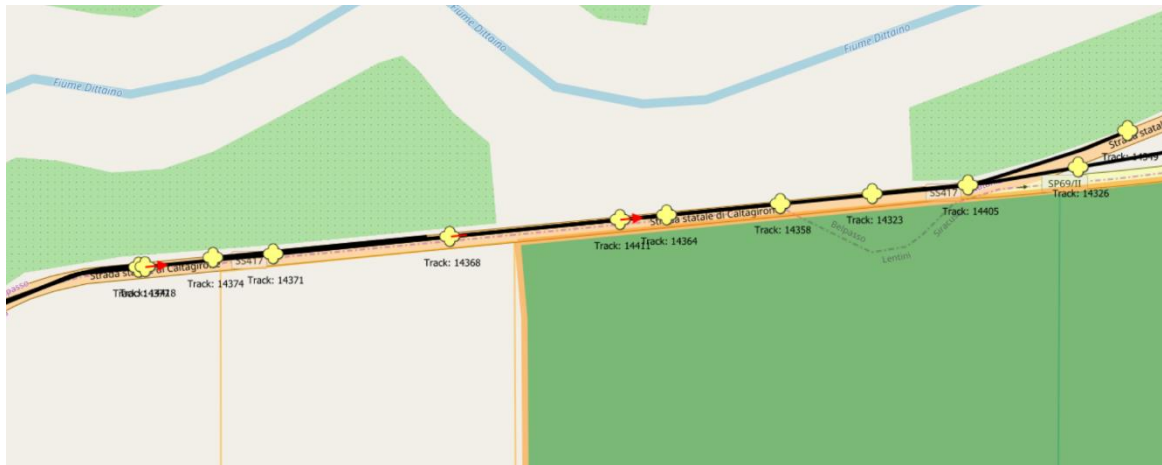
The Slew to Cue is controlled by the third-party Radar Processor and is kicked off when the Slew to Cue clicked event is triggered from a response plan configured within the client application. The Radar Processor will provide continuous updates about the polar co-ordinates of the target to the camera connector so that the camera can position itself and follow the target more closely.

The Video from cameras can be received through multiple interfaces either directly from a digital camera or through an encoder or via a VMS into Control Center. The video can be played live on a display area or played back from the recordings for the time chosen.

The Slew-to-Cue is executed by a third-party radar processor when an action is triggered from Control Center through a response plan. The manual control of the camera can be executed either directly against a camera or via a VMS. The manual command to the camera will always override the Slew to Cue action.

Track Display

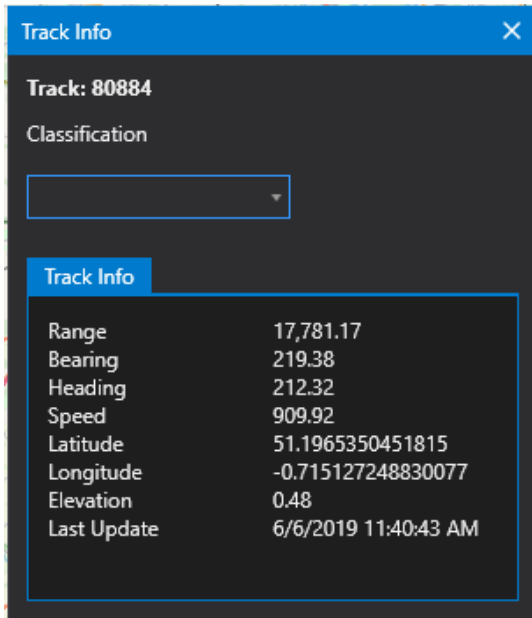
A classic radar surveillance device detects objects in its range and reports its polar co-ordinates to the radar server at regular intervals which is usually every few seconds.



Typically, the radar information will carry the following information:

- Unique track Id
- Speed of the object
- Heading
- Position of the object [Longitude and Latitude of the current position of the object]

A track for an object detected is established by the radar tracker by taking continuous updates of the same object from the radar system at regular intervals and plotting them on the map. A separate track is created for each target found within the range of the device. Upon clicking on a track, Track Info window opens up to display all information about the track. Note that the newly formed track will have no classification assigned to it and hence is displayed blank. By clicking on the down arrow of the classification field you will be able to see the available classifications for you to choose from. By default, there are three classifications; Friend, Foe and Unknown provided within the Control Center. The administrator can create more classification if requirement arises.



Upon selection, the classification for the track will dynamically be applied and can be seen on the map.

If any changes are made to the classification on the GIS Layer Manager, it will instantly reflect in the Track info window, but will not be dynamically applied on the map. You will have to unassign the current classification and reassign for it show up in the map.

There are two events made available in the map GUI:

- Trail Clicked
- Trail Double Clicked

A response plan can be configured to perform set actions when these any of these events occur.

Filtering the Track Events

Events from all devices within Control Center are gathered by the Connection Manager, filtered and passed on to the Rules engine for being used in collation of events and creating the alarms.

There are two events of interest which needs to be handled with caution.

- **TraceUpdated Event** This event is kicked off every time the device receives an update on the position of the target (which is approximately every second). If there are 50 tracks on the map and each triggering off an event every second will flood the Rules engine with loads of events which are deemed as futile and never going to be part of any alarm.
- **Orientation Changed Event** This event is initiated each time the camera is moved to follow the target object during the slew to cue action

These events are large in number and will essentially slow down other critical events trying to come through that needs to be addressed swiftly.

In order to address this issue, a filtering mechanism can be implemented in the connection manager to filter all the unnecessary events from reaching the rules engine. This is not automated at the moment and needs to be customized.

To set the filters for the events, do the following:

1. Go to **System Configuration > Services**
2. Double click on the **Connection Manager** service to open the **Device Events** window
3. Double click on one of the **TraceUpdated Event** or **Orientation Changed Event** to open the **Event Filter** window. The window will be populated with all the event details for the selected event.

Event Filter

Event Event Data

Connection Manager Reset Clear

Device Reset Clear

Device Type Reset Clear

Event Name Reset Clear

OK Cancel

4. Validate the entries and click **OK**.
5. A filter will be created which can be seen by clicking on the **Filters** option in the toolbar and selecting **Show All Filters**.

Event Filters

<input type="checkbox"/>	Connection Manager	Device Type	Device	Event	Properties
<input type="checkbox"/>	Default	DemoRadar	DemoRadar 1	TraceUpdatedEvent	0

Delete OK

Once the filter has been applied the events start to filter out from being passed on to the Rules Engine which are clearly marked with Red as shown in the figure below.

Events before filtering

	6/4/2019 2:46:16 PM	DemoRadar	DemoRadar 1	TraceUpdatedEvent	1
	6/4/2019 2:46:16 PM	DemoRadar	DemoRadar 1	TraceUpdatedEvent	1

Events after the filter has been applied

	6/4/2019 2:46:39 PM	DemoRadar	DemoRadar 1	TraceUpdatedEvent	1
	6/4/2019 2:46:39 PM	DemoRadar	DemoRadar 1	TraceUpdatedEvent	1

This will remarkably reduce the overhead on the Rules engine giving way for other critical events to take precedence.

Geofences

A Geofence is a virtual perimeter of the actual geographic boundary, drawn on the map that enables the application to trigger an event when an object enters or leaves a defined area. Geofences are defined in a connected subsystem and is imported into Control Center by the connector to be rendered on the map. A Geofence is rendered on the map by creating a separate Geofence Layer.

Bing Maps Layer

Geofences Layer

Geofences Layer line

OSM Layer

Radar layer

Trail Points Layer

WMS Map Layer

Layer Type Geofences

Layer Name

This layer enables the configuration of displaying geofence assets within IPSecurityCenter. This requires that IPSecurityCenter version 5.10 or later is running on all installations that Federate with this system.

Device

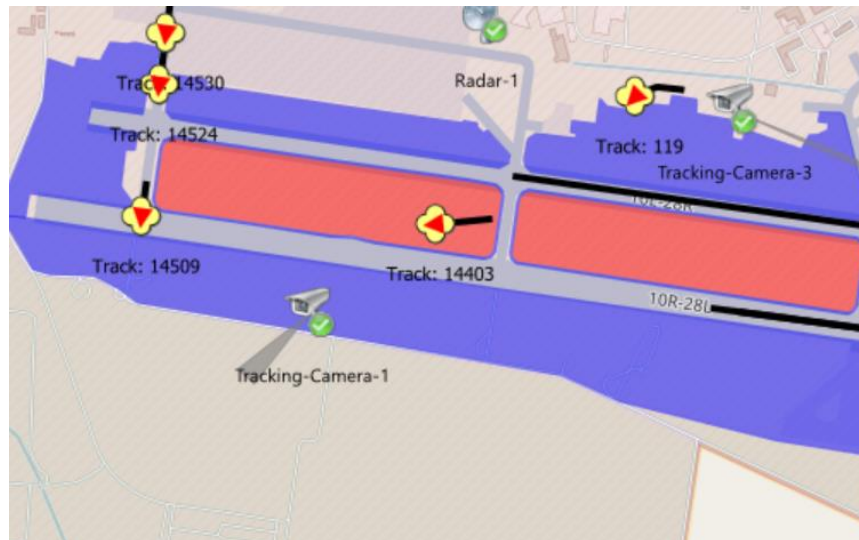
Device Type ...

Devices to Display Select All Geofence Devices

Style

Disabled Device Opacity

Styling Template ...



Each of the blue circular area defines a geofence. Geofences can be of three types:

1. Geofence area: Area can have three different shapes
 - Square
 - Round
 - Rectangle
2. Geofence Line
3. Geofence Point

Geofence is a Control Center Version 5.10 onwards only. In a federated environment if the NOC is running a client of version 5.10 and is publishing the GIS layer Manager to all sites which are on version 5.10 or older, all layers will be published as normal except the Geofence layer.

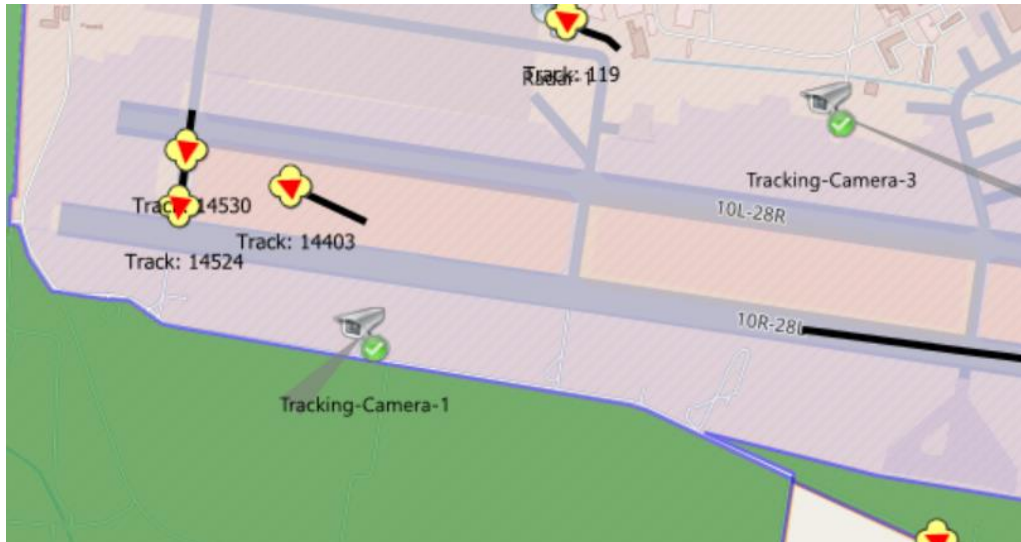
From Version 5.10 onwards the Trail Point Layer includes the classification details for tracks rendered on the map. In a federated environment when the central hub is publishing the GIS Layer Manager, the classification details will be blocked, while other details are published as normal.

Disabled Geofences

Geofences can be disabled temporarily and the area defined for the Geofence can be ceased from being monitored for the duration chosen in the Date Time schedule or until it is enabled. The disabled Geofence can either be shown as normal, made transparent to distinguish from the enabled ones or completely hidden from the map. A Style field called Disabled Device Opacity in the Geofence layer which when set to 100% will show the Geofence as normal and on set to 0% will completely hide from the map.



Sliding to a number in between will make it transparent to the level selected.



Geofences can also be customized by creating a style and applying it to the Geofence by selecting the style template here.

Events Triggering the Alarms

There are several events available to be included within an alarm type for creating alarms. The Geofence is an area of interest and any object or person intruding the area, needs to be monitored and relevant alarms raised to alert the security personnel.

Geofence-1	A geofence configured to represent an area within the GIS Tracking System	GIS Geofence
Events		
Approach	Track is approaching the zone	
Breach	Track has entered the geofenced area	
Crossed	Track has crossed the geofenced area	
Device State Changed	Raised when the online state of a device changes.	
Exit	Track has exited the geofence area	
Loiter	The track has remained within a given zone for too long	

Styling of Geofences


Geofence can be styled to increase visual appeal and enhance user experience. You can also distinguish between Geofences by styling them differently based on their threat levels so that the operator knows which ones to concentrate on for monitoring.

Applying Style for Geofences

Please see the [Object Style Template](#) section for details of how to create a styling template if you do not already have one configured.

To apply a style to a Geofence, do the following:

1. Go to **System Configuration** and click on **GIS Layer Manager** in the tool bar to open the **Layer Manager Window**
2. Select the **Geofence Layer** you want to apply the styling on.

3. Click on the  button against the **Styling Template** to select the template for the chosen layer.
4. Save the **Layer Manager**.
5. Refresh the scene to view the applied changes.

Date Time Schedule for Geofences

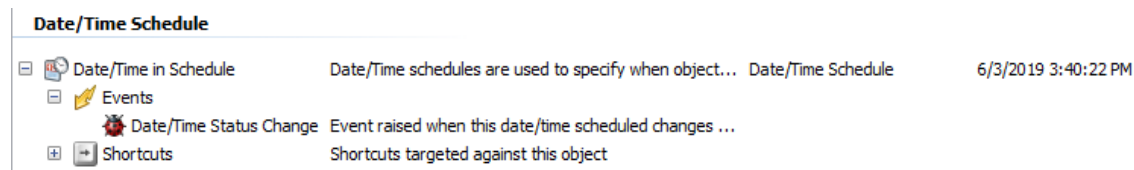
Monitoring of Geofences can be made easy by supervising only the critical areas at the time it is needed and hiding the rest from the scene. The display of the Geofences on the scene can be automated by scheduling the date and time for it to be in the enabled state and setting the Opacity accordingly.

In scenarios where, certain areas can be excluded from being monitored during certain time of the day/night as it poses little or no risk can be programmed in the Date Time Schedule Object.

Setting Date Time Schedule

To Set the Date Time Schedule for a Geofence, do the following:

1. Go to **System Configuration > System Objects**.
2. Right click in the center pane and select **New > Date Time Schedule**. A new **Date Time Schedule** object is created.
3. Double click on the object to open the **Date Time Schedule Window**.
4. Select the time interval you want the Geofence to be enabled for. For example: 9.00 - 9.10, 9.20 - 9.30, 9.40 - 10.00
5. Save the **Date Time Schedule**.
6. Configure a response plan to enable and disable the Geofences.
7. Go to the **Date Time Schedule** object and expand to see the events.



8. Right click on the **Date/Time Status Schedule > React To Event > Run Response Plan > Existing Plan** and choose the response plan created in step 6.

You will notice that the Geofence will be enabled for the selected time frame and is visible on the scene and is in disabled state and either displayed transparent or completely hidden from the scene as configured.

Alarms on Encroaching the Geofence

As seen in the previous sections, we are aware that Control Center is capable of plotting the Geofences and gathering tracks from a radar device and displaying them on the map. The information about tracks is gathered periodically and dynamically updated on the

map. The user can now see where the target object is heading and raise appropriate events which can then be included in the alarm types to alert the operator.

The main events are as listed below:

- **Approaching:** Object approaching the defined zone
- **Device State Changed:** Alerts when the device goes offline
- **Entering:** When the target object has entered the Geofence
- **Exiting:** When the target object has exited the Geofence
- **Loitering:** When the target has entered the Geofence and been in the area for too long
- **Crossed:** When the object has crossed the Geofence area before the radar could track it

When any of these events occur and is part of the alarm type defined within Control Center, then an alarm is raised. You can also configure an alert state to change the color of the Geofence when an event occurs and roll back to normal when another event occurs to normalize the situation.

For example: When an object enters the Geofence, Entering event is initiated and the Geofence changes to the color configured in the Alert state and starts to blink to grab the attention. An alarm is also generated in the alarm stack.



The operator can also choose to Slew to Cue and assign a camera to follow the object. When the target object makes its way out of the Geofence, an Exiting event is triggered, and the alert state is dismissed. The Geofence is restored to its default color

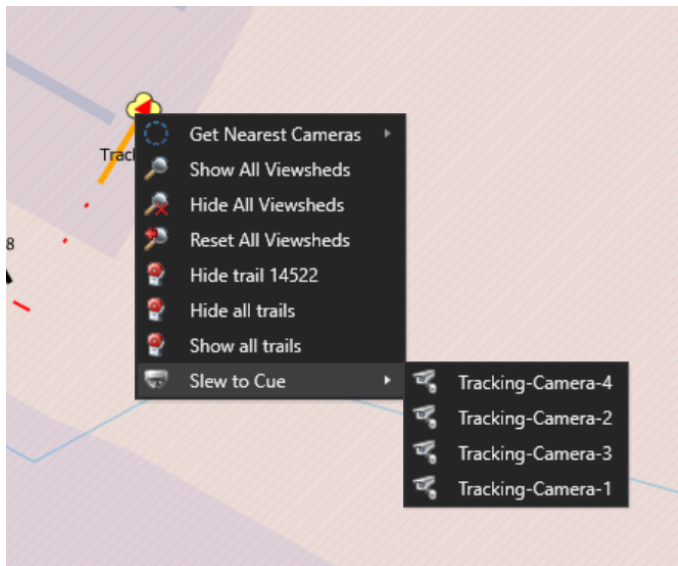


Slew to Cue

Slew to Cue is the terminology used to describe the process of integrating the radar device with the PTZ camera to send coordinates of the target object and instructions to the camera and tell where it needs to point. This process is designed to detect the target and pinpoint its position and continuously transmit the information to the PTZ camera for it to follow the object.

If an object has been detected within a geofence area and the operator needs to take a closer look or follow to make sure that it is not posing any danger and safely exits out of the defined area, he can select the Slew to Cue function by right clicking on the track that needs to be followed, select Slew to Cue and the closest camera to follow the target. This functionality is further extended during commissioning by defining the Slew to Cue clicked event in a response plan to take necessary action.

When the operator selects the camera to follow the response plan is fired which sends the instruction to the Radar Watch connector which in turn guides the Camera connector to send commands to move the camera in view of the target.



Currently, the Slew to Cue action is manually driven by the operator which fires a response plan for further actions.

The response plan must also contain an instruction to stop the Slew to Cue action as it is not yet made available in the context menu

Dynamic Viewsheds with Base azimuth Offset

When Slew to cue action is triggered the camera needs to position itself repeatedly to follow the target object from the co-ordinates provided by the Radar Watch Connector. So, the object's co-ordinates need to be seen from the camera's perspective as the originator of the scene. The Radar Processor transforms the real co-ordinates to the

view co-ordinates that are relative to the positioning of the camera and direction. To derive a camera position, you need:

- The exact position of the camera
- The camera must have a reference point to True North
- Elevation of the camera

The Azimuth offset refers to the rotation of the camera around a vertical axis.

For example: In the picture below if true North is considered as Zero degrees, East will be 90° , South 180° and west 270° .



The camera calibrations are done during installation and the reference point is set to True North. The angle that camera needs to look at during slew to cue action is calculated based on these offset values.

The viewshed of the camera is dynamically adjusted by the Radar Watch which receives the exact co-ordinates of the target object and calculates the distance of the object from the camera and sets the range for camera to be able to view the object.

Video

Control Center enables you to view live and recorded video. You can access a video by dragging a camera from the System Explorer or a map to a tile. See Tile Layouts.



Video Sequences

Sequences enable you to configure and deploy Video Management Systems.

Typically, a Sequence takes the outputs from the specified CCTV cameras and displays them to an operator in a sequence of tiles. A Sequence includes preset dwell times between camera changes and can also be paused, stepped forward, and stepped backward using the Tile toolbar. The Sequence can be set to run through indefinitely or only once. This gives the operator a standard sequence while retaining the flexibility to control what they see. In addition, the operator can even save snapshots of the displayed content.

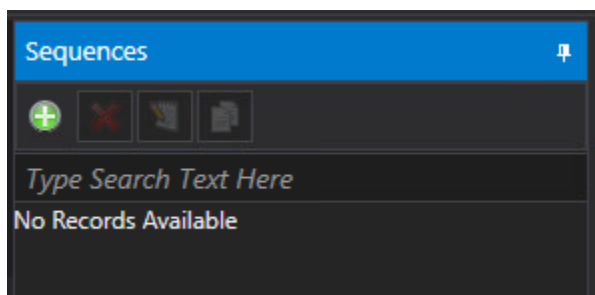
Video Prerequisites

As a sequence scrolls through multiple camera devices, you must first specify camera devices in Control Center.

Configuring Video Sequences

To create a sequence:

1. From **System Explorer**>**Sequences** menu, click + to create a new sequence or right-click anywhere in **Overview - System Objects** pane to select **New> Sequence**. A sequence is added to the **System Object** pane. Sequences can be saved globally, that is, you can save sequences local to the user or shared across all users.



- Open the new sequence. The **New Sequence** page appears.

The **Sequences** dialog displays the same view as the System Explorer if the base location is configured in the System Explorer.

- Enter the following parameters in the **Sequence** dialog:
 - Label** – The name of the sequence, for example Test Sequence.
 - Description**– A brief description of the sequence.
 - Allow all users** to access the sequence – Selecting this enables the **Location** search field and you can save the sequence to a Control Center folder or location by specifying a location for the Test sequence (sample sequence).
 - Location**– The folder location of the sequence, for example, **System Objects**. This field is available only if the **Allow all users to access the Sequence** check box is selected.
 - Available Assets** - The camera devices available to the logged in user that can be used in this sequence. To search for a known device, type the name of the device into the **Search** field or use the **Available Assets** hierarchy to find it in the device location tree.

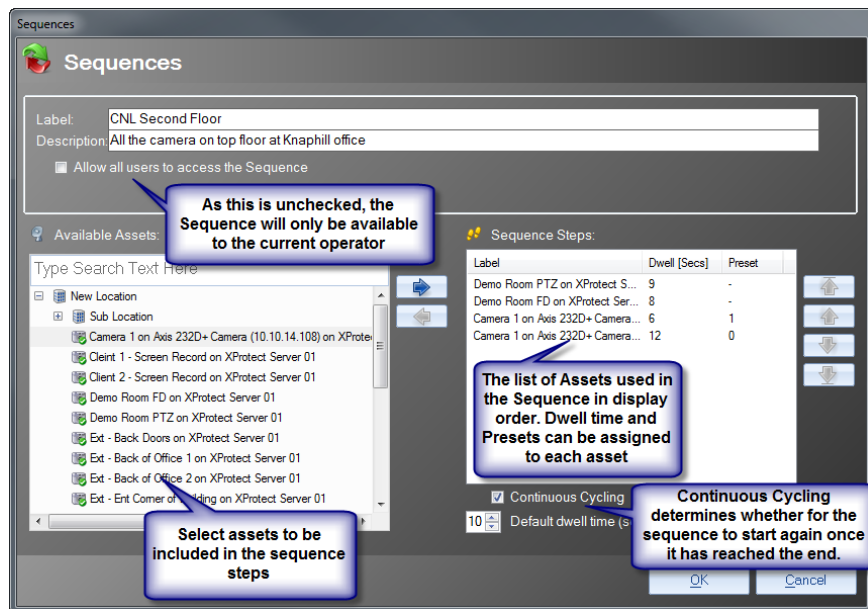
You can apply standard permissions as the object is in the folder hierarchy.

A camera might appear in a Sequence multiple times. This might occur when an area needs to be monitored more frequently. Alternatively, a PTZ camera can be included more than once but with a different preset.

4. Drag the Location into the sequence steps and select the check box **Include children on Locations** to enable all the cameras in that location to be used in the sequence.
5. Find a device in the **Available Assets** list and move it to the **Sequence Steps** field using the right arrow button or drag and drop it to the list.
6. The **Available Asset** is included as the first item in the sequence. For a sequence to work, it needs to include more than one device.
7. Continue to add devices to the sequence steps until there are three or four devices in the sequence steps.
8. You can choose devices from all locations configured as root nodes for each base folder in **System Explorer** if the base location is configured in **System Explorer**.
9. To reorder the sequence steps, use the Up and Down arrow buttons until the devices appear in the order that they should be sequenced.
10. The sequences steps are populated with the required devices in the order they should appear in the sequence.
11. By default, the dwell time on each camera in the sequence is 10 seconds. The default time can be changed in the **Default dwell time (seconds)** field. Once the default dwell time is changed, it applies to any new devices added to the sequence steps.
12. Dwell time for devices already in the sequence can be changed.
13. To set the dwell time of each camera already in a sequence, click the **Dwell (Secs)** field next to the first camera to enable it. The **Dwell** field is enabled.
14. Use the Up/Down arrows to increase or decrease the dwell time on the selected device.
15. Click the Preset column to save the **Dwell** changes and view the next feature.

Presets refer to preset camera configurations of PTZ cameras. PTZ is an acronym for pan, tilt, and zoom and reflects the movement options of a camera. Each time a Sequence displays a PTZ camera, the Sequence can specify what preset position to display. A PTZ camera with multiple Presets can be used multiple times in a Sequence with a different Preset defined for each camera, for instance.

16. To specify a **Preset** position for a PTZ camera, click **Preset** next to the camera. Use the Up/Down arrows to specify the **Preset** number to display at this stage of the sequence.
17. Click away to save the preset changes.



To repeat the Sequence indefinitely:

Select the **Continuous Cycling** check box and then click **OK**.

Test that the sequence appears in the list of available **Sequences**.

To view and use a Sequence:

Highlight the sequence in the list of available **Sequences** and drag it into the tile. The first camera in the sequence appears in the tile.

As a sequence is being played on the tile, the active camera shows highlighted in the map area and the System Explorer.

To delete a Sequence:

Highlight the sequence in the list of available sequences and click **Delete** in the toolbar. The sequence is deleted from the list of available **Sequences**.

To edit a Sequence:

1. Highlight the sequence in the list of available **Sequences** and click **Edit** in the toolbar or double-click it in the **Sequences** list. The **Sequence Editor** is displayed.
2. Make any changes and click **OK** to save them.

Changes made to a Sequence that is currently displayed in the Tile Display may not appear until the active window is closed and reopened.

To copy a Sequence:

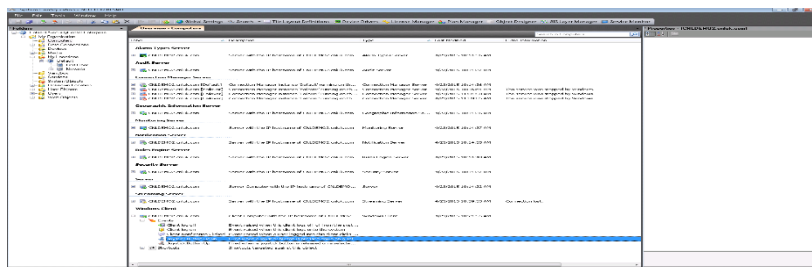
1. Highlight the sequence in the list of available **Sequences** and click **Copy** in the toolbar. The sequence is copied and appears in the **Sequence** list with the same name as the original appended by the word - **Copy**

2. Open the new sequence by clicking **Edit** in the toolbar (or double-click the sequence in the list). The **Sequence Editor** appears.
3. Rename the Sequence and make any changes. When finished, click **OK**. The renamed Sequence appears in the list of available Sequences.

Joystick

Control Center supports the DirectX joystick interface. This can be used to pan, tilt, and zoom a selected camera. In addition to this, Control Center also supports joystick button events.

When viewing a camera, pressing a Joystick button will trigger two events on the Windows Client object: first the Joystick Button Down event and then the Joystick Button Up event.





Link the events to a response plan to implement the button events functionality. The events will include the following metadata:

Event	Description
Button pressed	The Joystick button that was pressed
Current Server	The Control Center Server that the Joystick is connected to
Date_Time	The Date/Time of the event
Device	The selected camera
Sender	The Windows Client to which the joystick is connected
User	The user logged into the client to which the joystick is connected


In addition, the Joystick Button Up event also has a property ButtonPressedDuration, which returns the duration for which the button was pressed for.

Taking Snapshots From Video


You can save snapshots from live or recorded video to your local disk or as a media file in Control Center. This is useful if you want to send a snapshot to a third party or if the snapshot is required in another company system, for example.

- Select  to take continuous snapshots of a video if, for example, you are not able to re-wind or fast forward the video easily and you want to take multiple screenshots in one playback session.
- Select  to open the **Preview SnapShot** window. As well as previewing a snapshot, you can also change the snapshots appearance. For example, you can highlight areas of the video, add text, resize the snapshot or add effects.

Taking Continuous Snapshots

Select  to take continuous snapshots of a video if, for example, you are not able to re-wind or fast forward the video easily and you want to take multiple screenshots in one playback session. By default, the media files are saved as .bmp files. The filename is the camera name, date and time the snapshot was taken. For example, **UK-CAM-02-Building Entrance 25-03-2021 14-32-53-643**.

By default, the snapshot media files are saved in Entire Enterprise\My Organization\User Objects\Administrator Objects\My Snapshots.

If you are handling an alarm and you select  to take a snapshot of the video from the camera that generated the alarm, the snapshot is saved in Entire Enterprise\My Organization\System Objects\Alarm Media\Alarm *ID* where *ID* is the ID of the alarm you are handling.

You can change the media file format and saved snapshot filepath in **Global Settings**.

1. Go to **System Configuration > Global Settings**.
2. Select **Enterprise Settings**.
3. Navigate to **Camera**.
4. In **Video Snapshot Path**, type the filepath where you want your snapshot media files to be saved.
5. Select the media file format from **Snapshot Image Format** drop-down list.

You can disable this feature completely by leaving the **Video Snapshot Path** box empty.


Previewing or Changing a Snapshot

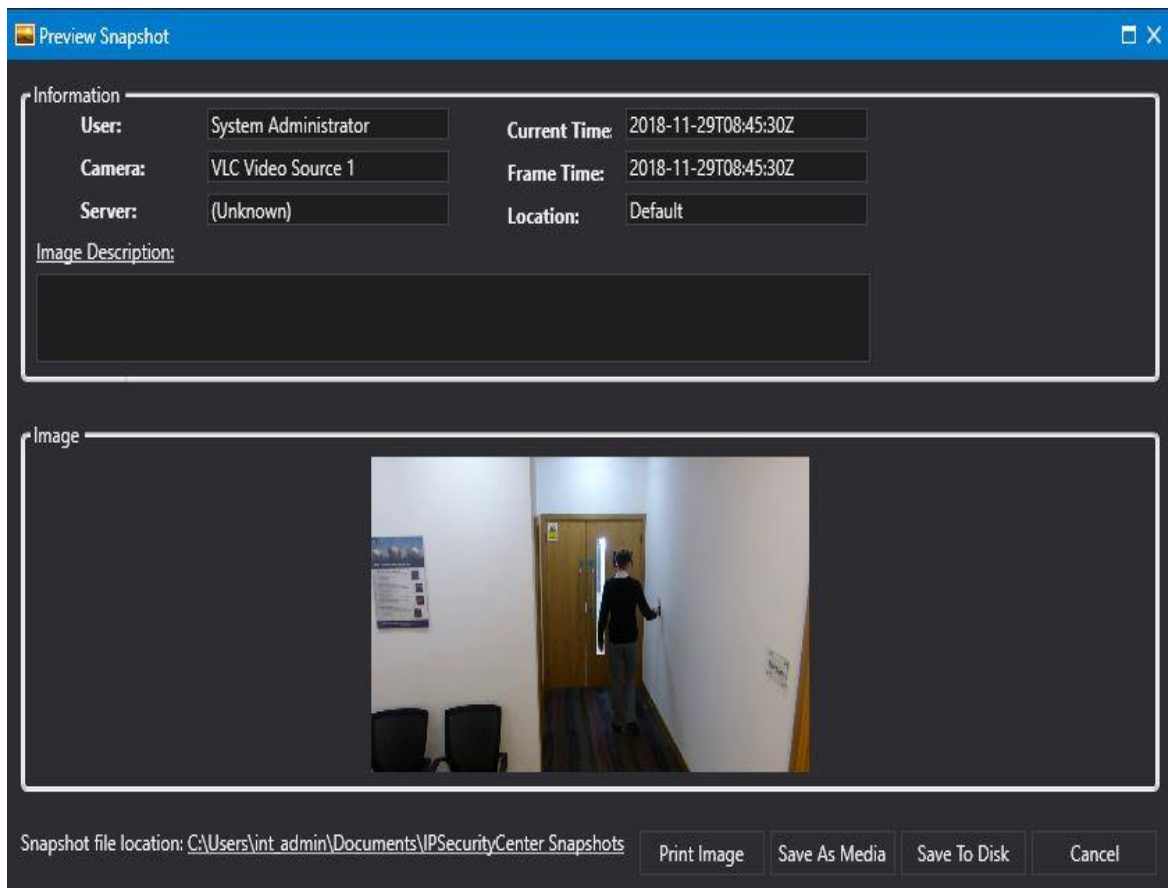
Select  to open the **Preview SnapShot** window.


As well as taking a snapshot, you can also change the snapshots appearance. For example, you can highlight areas of the video, add text, resize the snapshot or add effects.

The snapshot can be:

- saved to disk
- saved as a media file in Control Center
- attached to an alarm.

The options that are available to you when you select , depend on how your Control Center Administrator has configured how snapshots can be used in Control Center. This means that you may not have some of the options described below.



1. Select  from the tile layout displaying the camera whose video you want to take a snapshot of. The **Preview Snapshot** dialog displays. The **Information** panel displays:
 - **Username** of the user who created the snapshot.
 - **Camera** name whose video this is a snapshot of.
 - **Server** where the camera resides.
 - **Current Time** the snapshot was created.
 - **Frame Time** reported by the sub-system when the snapshot was created.

- **Location** in **Control Center** where the snapshot was taken.
2. Optionally, add an **Image Description** for the snapshot.
 3. Use the tools in the **Image** panel, to make any changes required to the snapshot.
 4. Select **Snapshot File Location** to browse to the location where you want to save the file.
 5. Select one of the following:

Option	Description
Email	Select this to enable the Send Email button. This option is only available when the SMTP settings are enabled in the Global Settings dialog.
Send Email	Sends an email of the snapshot to another user. This requires the SMTP (Email) Global Settings to be configured correctly. The snapshot is also saved to the database.
Attach to Alarm	<p>Attach the snapshot to the alarm that is currently being handled. Attach to Alarm is only available if you are handling an alarm in Control Center.</p> <p>The snapshot is saved in the System Configuration > System Objects > Alarm Media folder. In a federated system, once the snapshot is saved as a media object, you can publish it to other sites in your federated system, if required.</p> <p>If you have process guidance configured, you will see Map Snapshot or Camera Snapshot in the alarm activity grid when you are completing the alarm resolution form.</p> <p>Notes:</p> <ul style="list-style-type: none"> ○ You can attach multiple images to the same alarm as long as the alarm is in a handled state by your current user. ○ You cannot have more than one alarm handled by the same user in Control Center. ○ The snapshot is saved to the [Alarms].[AlarmActivity] table in the Control Center database.
Print Image	Print the snapshot.

Save As Media	Save the snapshot as a media object in Control Center . When a snapshot is saved as a media object, it is stored in System Configuration > User Objects > Snapshots folder. For federated node sites, snapshots stored with the user objects folder are federated to any configured hub.
Save to Disk	Save the snapshot to the location you specified in Snapshot File Location .
Cancel	Close the Snapshot Preview dialog without saving the snapshot.

Once you have created your snapshot, you can open it in any image viewer.

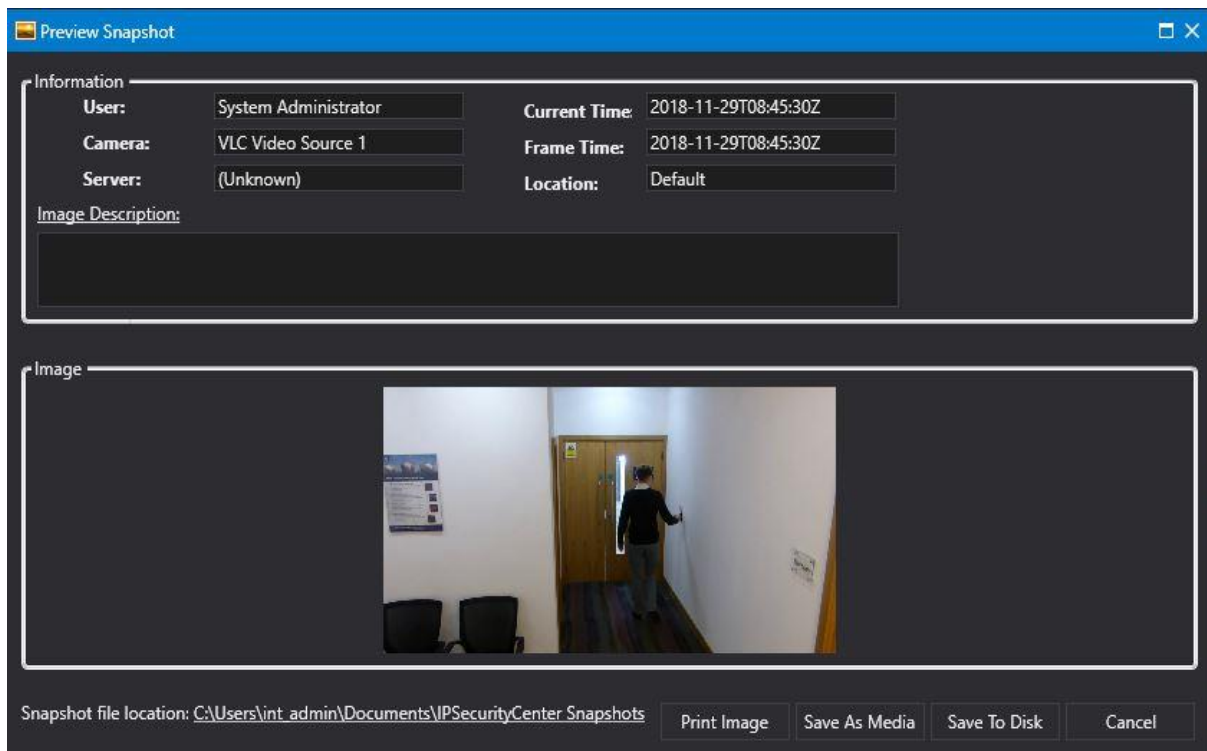
Saving Snapshots to a Disk

The snapshots taken from a video can be saved locally on your system for easy access. The default folder in which the screen shots are saved need to be pre-defined. This path is specified in the **Enterprise settings** configuration under the **Global Settings**. To set the file save path, do the following:

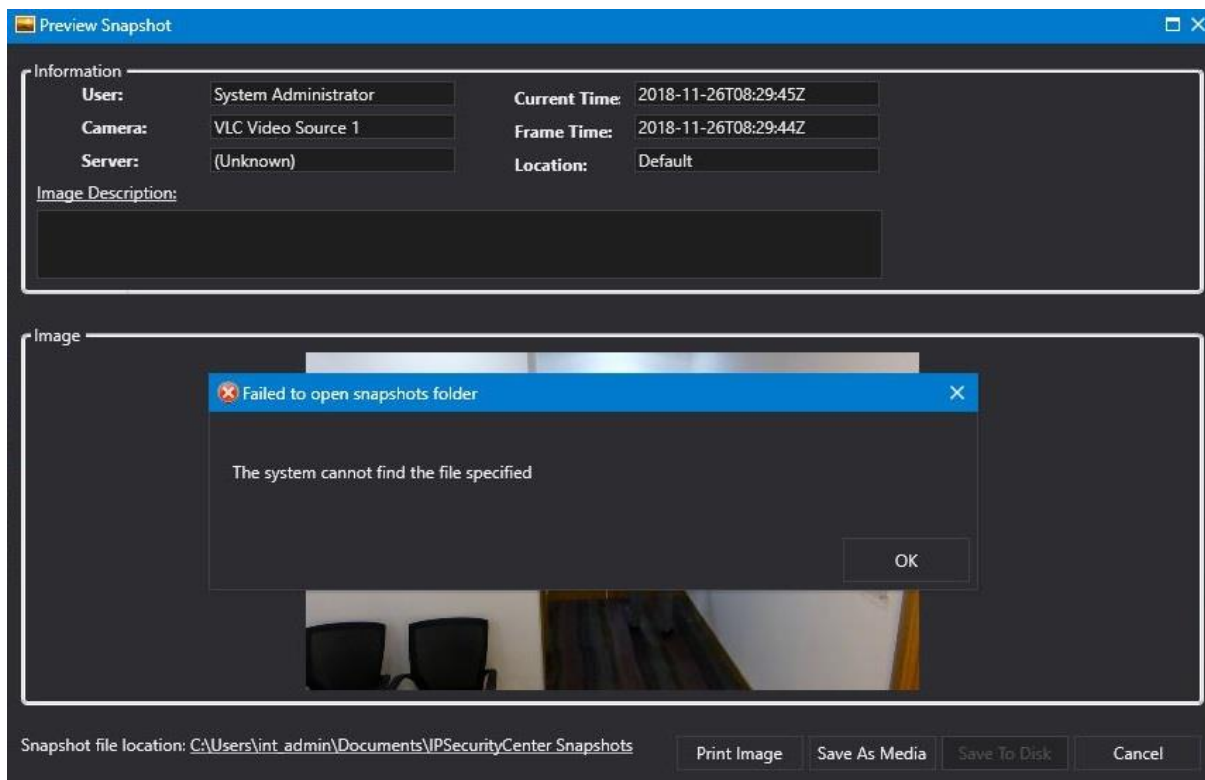
1. Go to **System Configuration window**.
2. Click on the **Global Settings** tab in the Top Menu ribbon.
3. Select **Enterprise Settings** from the left pane options.
4. In the right window, for the **Video Snapshot Path** variable, specify the destination path name in which you wish to store the snapshots.
5. Click on **Apply**.

This path will now be used to store all snapshots being saved on disk. The saved path is displayed on the **Preview Snapshot** window as shown in the picture below. This is a read-only link which can be edited in the **Enterprise Settings** only, by a user with

administrative rights. Nevertheless, any user will still be allowed to click on the link to navigate to the folder in which the images are being stored.



Upon successfully saving the image on to the disk, a confirmation message will be displayed along with the path in which it was saved on the disk, which will typically be the path established in the Enterprise Settings. In the circumstances where the pathname is not specified or is invalid, the save to disk Option will be disabled as seen in the figure below. On clicking the read only path link, an error message will be displayed to the user prompting that the pathname is invalid and needs to be changed for storing the images locally.



If the save was unsuccessful, due to the file path not accessible or the user not having the rights to save in that location, an error message will be displayed along with the path attempted to reach.

Configuring the Path for Saving Snapshots

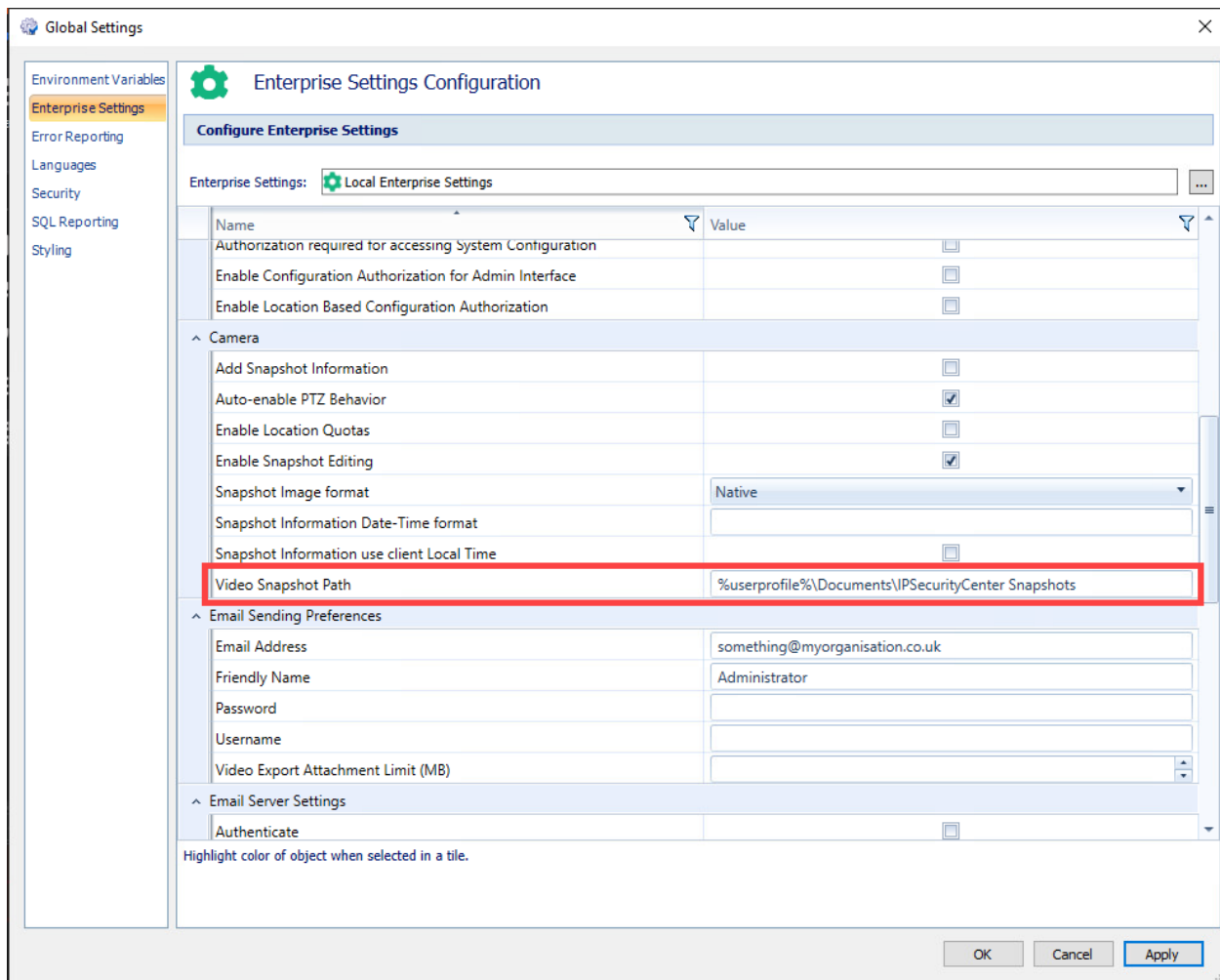
The administrator can set the default path in which the snapshots will be stored across all sites in Enterprise Settings and publish it. This can be achieved by using the windows environment variable or creating a user defined environment variable within Control Center.

The environment variable is used to place dynamic value in the path name which is populated by the local system when the process is running at a local site.

The environment variable can be an entire file path or can be used to define a part of it.

For example, if the images have to be stored in users\documents\IPSecurityCenter Snapshots folder, the administrator can set the video snapshot path variable in Enterprise Settings configuration as follows:

Video Snapshot Path %userprofile%\Documents\IPSecurityCenter Snapshots



Where *userprofile* is windows defined environment variable which dynamically gets the value of it from the local system to populate the entire file path name.

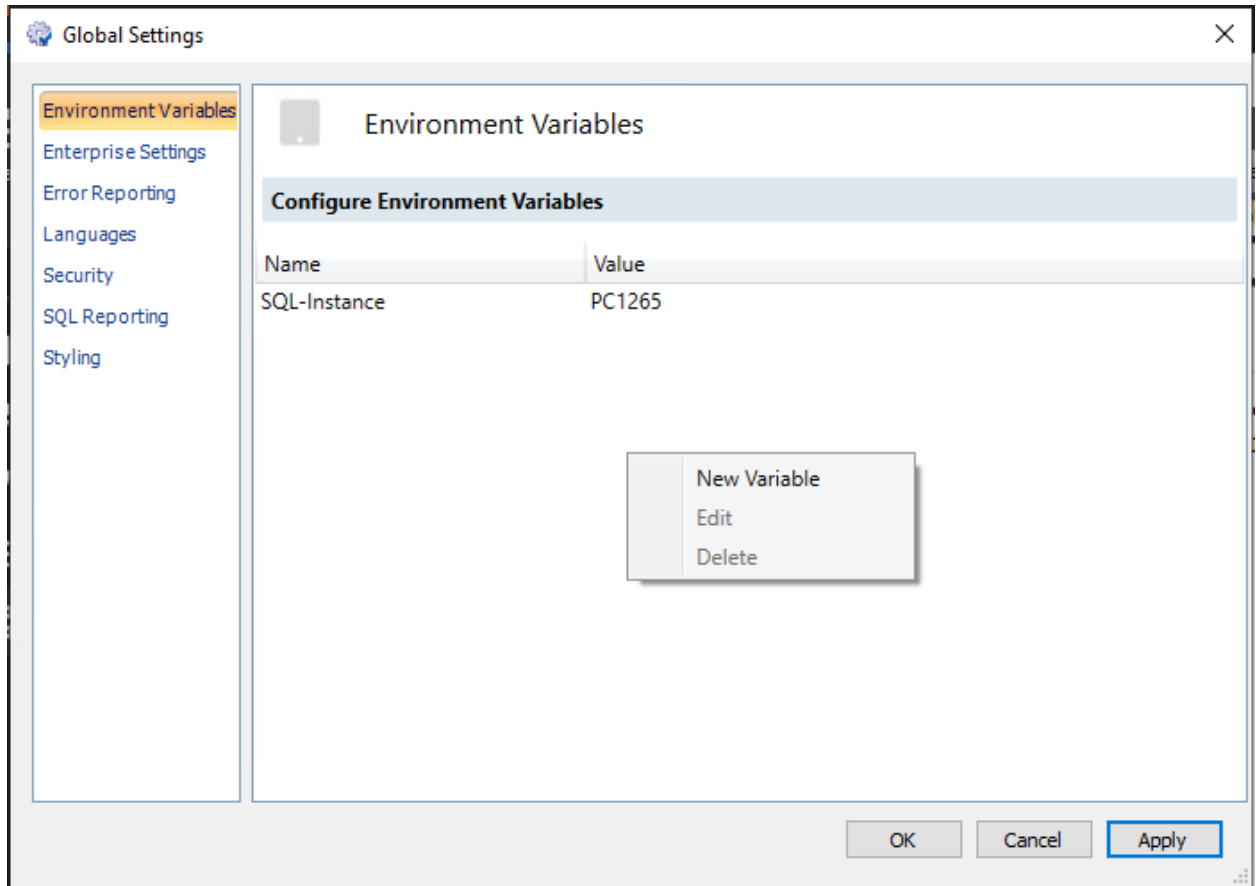
You can also create environment variables in Control Center to be used within the application. The variable names need to be unique and care must be taken that they are different to the ones used by windows. If a variable is created which matches the windows environment variable name but has different value to it, Control Center looks for the value within Control Center first and uses it. If you intend to use the value assigned by the windows, either use the standard variable name specified by the windows system or use a different variable name.

Creating an Environment Variable

To create a Control Center specific environment variable, you need to:

1. Go to **System Configuration** and click on the **Global Settings** tab in the main toolbar ribbon on the top.

- In the left pane, select **Environment Variables** which will take you to the screen below:



das

- Right click in the window on the right to show up the Menu.
- Select **New variable** option to create a new variable.
- Populate the **Variable** name and **Value** field.
- Click on **Apply**. A new environment variable is created to be used within the Control Center setup.

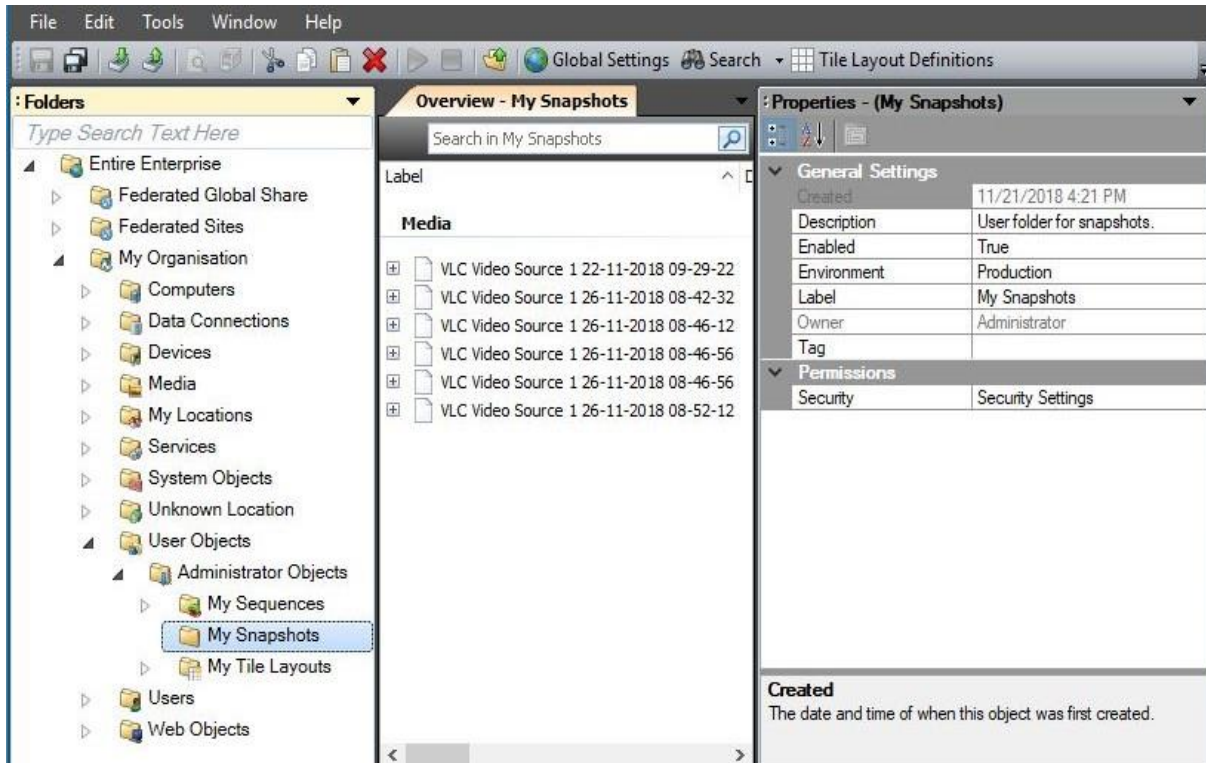
You can also edit a variable and delete it as required.

Furthermore, two environment variables can be defined to hold file path names and concatenated to make an entire path where the images can be stored. During this process if the system detects more than one \ in its path it will automatically be removed.

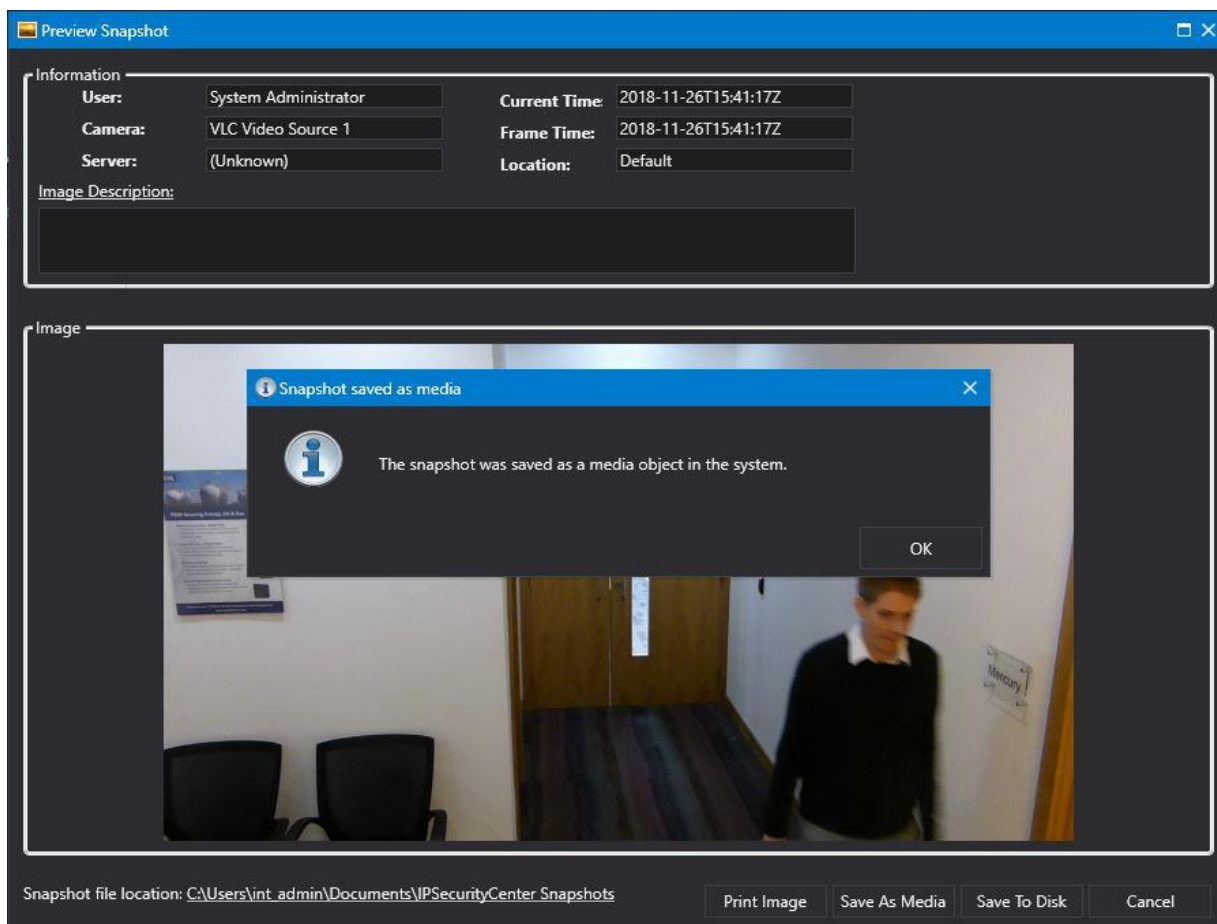
Snapshot - Save As a Media File In Control Center

The screen shots grabbed from a video can be stored as a media file in Control Center. When a snapshot is saved as a Media object, it will be stored in the **User Objects > Username Objects > My Snapshots** folder accessible from **System Configuration**.

For Federated Node Sites, snapshots stored within the **User Objects** folder will be federated to any configured Hub.



When you click on **Save as Media**, the snapshot will be saved in the location shown above and a message will be flashed to the user to confirm the action.



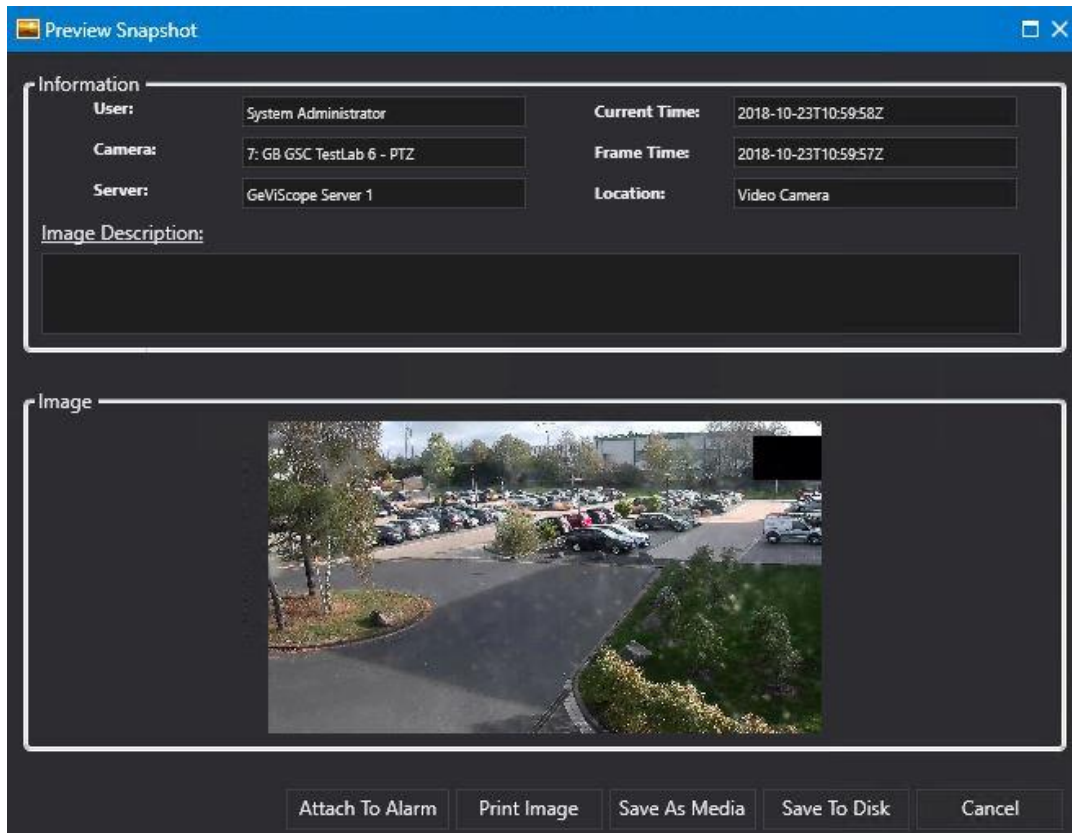
Alarm Snapshots

You can save a copy of an alarm snapshot as a media object and reuse it when generating reports specific to alarms. Selecting **Attach to Alarm** from the **Preview Snapshot** dialog can be used to perform the following functions:

- Attach an image coming from the connector to an alarm in the form of snapshots
- Attach the image to a currently handled alarm
- Link to any alarm that's currently being handled
- Federate the alarm attachment details to applicable sites

You must be handling an alarm in Control Center for the **Attach to Alarm** option to be displayed.

1. Log in to Control Center and display a camera on a tile.
2. From the tile where the camera is being displayed, click **Save as Snapshot**. The **Preview Snapshot** dialog appears.



3. Click **Attach to Alarm**. The snapshot of the image is saved in the **Alarm Media** folder.

Label	Description	Type	Last Modified	Extra Inform
Media				
1_GB GSC TestLab 1 03-09-2018 09-22-15 for alarm 2		Media	9/3/2018 10:22:44 AM	
1_GB GSC TestLab 1 03-09-2018 14-35-01 for alarm 4		Media	9/3/2018 3:39:18 PM	
1_GB GSC TestLab 1 31-08-2018 16-41-00 for alarm 1		Media	8/31/2018 5:42:47 PM	

You can attach multiple images to the same alarm as long as the alarm is in handled state. You cannot have more than one alarm handled by the same user in Control Center.

4. An additional alarm activity is added to the alarm. A new view in the database provides access to the snapshots for an alarm. This can be used when creating reports. The view is called [pacific].[IPSC].[AlarmSnapshotActivityView].

Snapshot Time Zone

When configuring the date/time format that is displayed in your snapshot information, you can use:

- The default: yyyy-MM-ddTHH:mm:ssK
- Your own custom date/time format

- The local date/time of the client

Using Default Date/Time

The date/time format for the saved snapshots conform to ISO 8601.

The format used to display time and date is: yyyy-MM-ddTHH:mm:ssK

In this context, the T character separates the date and time components and the K character is the offset from UTC and this is appended to the time in the same way that Z was above, in the form \pm [hh]:[mm]. So, if the time being described is one hour ahead of UTC (such as the time in Berlin during the winter), the zone designator would be +01:00, +0100, or simply +01. To represent a time behind UTC the offset is negative. For example, the time in New York in winter is UTC-05:00. For more information on configuring Time Zones, see the Control Center Installation Guide.

Using a Custom Date/Time Format

You can define your own custom date/time formats. To do this:

1. Go to **System Configuration**.
2. Select the **Global Settings** tab.
3. Select **Enterprise Settings**.
4. In the **Snapshot Information Date-Time Format** box, enter **Other:customformat** where *customformat* is your custom date and time format. For example, **Other:yyyy-MM-dd** only displays the date.

Using Local Date/Time

You can use the local date/time of the client machine that captured the snapshot preview. To do this:

1. Go to **System Configuration**.
2. Select the **Global Settings** tab.
3. Select **Enterprise Settings**.
4. Select the **Snapshot Information use Client Local Time** checkbox.

Video Player Playback Mode

The playback speed controller control which is displayed during playback of video allows you to select from the available playback speeds.



When you select a playback speed by moving the control to the left or right of the center point, the desired speed appears under the Playing label.



If you release the mouse, this selection of playback speed will persist until you manually adjust the speed or Pause and Restart the playback using the Play/Pause button.

Video Time bar Zooming

You can press the Ctrl key while scrolling the mouse wheel from up or down to zoom in and out of the time bar to view a detailed breakdown of the time bar and take a wider view.




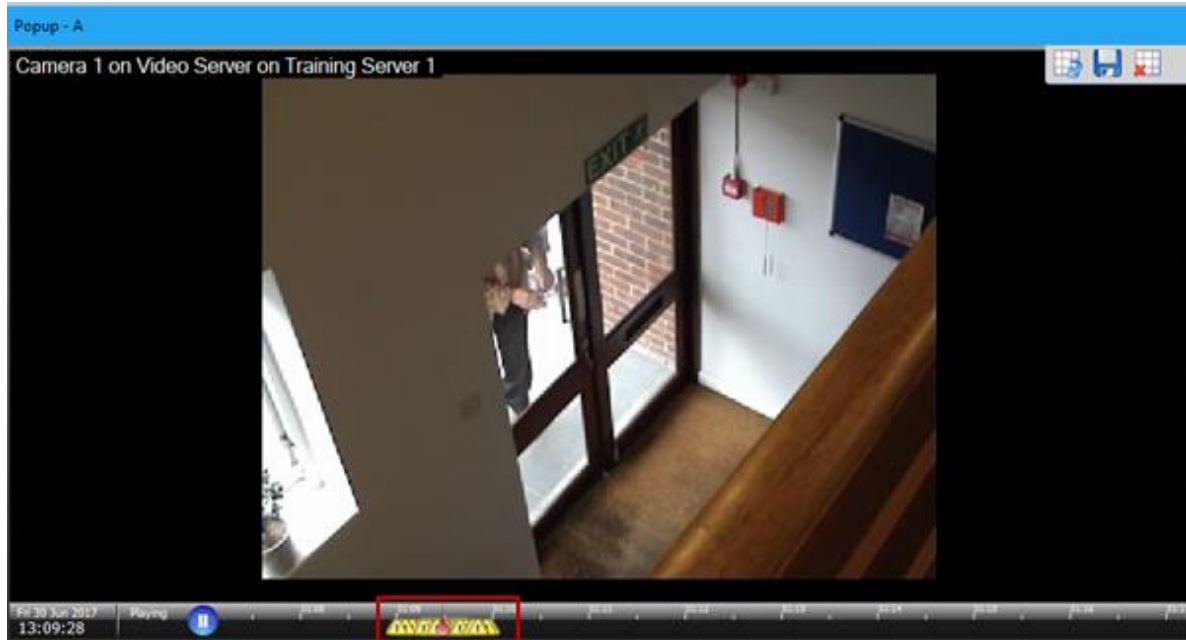
Alarm indicators on Video Playback mode

You can track when alarms were raised while in Video playback mode with the help of alarm indicators. In addition, you can handle alarms by right-clicking on the alarm indicator icon.

Make sure to configure playback supported cameras.

To configure alarm indicators:

1. Create an Alarm Type with an event on Training Server, for example BMS event. For more information, see [Defining an Alarm Type](#).
2. Drag and drop a camera on to the display area to show a live camera.
3. From the toolbar, click  to set the live camera in playback mode.
4. Generate alarms and view them in the **Alarm Stack** area.
5. View the playback camera on the display area during the time when alarms were raised. The alarm indicators are displayed in the form of icons on the time bar. Shown below are alarm indicators in playback mode.




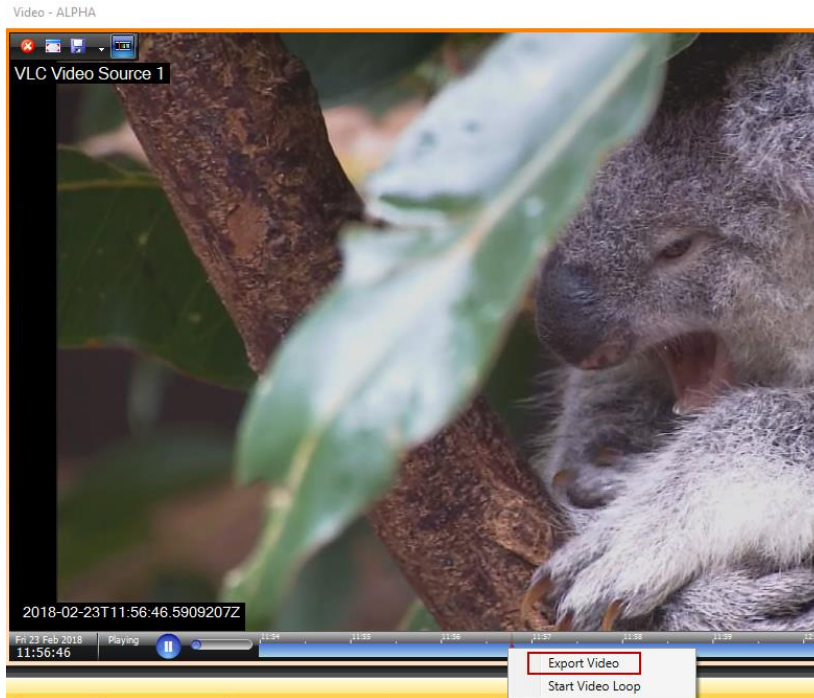
You can only handle alarms from the alarm indicator icon, if the required permission for handling an alarm type is set against the alarm handling group.

Video Export Wizard Shortcut

Using the Export Video Shortcut option from the time bar, operators can export video while the video is in playback mode. It is possible to control which users can invoke the Video Export Wizard by configuring the relevant security policies.

To use the Video Export tool from the video tile layout:

1. From the **Video** tile layout, click  to set the live camera in playback mode.
2. On the time bar, select a specific duration for which you want to export the video by hovering on the time bar and selecting it with the mouse, then right-click and select the **Export Video** option from the context menu that appears. The **Video Export Wizard** appears. For details on creating a new video export, see [Creating a new export](#). Any changes made to the video export gets recorded in the audit log using the existing auditing rules.




Video Loop Playback

Use the Video Loop Playback functionality to loop a section of the video shown on a tile layout back-to-back for a specific duration in playback mode.

You can define the Playback Start Time and Playback End Time in a response plan using the Set Tile Contents shape, such that when the playback video is displayed, and the recording reaches the end of the loop, the video restarts from the Playback Start Time. It will continue to repeat until the camera is switched to live or closed. In addition, you can pause the video at any time during the loop.



To enable the video loop playback function:

1. From the video tile, click  to switch to playback mode.
2. On the time bar, select a specific duration for which you want to loop a video by hovering on the time bar and selecting it with the mouse, then right-click and select **Start Video Loop**. The video will start looping and continue to repeat until the camera is switched to live or closed.


Event Indicators in Video Playback Mode

The time bar displayed on the Video Player window can be configured to display event information from a sub-system that is associated with Control Center. The event indicators appear on a video camera configured within Control Center that is in playback mode at the time. Using the event indicators, you can track when an event was raised.

Prerequisite: When adding cameras, make sure to add playback supported cameras only.

To view the event indicators on the time bar:

1. Install a device connector that supports displaying event indicators in playback mode. In this example, install the American Dynamics VideoEdge connector or Intellex connector, and then add the device to your Control Center solution.
2. From System Configuration, make some changes to the newly added device such that an event is generated. For example, edit the existing label of the camera that is configured with the device.
3. Drag and drop a camera on to the display area to show a live camera.

4. From the **Video Player** toolbar, click  to set the live camera in playback mode or directly view the camera in playback mode.
5. View the playback camera on the display area around the time when the event was raised. The event indicators are represented by a small blue dot on the time bar.



Hovering on the blue dot will display additional information about the event. For example, in this example, the following event properties are displayed:

- The date when the subsystem was configured
- The Device identifier
- The label of the subsystem that generated the event
- The date and time when the event was created

The event information that appears on the time bar depends on the connector installed and event selected.



To configure the time bar properties:

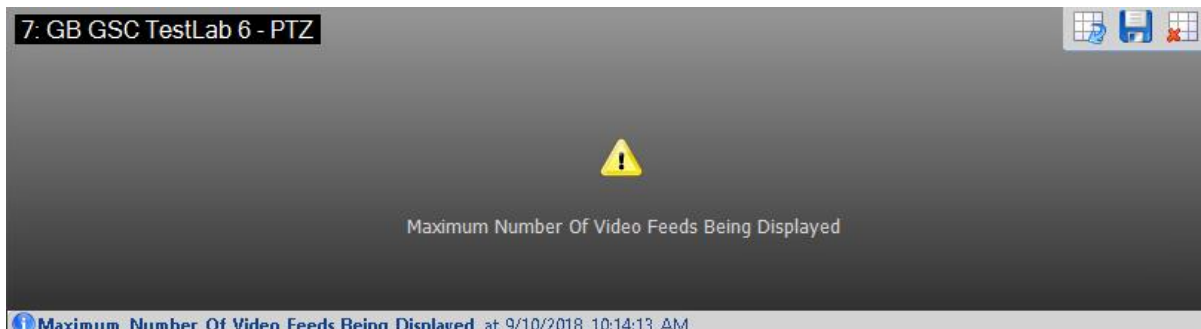
1. Select the device that you installed in the previous section.
2. In the **Properties** pane, click **Time bar** events. A new popup window with the available event types appear.
3. Select the required event types to be displayed on the time bar when you hover on the event indicators.

Limiting the Number of Concurrent Video Feeds for Specific Users

It is possible to limit the number of concurrent video feeds that users can view at any time. Using the Maximum Concurrent Video Feeds property for a user object or group object, you can restrict the user object or a group object to view a specific number of camera feeds, for example, two camera feeds. When the same user is logged on to the

multiple clients, they will be able to view only two camera feeds on each client. When this property is set to 0, you can display unlimited video feeds.

Note that if a user is a member of multiple groups, then the highest values will be considered. In addition, if you try displaying additional feeds than the maximum limit specified for the user or group, then instead of displaying the video, the following warning message will appear:



You must restart the Windows Client for the changes to apply.

Federated Control Center

Federated Control Center enables users of one instance of Control Center to handle and manage alarms generated from another instance of Control Center. It supports sharing alarms, devices, events, locations, and other relevant data synchronized. A federated instance of Control Center can be configured as a federated Hub or a federated Node.

A federated Node site is characterized as a sender of Alarm data to a federated Hub. A federated Hub can receive Alarm Data from any number of connected federated Nodes and may also send Alarm Data to another Federated Hub.

The main objective of federated Control Center is to support the following requirements:

- Each site must be able to work independently of the other
- Alarms at one site should be handled by users at another site
- Devices at one site should be visible to users at another site
- Publishing configuration objects (for example, Response Plans) to remote sites



An alarm does not exist in isolation from the rest of the Control Center eco-system, therefore all the components required to manage alarms at a remote site are made available from the Node (Site B in Simple Federated Alarms figure) to the Hub (Site A in Simple Federated Alarms figure).

In addition to the alarm information, each site will also include a set of commissioned workflows, graphical user interfaces, and user and client data that are required through the lifecycle of the alarm.

System-to-System Communication

When two independent installations of Control Center are configured to share content, the following process occurs:

- **Negotiation Phase** - Establishes that there is another system correctly configured and ready to begin communications.
- **Initial Synchronization Phase** - Ensures that all prerequisites needed for the two systems to share information have been passed between the sites. Once all the required content has been shared between the sites, alarms can then be synchronized by the on-going synchronization process. The initial synchronization

phase is also responsible for determining whether there are historic alarms to be synchronized. Where historic alarms exist, they are batched up and transferred to the federated Hub to ensure that current or newly created alarms are not impeded.

- **On-going Synchronization Phase** – Keeps the synchronized content current at each site and ensures new alarms are immediately communicated to the Hub. Heartbeats are sent between the sites to ensure communication status between the sites can be monitored.

If the connection between the Hub and Node sites is interrupted, the systems will continuously attempt to reconnect with each other until the connections are disabled.

After the connection is re-established, the same process will be followed. The Initial Synchronization phase will only re-synchronize changed items and will not perform a full Synchronization.

Alarm Synchronization

In a federated system, the Node sites send Alarms to the Hub sites. Therefore, the base alarm information, additional components, and the associated data must be transferred between the sites.

When configuring a federated Control Center environment, a site may be configured as a federated Node or a federated Hub.

- **Federated Node(Sender)** – Can only send alarms to any number of sites configured as Hubs.
- **Federated Hub(Receiver)** – Can receive alarms from any number of federated Nodes. In addition, a Hub can also send its own alarms to other Hubs, as long as a Node license is also applied.

Control Center does not support sending and receiving alarms from the same remote site.

Federating content between sites does not indicate exchange of equal information between the sites. Typically, a Hub site that handles alarms on behalf of a Node site receives more information than it sends.

The components that make up an alarm are:

- The alarm itself
- The events that make up the alarm
- The devices that send the events
- The folders that provide context to the hierarchy of the site generating the alarms
- The locations where the devices are stored as these may be alarm points for the alarm

- Any Placeholders as these may be used as alarm points
- The users at the Federated Node so that when alarms are handled by a user at the Node site, the Federated Hub can interpret which users handle the alarms
- The Windows clients at the Federated Node so that when handling alarms at the Node site, the Federated Hub can interpret where the alarms are being handled
- The Date/Time schedules that could impact how the alarm behaves through the lifecycle of the alarm
- The alert states associated to the alarm so that the alarm can be displayed in visual form

Although not directly related to the handling of the alarm, the following items are also synchronized to provide a visual context of the alarm.

- The scenes that include where the devices are plotted
- The media objects and hi-res images that are used for schematic and 3D scenes
- The GIS maps service information that is used for geographic scenes

In Control Center, a site configured as a Federated Node sends the following object types from the local store to a configured Federated Hub:

- Alert States
- Contacts
- Contact Groups
- Date/Time Schedules
- Devices
- Folders
- Locations
- Media Objects
- Placeholders
- Scenes (Schematic and Geographic)
- Site References
- Users
- Windows Clients
- 3D Scenes (where 3D capability is included)

A Federated Hub site sends the following object types back to the Federated Node:

- Folders
- Locations
- Users

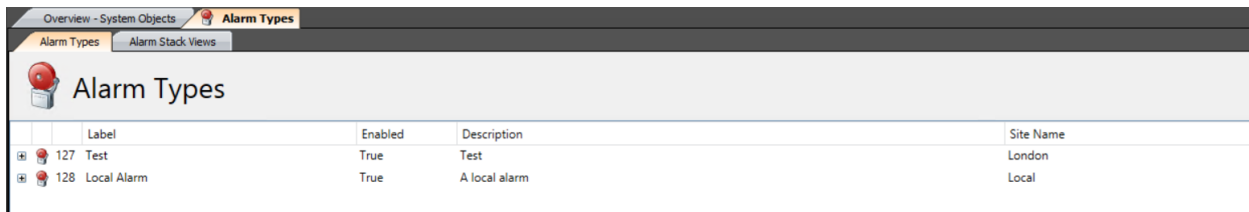
- Windows Clients

These objects are stored in the Federated Sites folder under the remote site that owns the content.

Federated sites can run independently of each other, therefore, a break in connectivity between the sites will not impact normal operational use of Control Center. When connectivity is restored, the Node site will begin synchronization of any alarms that were resolved during the outage. During this process, periodic checks for new alarms are made and any new alarms are synchronized immediately.

Federated Alarm Types

In addition to the base objects required for synchronizing sites that federate alarm data, the Hub requires the Alarm Types object, which represents the alarm logic that the Node site uses to evaluate whether to create an alarm or not. Instead of copying the entire Alarm Types Object to the Hub, individual Alarm Type definitions are added to the system Alarm Types Object that already exists on the Hub site.



	Label	Enabled	Description	Site Name
127	Test	True	Test	London
128	Local Alarm	True	A local alarm	Local

The originator of the Alarm Type definition can be viewed in the Alarm Types tab by opening the object and comparing the Site Name property.

All Alarm Types that originate from the local server will be labelled as Local. Any Alarm Types that originate from any remote site will be labeled with the name of the site. The name for each site is taken from the label of the Remote Federation Service object that links the sites together.

The logic for creating the alarm is evaluated at the site that owns the device generating the event which is typically the federated Node.

Each individual Alarm Type describes the conditions for creating the alarm, how the alarm point is determined, how the alarm will be described in the alarm stack as well as defining what happens at the various points of the alarm lifecycle.

The Alarm Type defines the Alarm Actions that will be executed when:

- Creating the alarm
- Handling the alarm
- Modifying the alarm
- Parking the alarm

- Resolving the alarm
- Using the Alert State for alarm creation

On the Federated Node site, Alarm Actions are used to define how an alarm is handled on the site that is local to the Alarm Types object.

Alarm Types Wizard

Collation & Alarm Actions

Collation:

- Collate by Location
- Collate by Alarm Point
- Collate by Alarm Type
- Collate by Track ID
- Collate by Event Property:

Alarm Actions:

	Response Plan	Alert State
Created:	None Set	Red
Handled:	Template Handled VRP	Yellow
Modified:	None Set	None
Parked:	None Set	Blue
Resolved:	None Set	Clear Alarm Point Alert

Threat Level:

Allow Bulk Resolving

< Back Next > Cancel

A Hub site that is remote from the Node site where the alarm originated may have different physical or geographic constraints when managing alarms. However, in Control Center, the Alarm Actions for an Alarm Type that originates from a Federated Node site can be modified to suit local requirements.

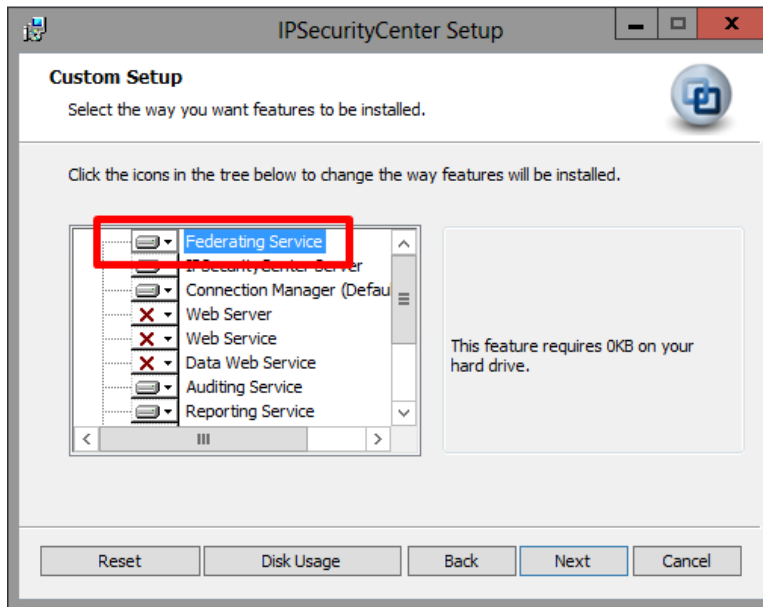
To modify the Alarm Actions for an Alarm Type, open the local Alarm Types object on the receiving site and edit the appropriate Alarm Type Definition to call the required Response Plans. When editing an Alarm Type from a remote site, all response plans are reset to None Set regardless of what was defined at the Node.

This allows configuration of appropriate responses to the various stages of the alarm lifecycle.

Setting Up a Simple Federating Control Center Environment

Configuring a simple environment that includes Alarm Synchronization between two sites requires that both sites are licensed to run Federated Control Center and the

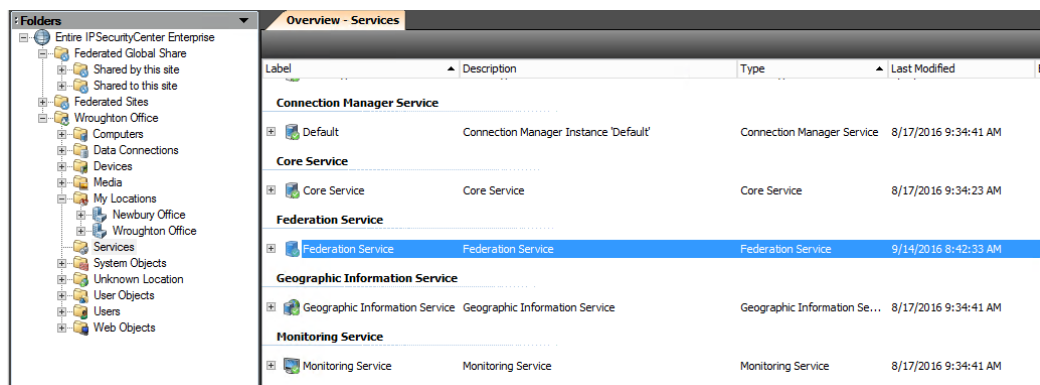
Federated option must have been selected during the installation process as shown below.



The Federating Service handles the communication between this server and all remote servers. The Federating Service must be running on both machines for the sites to Federate with each other.

The Federating Service object within System Configuration contains information related to the instance of Control Center that it is installed on.

To view this information, open System Configuration and click the Services > Federation Service object. An entity called Remote Federating Service object already exists in the system to store the Federating information about the remote site.



To successfully establish communication between two sites, each site must have a Federating Service and a Remote Federating Service.

Federating Service Object

As part of the Federating Service object, the following properties are available.

Label	Description	Type	Last Modified	Extra Information
Federation Service				
Federated Service	Federation Service	Federation Service	7/22/2016 4:00:49 PM	

Connection Settings	
Load Balanced Host Name	hostname.dev.cnluk.com
Load Balanced Port Number	9901
Password	*****
General Settings	
Alarm Types Service	Alarm Types Service
Core Service	Core Service
Created	4/18/2016 9:20 PM
Description	Federation Service
Enabled	True
Environment	Production
GeographicInformationService	Geographic Information Service
Label	Federated Service
Notification Service	Notification Service
Owner	System
Rules Engine Service	Rules Engine Service
Schedule	No schedule set
Tag	
Permissions	
Security	Security Settings

Connection Settings Properties

- **Load Balanced Host Name** - The fully qualified name for the server address. This value is determined automatically as the HOSTNAME reported by the operating system. This value cannot be changed by the user. When connecting to this server from another, use this value as the Host Name to connect to.
- **Load Balanced Port Number** - The port that the Federated service used to communicate on. This is currently a fixed value that cannot be changed.
- **Password**- Any remote instance of Control Center that wishes to share data with this site must include this password as part of the Remote Federating Service Object configuration.

General Settings Properties

The following General Settings are automatically configured when the system is set up to federate with another instance of Control Center. Everbridge recommends that the following default values are not changed:

- **Alarm Types Service** - The Alarm Types Service that is running on the local server.
- **Core Service** - The Core Service running on the local server.
- **Geographic Information Service** - The Geographic Information Service running on the local server.
- **Notification Service** - The Notification Service running on the local server.
- **Rules Engine Service** - The Rules Engine Service running on the local server.

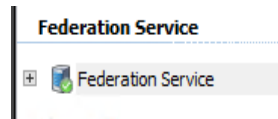
The rest of the settings are standard Control Center settings, which include **Created**, **Enabled**, **Environment**, **Label**, **Description**, **Owner**, **Schedule**, and **Tag**.

Permissions

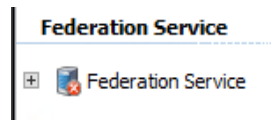
You can control which users have the Read, Write, or Execute permissions on the Federating Service Object using the standard Control Center controls.

Object States and Statuses

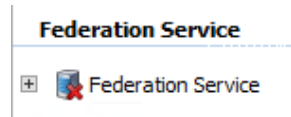
The Federating Service object can be enabled or disabled using the standard Control Center controls.



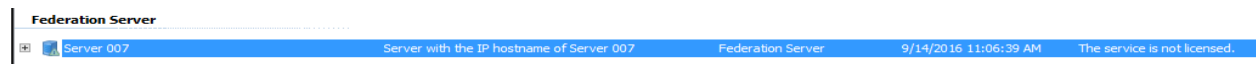
When enabled, the Federation Service will accept incoming data from, and send data to other remote sites through appropriately configured Remote Federation Service objects. If an exception occurs, the Federation Service will remain Enabled, but may revert to an Offline state.



A disabled Federation Service does not attempt to send or receive information from remote sites.

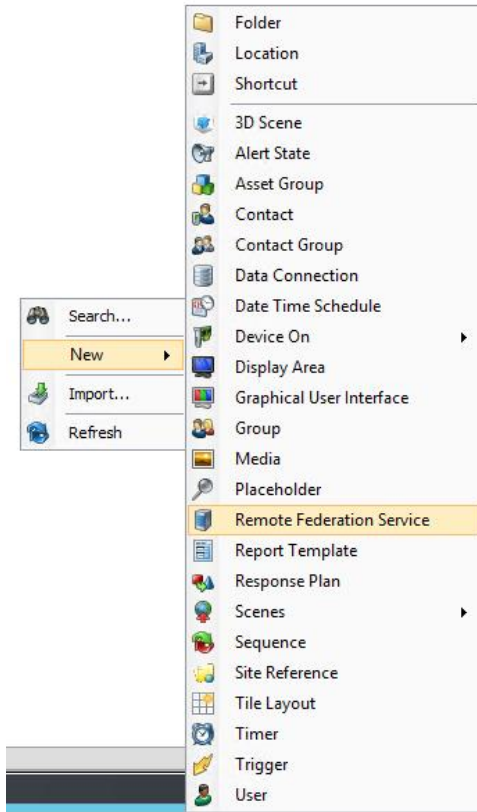


A Federation Service object can also be enabled and offline at the same time, for example, when the service is trying to communicate and encounters an exception. The most common exception is that the Federating module is installed but not licensed correctly. Check the Federated Server in the Computers folder for further information.

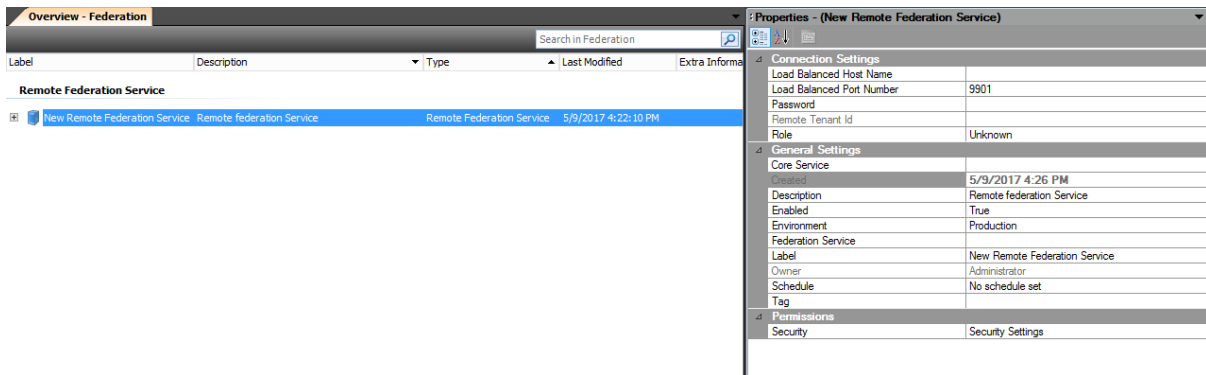


Remote Federating Service Object Properties

You can create a new Remote Federating Service object by clicking **New > Remove Federation Service**. This object stores the connection details for the remote site.



After creating the new object, complete the appropriate properties, for example, which remote Host to connect to, the Local Core Service, and Federating Services.



Time	The local time of the message.
Context	The source of the message that may refer to an RFS or the Hostname stored within the Federation Service.
Message	The details of the message.

Operation	The operation type the message refers to.
Status	This provides additional information on the operation that is being performed.
Mode	Provides a description to indicate whether the message describes a Send or a Receive operation. None may be shown for status update messages.

Connection Settings Properties

- **Load Balanced Host Name:** The address of the remote computer that is being connected to. This information is stored in the Federating Service object properties on the remote computer.
- **Load Balanced Port Number:** A read-only value for the port number that will be used to communicate with the remote machine. Changes to which port is used for communication may be made with support from Everbridge.
- **Password:** The password required to connect to the remote machine. This value must match the password set on the Federating Service on the remote system.
- **Remote Tenant ID:** The unique identifier that identifies the content from each remote site. It is not editable and is provided for information and diagnostic purposes only.
- **Role:** This property defines whether the Remote Federating Service object acts as a Sender or Receiver of alarms. Federated Node sites must be configured with the role set to Sender. This will send alarms and event data associated to Alarms to the Federation Service of the specified Hub. Federated Hub sites must be configured as Receiver. This will receive alarms and event data from the Federation Service of the specified Node. When the Remote Federating Service is initially created, the Role property will be set to Unknown and must be changed before the site will Federate.

General Settings Properties

- **Core Service:** Set this to point to the Core Service running on the local server.
- **Federation Service:** Set this to point to the Federating Service running on the local server. Created, Description, Enabled, Environment, Label, Owner, Schedule and Tag properties function per existing Control Center documentation.

Permissions

You can control which users have the Read, Write, or Execute permissions on the Remote Federating Service object as per the existing Control Center model.

Remote Federation Service object states and statuses

You can enable and disable Remote Federation Service objects using the standard Control Center controls.



Enabled and Online Remote Federation Service Disabled Remote Federation Service

To federate information between two sites, one site must be sending alarms and one must be receiving, and the Federation Services and Remote Federation Services at each site must be enabled and online. Additional information may be shown by the Remote Federation Service object, the Federation Service object or the Federation Server object.

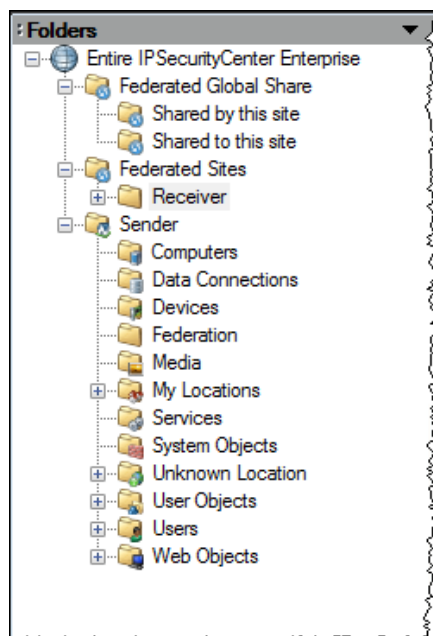


Enabled and pending Enabled and Offline

When an initial synchronization takes place, the Remote Federation Service will show as enabled and pending as shown in the figure above. If the initial synchronization takes longer than 30 seconds, the RFS may temporarily show as offline until the initial sync is complete.

Federated Control Center Instance

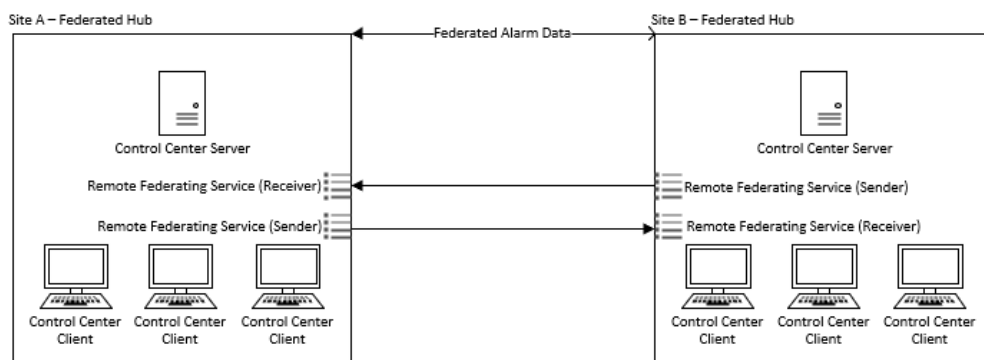
For a system to be correctly configured with Control Center Federated feature, additional System folders appear in System Configuration next to the default My Organization folder. The Federated Sites folders contain copies of the folders from each of the remote sites that this site is Federating data with.



The Federated Global Share folder contains content related to publishing, which is covered in more detail in **Publishing**.

Bi-directional Federation

Bi-directional Federation is when you configure a site as a Sender and Receiver of Alarms to the same site.



Federation Service Event Viewer and Loupe

For troubleshooting and diagnosing issues related to Federated Control Center instances, additional information is available within the Federation Service Event Viewer.

The Federation Service Event Viewer can be accessed in the following ways:

- In **System Configuration**, click **Services** and double-click the **Federation Service** object.

- Right-click the **Federation Service** object and select **Federation Service Event Viewer** from the context menu that appears.

The screenshot shows the Everbridge interface with a context menu open over the 'Federation Service' object. The menu options include: Search..., Search for more Federation Services..., New, Import..., Refresh, List Referencing Objects, Delete, Create Shortcut, Disable, Rename, and Federation Service Event Viewer (highlighted).

Below the menu is the 'Federation Service Events on 'S-007' window, which displays a table of events. The table has columns for Time, Context, Message, Operation, Status, and Mode.

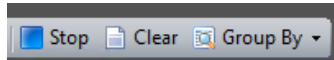
Time	Context	Message	Operation	Status	Mode
9/14/2016 11:47:26 AM	RFS for Sender to Server 006	Notification queue length 0	Sync	Processing	None
9/14/2016 11:47:23 AM	RFS for Sender to Server 006	Notification queue length 1	Sync	Processing	None
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync all objects completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync ThreatLevelSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync ThreatLevelSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmOfflineParkSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmOfflineParkSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmSync sync-all with: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Completed syncing 0 resolved alarms between 9/14/2016 10:45:52 AM and 9/14/2016 10:47:19 AM in 0.1	Sync	Sync	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Start syncing 0 resolved alarms between 9/14/2016 10:45:52 AM and 9/14/2016 10:47:19 AM	Sync	Sync	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Syncing check for current alarms	Sync	Sync	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Start AlarmSync sync-all with: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmResolutionTypeSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Finish AlarmResolutionType sync to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Start AlarmResolutionType sync to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmResolutionTypeSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmActivityTypeSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Finish AlarmActivityType sync to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Start AlarmActivityType sync to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmActivityTypeSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync CorrelatedAlarmTypeSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Finish CorrelatedAlarmType sync to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Start CorrelatedAlarmType sync to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync CorrelatedAlarmTypeSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmTypeSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Finish AlarmType sync to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Start AlarmType sync to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlarmTypeSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlertSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync AlertSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync ObjectStateSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sending object states for 13 objects to Remote Federation Service: RFS for Sender to Server 006	Sync	Sync	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync ObjectStateSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync VisibilityObjectMappingSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Saving GIS layers	Sync	Saving	Incoming
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync VisibilityObjectMappingSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync FolderMappingSync completed to: RFS for Sender to Server 006	Sync	Complete	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync FolderMappingSync started to: RFS for Sender to Server 006	Sync	Start	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Completed publishing to: RFS for Sender to Server 006	Publish	Success	Outgoing
9/14/2016 11:47:19 AM	RFS for Sender to Server 006	Sync changes requires 1 objects	Sync	Complete	Incoming

The Event Viewer provides a real-time view of status messages from the Federation Service. It is divided into the following columns:

Time	The local time of the message.
-------------	---------------------------------------

Context	The source of the message that may refer to an RFS or the Hostname stored within the Federation Service.
Message	The details of the message.
Operation	The operation type the message refers to.
Status	This provides additional information on the operation that is being performed.
Mode	Provides a description to indicate whether the message describes a Send or a Receive operation. None may be shown for status update messages.

When the Federation Service Event Viewer is displayed, the following buttons appear on the toolbar that allow the user to interact with the message list.



The **Stop** button stops the viewer from updating. When clicked, the button will change to **Start** and new messages will not be displayed in the Viewer.

The **Clear** button clears all messages from the Event Viewer Window. These messages cannot be recovered although they may still be viewed using Loupe.

The Group By groups the list of messages by Context, Operation or Mode. This can be useful when troubleshooting.

Time	Context	Message	Operation	Status	Mode
Sync (47 Items)					
3/22/2018 2:33:54 PM	Site 1 > NOC	Notification queue length 0	Sync	Processing	None
3/22/2018 2:33:50 PM	Site 1 > NOC	Notification queue length 1	Sync	Processing	None
3/22/2018 2:33:50 PM	Site 1 > NOC	Threat level changed: OldThreatLevel: 1, NewThreatLevel: 1, TenantId: 1072bc7-7128-e811-968a-0050	Sync	Saving	Incoming
3/22/2018 2:33:49 PM	Site 1 > NOC	Receiving object states for 43 objects	Sync	Saving	Incoming
3/22/2018 2:33:49 PM	Site 1 > NOC	Saving GIS layers	Sync	Saving	Incoming
3/22/2018 2:33:49 PM	Site 1 > NOC	Sync changes requires 1 objects	Sync	Complete	Incoming
3/22/2018 2:33:49 PM	Site 1 > NOC	Calculating changes for 77 objects	Sync	Info	Incoming
3/22/2018 2:33:46 PM	Site 1 > NOC	Sync all objects completed to: Site 1 > NOC	Sync	Complete	Outgoing
3/22/2018 2:33:46 PM	Site 1 > NOC	Sync ThreatLevelSync completed to: Site 1 > NOC	Sync	Complete	Outgoing
3/22/2018 2:33:46 PM	Site 1 > NOC	Sync ThreatLevelSync started to: Site 1 > NOC	Sync	Start	Outgoing
3/22/2018 2:33:46 PM	Site 1 > NOC	Sync AlarmOfflineParkSync completed to: Site 1 > NOC	Sync	Complete	Outgoing
Connection (7 Items)					
3/22/2018 2:33:49 PM	Site 1 > NOC	Successfully connected to: Site 1 > NOC (test3server.cnluk.com:9901)	Connection	CreateSession	Incoming
3/22/2018 2:33:49 PM	Site 1 > NOC	Connect request from: Site 1 > NOC	Connection	Connect	Incoming
3/22/2018 2:33:45 PM	Site 1 > NOC	Connected to Site 1 > NOC	Connection	Success	Outgoing
3/22/2018 2:33:45 PM	Site 1 > NOC	Response from Site 1 > NOC : ConnectionResult: Success, Federation Compatibility Version: 2.1.0.0	Connection	Success	Outgoing
3/22/2018 2:33:45 PM	Site 1 > NOC	Connecting to Site 1 > NOC	Connection	Start	Outgoing
3/22/2018 2:33:45 PM	Site 1 > NOC	RemoteConnectionManager.Start: Connecting to remote site: Site 1 > NOC	Connection	Connection	None
3/22/2018 2:33:45 PM	Site 1 > NOC	SyncRequest Invalid Session Id: b3773761-46bc-43e2-80d3-780fd9617feb	Connection	ValidateSession	None
Publish (4 Items)					
3/22/2018 2:33:45 PM	Site 1 > NOC	Completed publishing to: Site 1 > NOC	Publish	Success	Outgoing
3/22/2018 2:33:45 PM	Site 1 > NOC	Publishing 0 GIS layers	Publish	Info	Outgoing
3/22/2018 2:33:45 PM	Site 1 > NOC	Publish changes required 0 objects	Publish	Info	Outgoing
3/22/2018 2:33:45 PM	Site 1 > NOC	Initialise publishing to: Site 1 > NOC	Publish	Info	Outgoing
StateChange (4 Items)					
3/22/2018 2:33:45 PM	Site 1 > NOC	Connected to test3server.cnluk.com	StateChange	Info	Outgoing
3/22/2018 2:33:45 PM	Site 1 > NOC	Federation Service enabled = True, Remote Federation Service enabled = True	StateChange	StateChange	None
3/22/2018 2:33:43 PM	Site 1 > NOC	Disconnected from test3server.cnluk.com	StateChange	Warning	Outgoing
3/22/2018 2:33:43 PM	Site 1 > NOC	Federation Service enabled = True, Remote Federation Service enabled = False	StateChange	StateChange	None

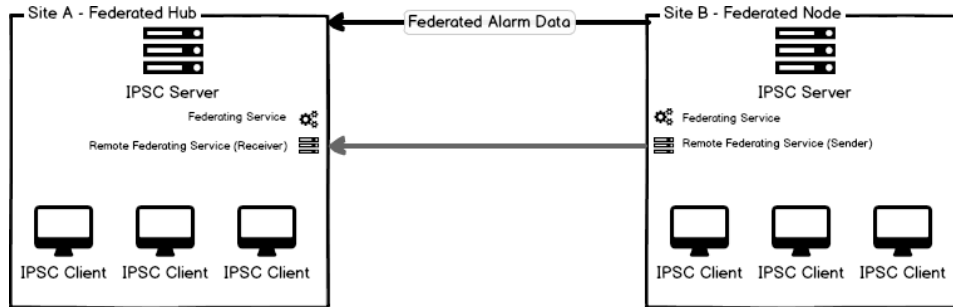
In addition, right-clicking the message list allows either an individual message or the entire log to be copied, as a comma-separated list to the Windows clipboard.

The Federation Service also records diagnostic information in Loupe.

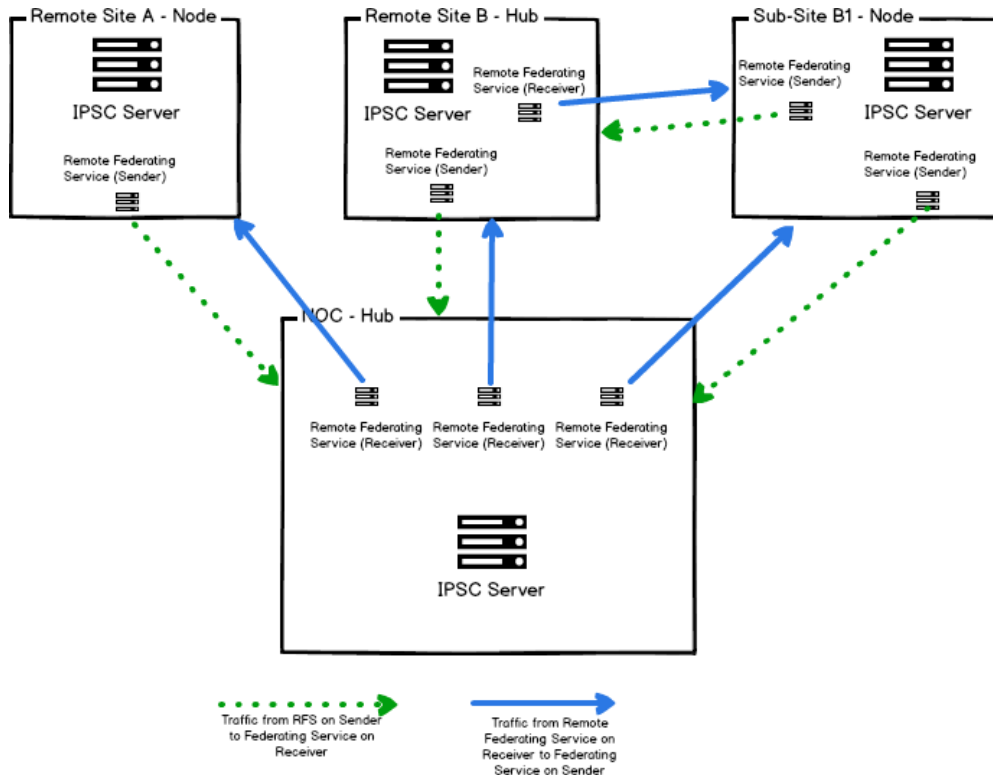
Product	Application	Environme...	Promc
IPSecurityCen...	Windows Client		
IPSecurityCen...	Notification Service		
IPSecurityCen...	Core Server		
IPSecurityCen...	Security Service		
IPSecurityCen...	RulesEngine Service		
IPSecurityCen...	VideoExport Service		
IPSecurityCen...	Monitoring Service		
IPSecurityCen...	Geographics Service		
IPSecurityCen...	Federation Service		

Setup of Multiple Federating Control Center Environments

When configuring multiple systems that are federating, each pair of systems must have a Hub and Node configured.



For complex networks of Federating Systems, pairs of Nodes and Hubs must be configured appropriately.



In the above figure, the central NOC site acts as a Hub and receives alarms from Nodes configured at Remote Site A, Remote Site B and from Sub-Site B1. Therefore, there are three Remote Federating Service objects configured as Receivers at the NOC site. A Remote Federating Service configured as a Sender is present at each of the sites and sub-sites to send alarms to the NOC.

At Remote Site B and Sub-Site B1, there is another relationship wherein Sub-Site B1 federates alarm data to Remote Site B. Therefore, Remote Site B must be configured and licensed as a Hub that supports sending and receiving Alarm data. This supported

configuration ensures that Remote Site B can act as a point of escalation for Sub-Site B1 and that the NOC can act as a point of escalation for both.

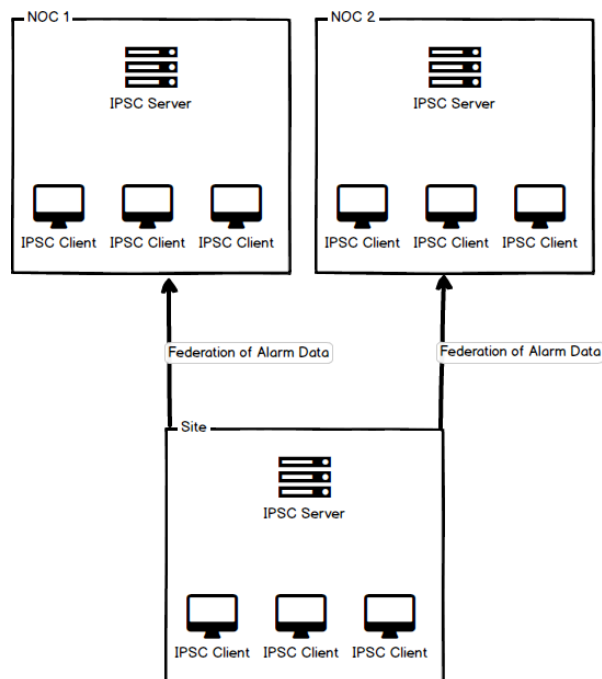
Remote Site B will not forward any alarms it receives from Sub-Site B1 to the NOC.

Non-Supported Federating Scenarios

The following scenarios are not currently supported in Control Center.

Multiple NOC Federation

Part of the core requirement for successful alarm federation between instances of Control Center is that each site involved in the communications must allow users to handle and manage alarms on behalf of a remote site. For example, in Site Federating Alarm Data to Multiple NOC's, the only source of alarm data comes from the site. The Site performs initial synchronization activities with both NOCs which means that both NOCs have a copy of the information required to resolve an alarm originating from the Site. The site does not pass through any information about NOC 1 to NOC 2 or vice versa. This means that if a user at one of the NOCs handles an alarm, this cannot be accurately presented at the other NOC.



Pass Through Federation

When a site behaves as both Node and Hub to different sites (as shown in the above figure), the configuration will not support the passing through of data from the lower levels to the top level. Each Federating Server pair must have Remote Federating Services configured for each communication pathway.

Content Ownership

In a Federated environment, the ownership and ability to edit content is of utmost importance. Normally, an object that is owned by a remote instance of Control Center cannot be edited on any site other than the owning site regardless of individual user permissions.

Each instance of Control Center includes a tenant ID to identify which site owns each piece of content. The Tenant ID information is not visible on objects but the Tenant ID for a remote system is stored in the properties of the Remote Federation Services object for the site.

Data Connections and Alarm Types Alarm Actions are the only exception which are described in later sections.

The Alarm Actions (from an Alarm Types object) can be modified at a local site to configure local responses to alarm conditions (see [Federated Alarm Types](#)).

Location Reference

Using Location References, a control room user can interact with the locations and devices that are managed at a remote site.

As Location References use the location data that is already synchronized through Federation, they only work between sites that are federating data between them and are designed to allow Hub sites to view the content from connected Node sites. Location References do not allow Locations and Devices from a Hub to appear at the Node site. In addition, during Federation, Location References are sent by Federating Nodes, and are not sent back by the Hub.

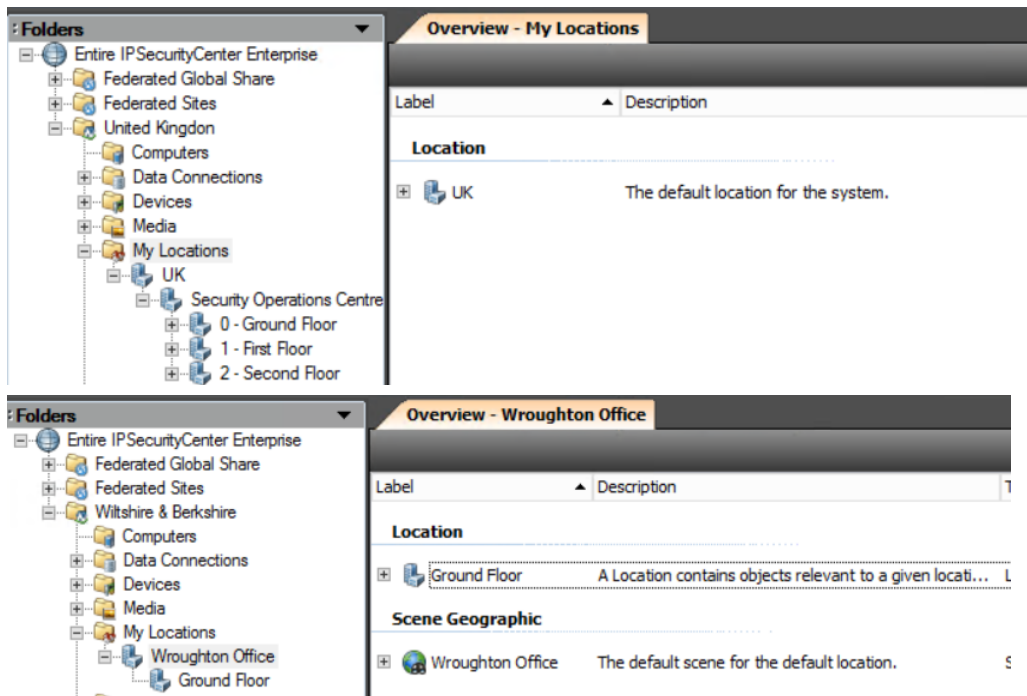
You can publish Location References to remote sites using the Publish feature. This publishes the Location Reference object and not the underlying Locations to the receiving sites.

Typically, users located at the site where the devices are deployed are responsible for location maps and devices. Control Center allows users to leverage this information dynamically across federating sites to ensure that updates to locations, devices, and other useful information is kept synchronized with the least possible delay.

You can also create multiple Location References to the same remote instance of Control Center. For backward compatibility purposes, Location References on upgraded sites will continue to operate as designed.

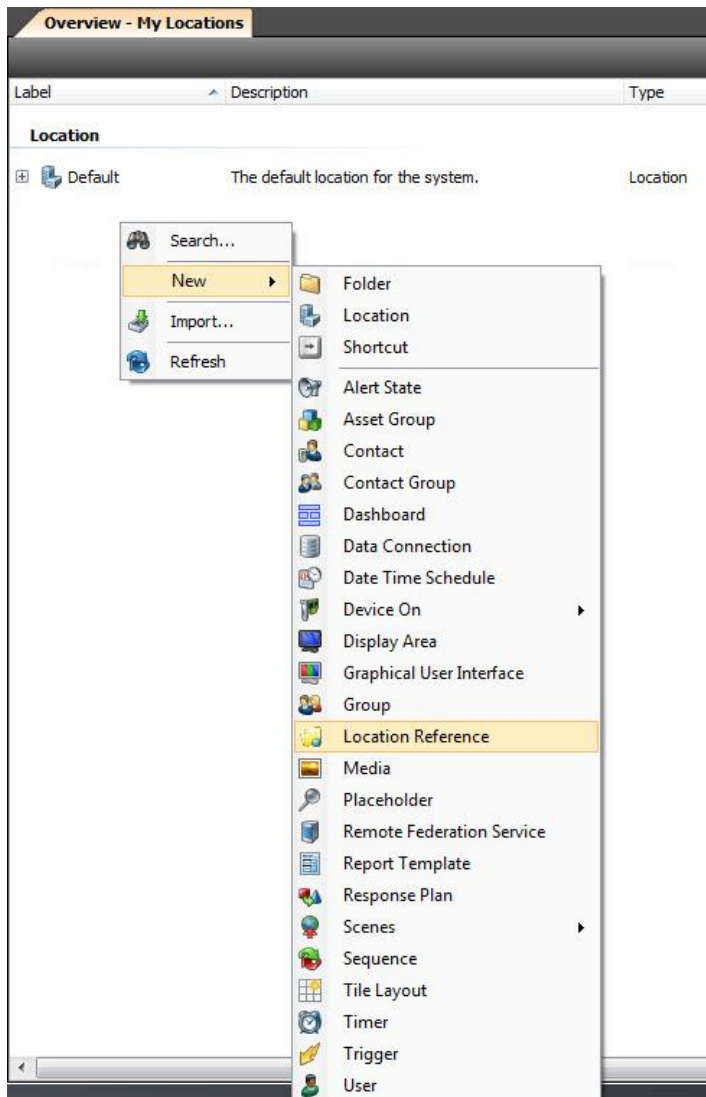
Location Reference example

Consider two sites that are federating: Site 006 which is a Hub and Site 007 which is a node.

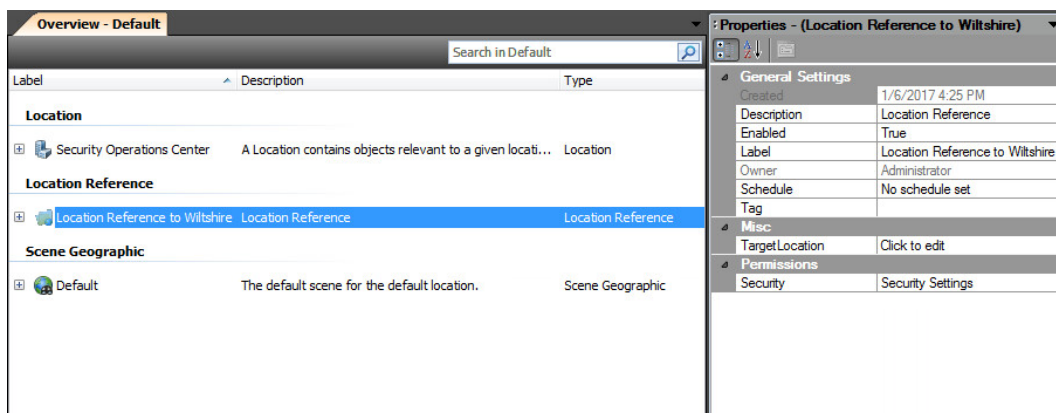


Creating a Location Reference on Site 006 (configured as a Hub) in the UK location allows the Locations, Scenes, and Devices configured on Site 007 (configured as a Node) to appear within the Control Room Client UI for users at Site 006.

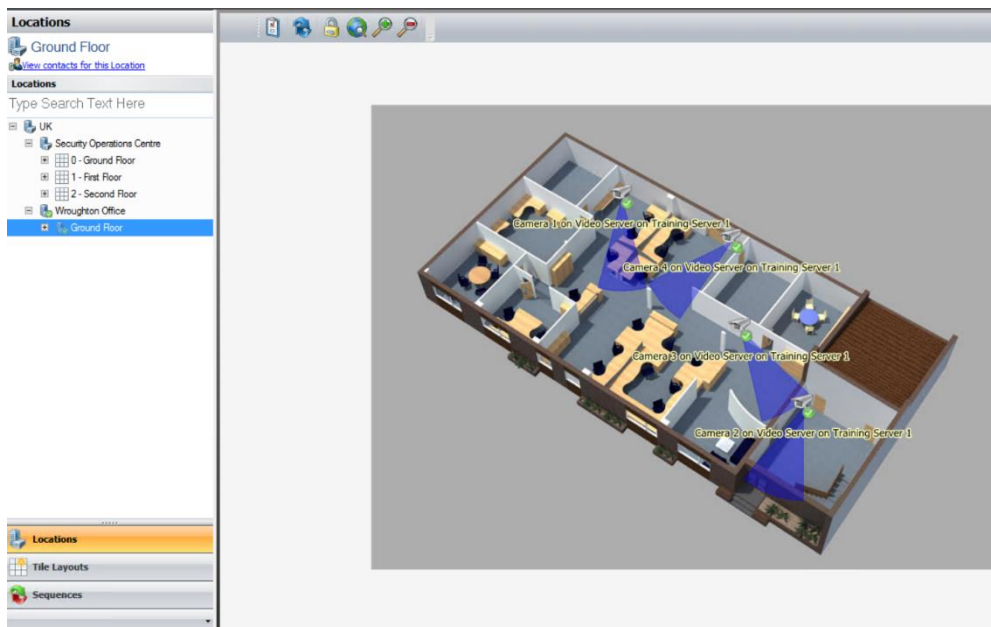
To create a new Location Reference, right-click the context menu and select **New> Location Reference**.



After adding a label for the Location Reference object, select the TargetLocation property from the remote site.



The main interface shows the locations from the remote server in the System Explorer. These locations behave in the same manner as a locally configured location as displayed in the Location Reference displayed to End User figure.



Once the Location Reference is created, it can be treated as any other object in Control Center System Configuration.

The label that appears on screen will be the label of the Location at the remote site.

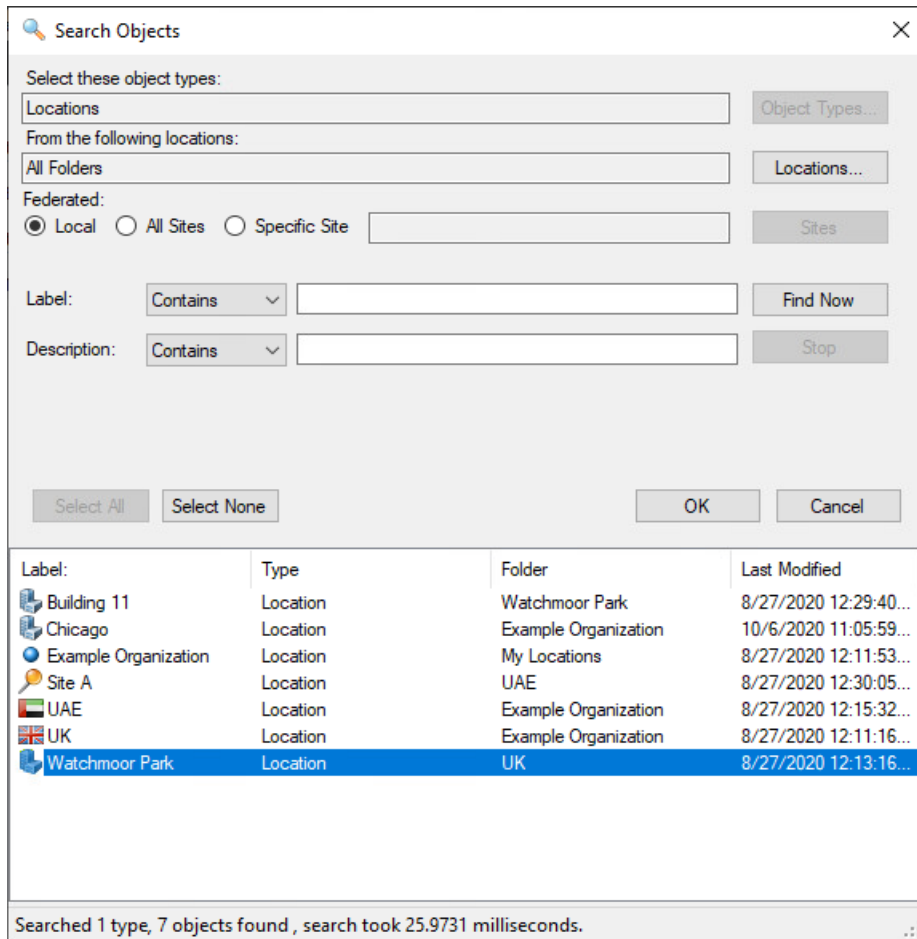
You must restart the Control Center Client after moving a Location Reference to a new location to get the correct alarm counts in the System Explorer.

Configuring Location Reference to Appear as Base Location

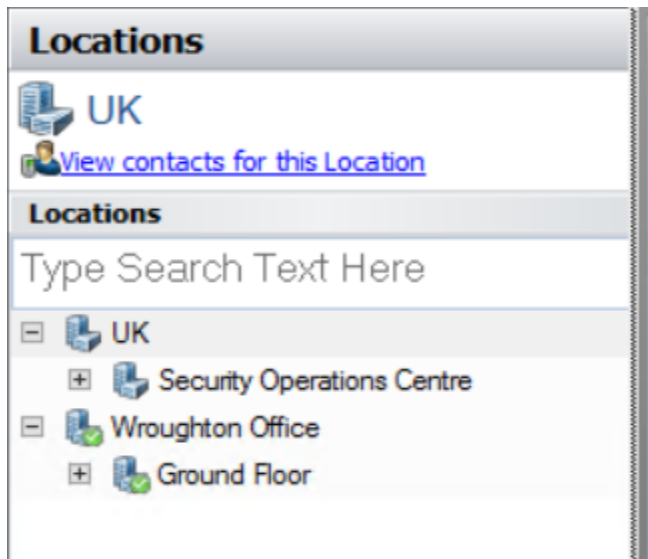
You can configure a Location Reference as a base location in the System Explorer GUI.

To configure a location reference to appear as base location:

1. From **System Objects**, open **System Explorer** and edit **Locations** by selecting the **Base Locations** property. The following dialog appears:

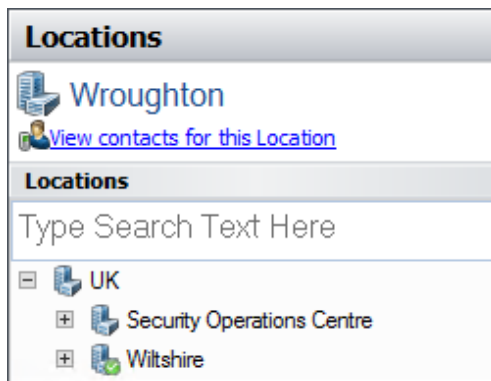


2. Select the **All Sites** option to configure the System Explorer to show any remote location without using a **Location Reference**. In the **Search** dialog showing **All Sites**, the remote site Wroughton Office is configured as a base location beside the local, Location UK.



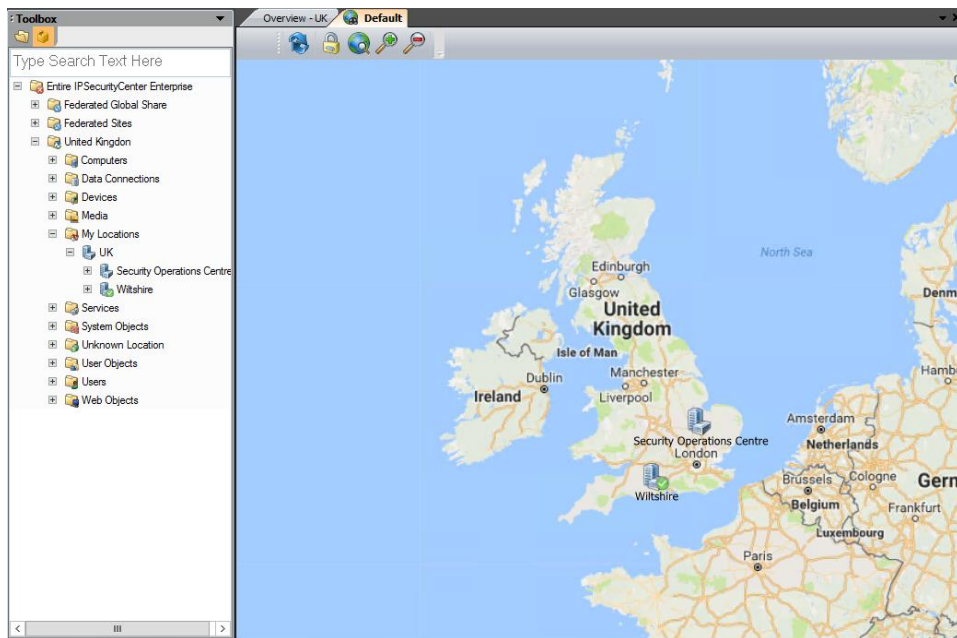
Circular Location References

Location References can refer to a remote site which itself has a location reference to the original location. However, it requires the Location information to be federated to the locations concerned and that the Location Reference object has been Federated or Published to the site concerned.



The above figure shows a site where a circular reference is configured. The Top location UK includes a Location Reference to the remote location Wiltshire. This remote location contains two locations as well as a Location Reference back to UK.

Expanding the Wiltshire location shows the two locations at the Wiltshire site, namely Newbury Office and Wroughton Office in addition to the location UK. You can expand it to reveal the locations for the UK site which will include the references to the Wiltshire location.



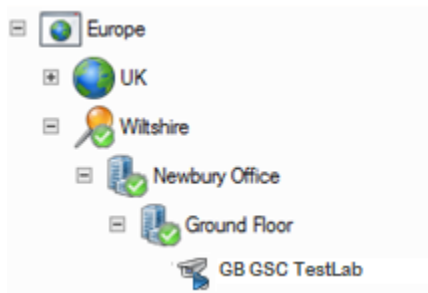
For example, in the above figure Security Operations Centre location and the Wiltshire location are plotted on the scene. Wiltshire location is available due to a Location Reference to a remote server.

The plotted asset acts as a standard plotted location and will observe all the default behaviors for alerting, icon display, and zoom levels.

Location References are transparent to Alarm Alert State Parent propagation, that is the Alert States that the remote sites generate will continue to alert parent Location Types as defined in the Alert State property regardless of whether the Locations are local or at a remote site. For more information, see [Managing Alert States](#).

Location and Device Online Status on System Explorer and Map

Locations and Devices that are owned by a remote site support showing the online state for the device or location.



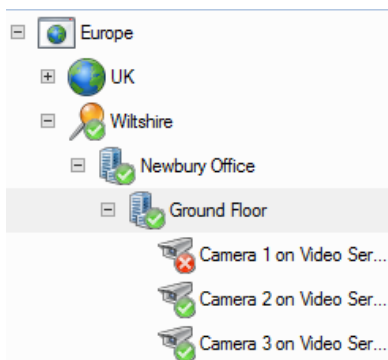
In the above figure, Europe and UK are local to the site, therefore no online state is shown on the icon. For all items in the tree below Wiltshire which are provided from a

remote site, a green check icon appears to indicate that the Devices and Locations are online.

Similarly, when viewing these icons plotted to a scene, the same green check appears. If the video is being displayed on a tile, then the green check icon is replaced with a blue play button.



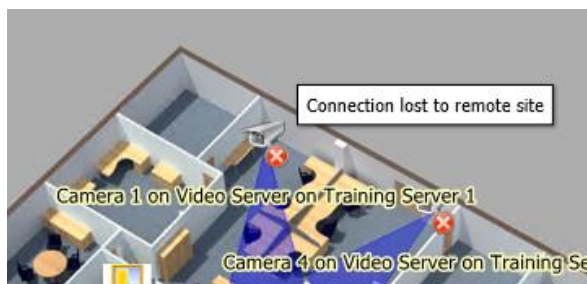
Individual devices that are disabled on the site owned by them, appear with a red cross icon as shown below:



In addition, if the federated communication between the Hub and Node site is interrupted by communications outage or by disabling the Federation Service links, then all devices and locations are set to offline.



For additional information, check System Configuration or hover the mouse over a plotted item as shown below:



When connections are restored to the remote site, the User Interface shows the status of all devices and locations at the remote site.

Handling Exceptions

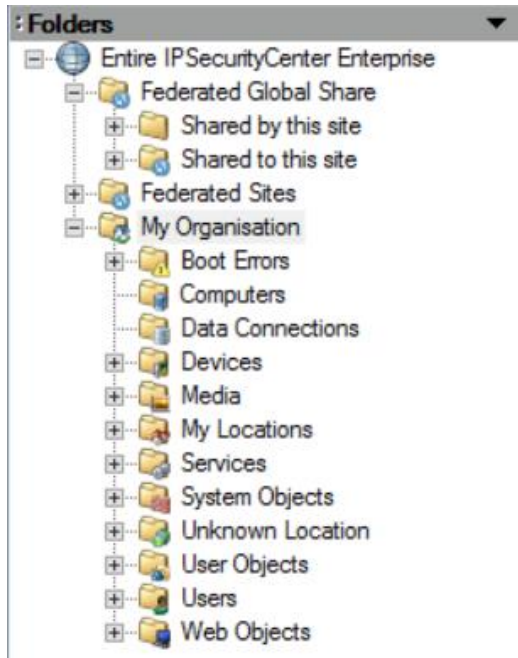
When a Federated Service encounters an exception from a remote site, the Service will disconnect from the remote site and reconnect forcing an initial sync. This is designed to resolve most scenarios where an exception occurs.

Publishing in Federated Control Center

Federated Control Center enables sharing objects between individual instances of Control Center, which is termed as Publishing. It allows one installation of Control Center to deploy copies of objects to other instances of Control Center electronically to ensure that all the connected installations are using the same Response Plans, GUIs and Process Guidance.

Publishing is included with the Federated license in Control Center.

A Hub or Node site that is configured and licensed to federate with another site can send and receive Published objects to and from another Hub or Node instance of Control Center.



For a system that has Control Center Federated feature enabled, additional System folders appear in System Configuration along with the default My Organization folder.

The Federated Global Share folder includes the following System folders:

- Shared by this site
- Shared to this site

Objects to be published must be placed within the Shared by this site folder. Also, any object that has a dependency of a Published object must also be published otherwise the Publish process will fail validation checks.

There is currently no option to rename sub-folders within the Shared to this Site folder in Federated Global Share.

The following objects can be published:

- Alarm Media
- Alarm Types
- Alert State
- Client Templates
- Contact
- Contact Groups
- Dashboard
- Data Connection

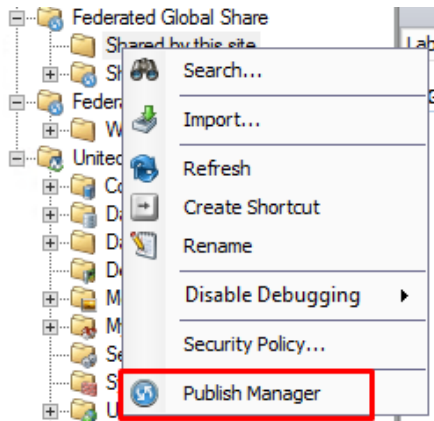
- Date Time Schedule
- Display Area
- Folder
- Graphical User Interface
- Hot Key Mappings
- Local Enterprise Settings
- Location
- Location Reference
- Media
- Modern Client Theme
- Response Plan
- Tile Layouts
- Timers
- Triggers
- User Group
- 2D Scenes (Schematic and Geographic)
- 3D Scene

Publishing a Federating Object

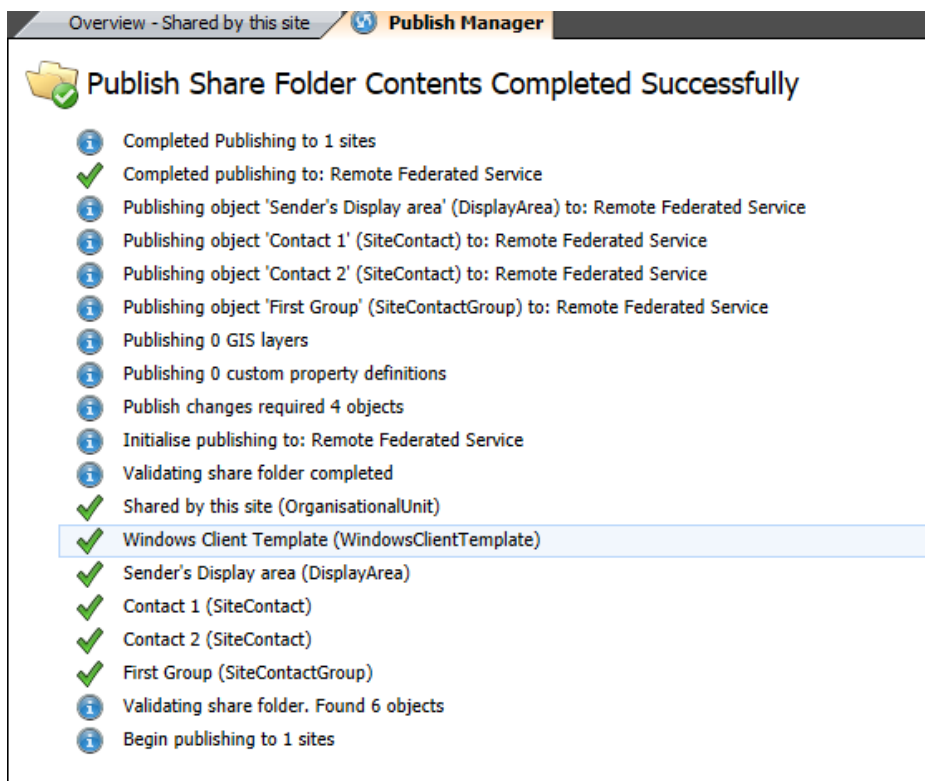
You can publish an object that is federating using the Publish Manager to post content to remote sites. The following example describes how to publish contact and contact groups.

To publish contact and contact groups:

1. Create two sites and set up a federated environment. That is, set up servers on two different machines with one client for each server, for example a Sender and Receiver.
2. Create the following contacts and the contact groups to start with:
 - **New Contact 1**
 - **New Contact 2**
 - **Contact Group 1** (via add members)
 - **Contact Group 2** (via add members)
3. From the **Sender's** client, right-click the **Shared by this site** folder and select **Publish Manager**. The **Publish Manager** screen opens.



4. Click **Publish**. The **Contact** contents are published to the **Receiver's Site**.



5. On the **Receiver** site, view the folders to see the newly created contacts and contact groups appear.
6. Log in to the other machine to check if they are federating. View the **Shared to this site** folder received from the other site.
7. Replicate the same steps on the **Receiver** machine to create the same **Contact Groups & Contacts** on the other site.
8. Check the **Federation Service Events** to see the objects that are getting federated. The newly created items should appear in the list.

You can use the **Clone** from button in the **Setup Display** dialog to clone display configuration from a published **Client Template** object to clone Windows display configuration.

Publish Manager

The Federated sites folder contains sub-folders for each site that the current system is federating with. Each sub-folder is labeled as the name of the RFS that links the site together when the Federation Service first starts.

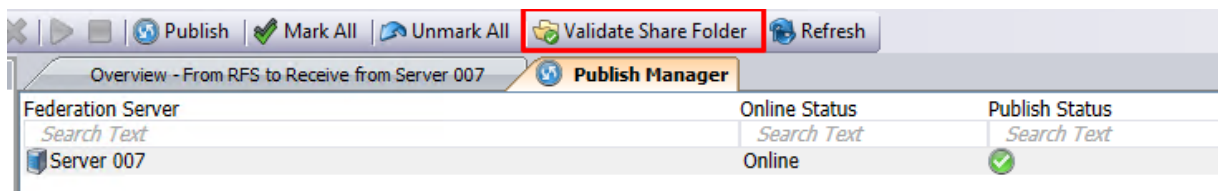
As Publishing tasks differ from automatic synchronization, there is no feature that will automatically keep published content up to date across all the sites, therefore Publishing requires individual Publish session to be initiated by a user.

Publishing has been designed to support simultaneous content distribution to multiple end points. Performance of Publishing content is influenced by the bandwidth and latency between the servers as well as the resources available to the site that initiates the publish.

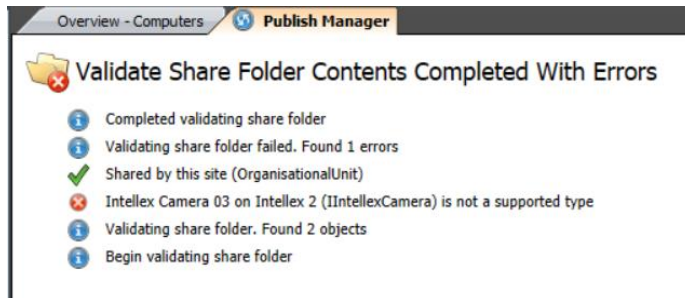
To retain system integrity, Control Center enforces consistency checks before a publish action takes place. This ensures the dependencies (if any) are present and that no unsupported object types have been moved or copied into the folder.

If a Published asset depends upon another asset, it must also be present in the Publish folder. If an object fails the dependency checking process, the publish action will be aborted. Dependency checks will check all references to users or groups, therefore it is recommended to use Active Directory Groups rather than Control Center groups when building published content.

You can perform a consistency check without Publishing, using the Validate Share Folder option in Publish Manager.



After a successful validation step, Publishing will check for any existing content on the remote site and send anything that is missing in each site to bring the remote sites up to date with the content.



When the content is published, the Publishing site retains ownership of the content, and the copy of the content is published to the selected site folder, which will be read-only on any site that receives it.

For assets that include complex editors (GUIs, Response Plans), remote sites that receive these objects can view the asset in a read-only editor to assist with troubleshooting. Response Plans can also be debugged without having to modify the properties of the Response Plan. For more details, see [Debugging Published Content](#).

For every installation, only one concurrent Publish is supported. A second Publish cannot be started if a Publish is already occurring.

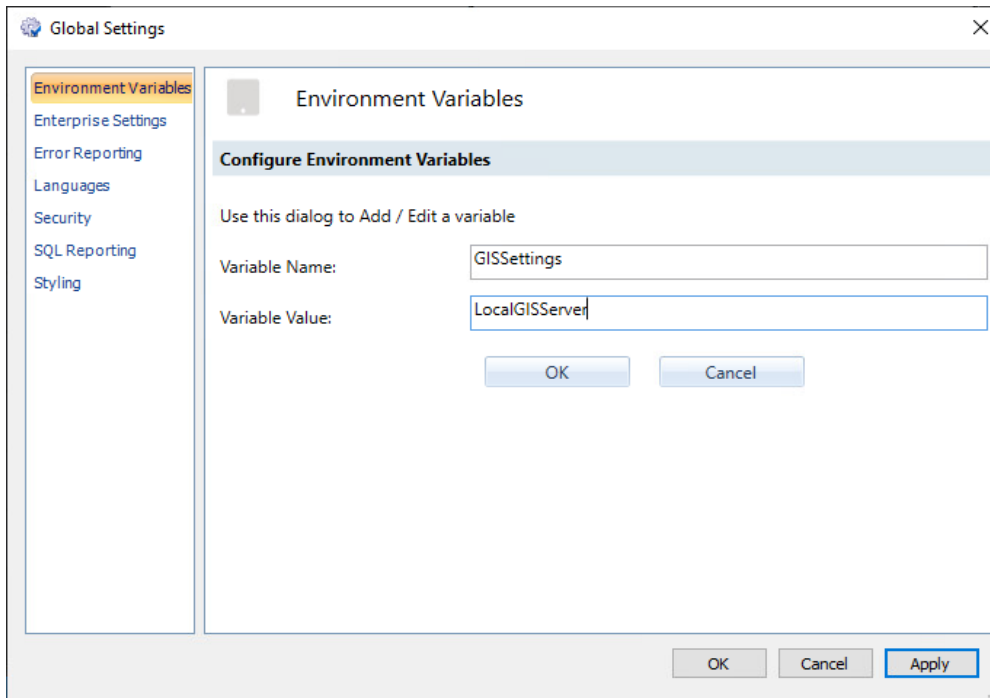
As shown in the Validate Share Folder figure, you can identify when a remote site has copies of the latest contents of the Publish folder, whether all sites are currently online, the date of the last attempted Publish and any errors that occurred during the last Publish process.

Users and Groups

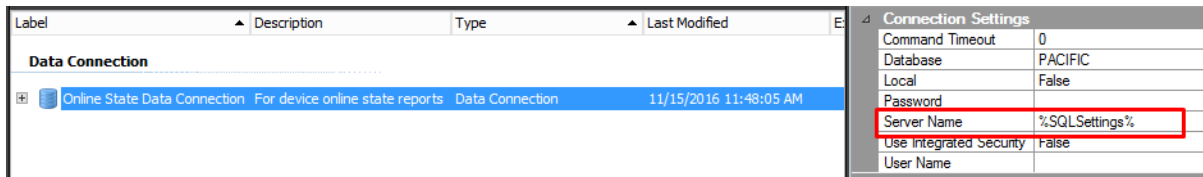
Publishing does not currently support the publication of User Accounts. Therefore, when you have to publish content that is dependent upon or restricted by User from one instance of Control Center to another, you must configure it using Active Directory Users and Groups.

Environment Variables

Environment Variables allow published content to interact with local configurations. Environment Variables are useful when specifying GIS layer information and in Data Connections. Environment Variables are managed in **System Configuration > Global Settings > Environment Variables**.



The environment variable is represented as `%variablename%`. During evaluation, the server looks up the variable name against the list of locally defined environment variables and replaces the value stored in the environment variable for the required value. In the figure below, the data connection to Pacific connects to the SQL Server called `%SQLSettings%` which resolves to `LocalSQLAddress` of the site.



For a GIS Layer, the environment variable is used as part of the address for a WMTS service, where the value `http://%GISSettings%:8180/geoserver/gwc/service/wmts` is published to multiple sites, and each site can individually define the value for `%GISSettings%`.

Version

Enter an address of a [ServiceType] and click Go, to list the available layers.

Address:

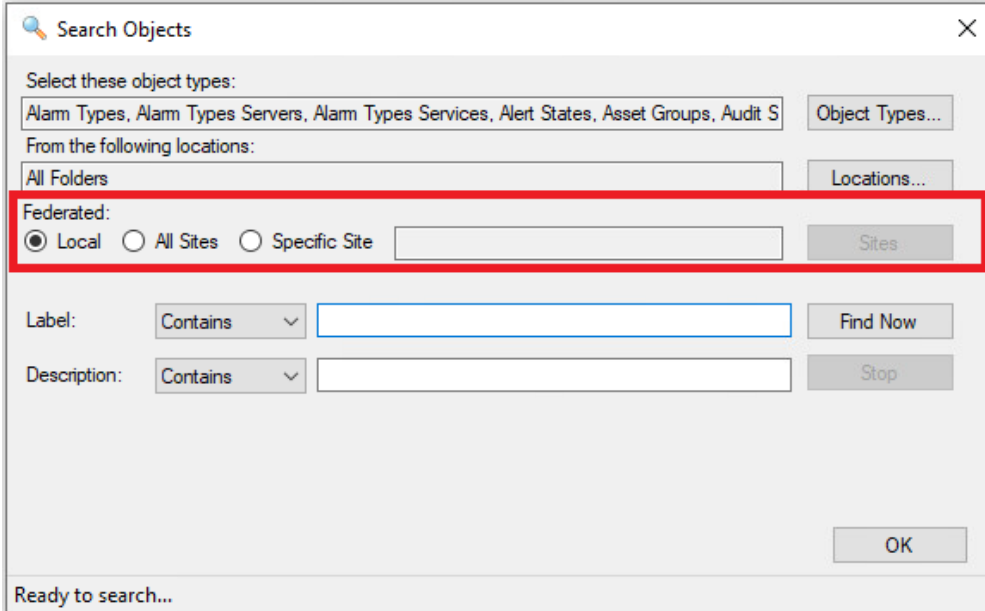
Layers:

Selected Layer:

EPSG:

Search

Federated and published content may be searched through using the existing search capabilities. The **Search Objects** dialog (in System Configuration) allows searching through content received from remote installations.

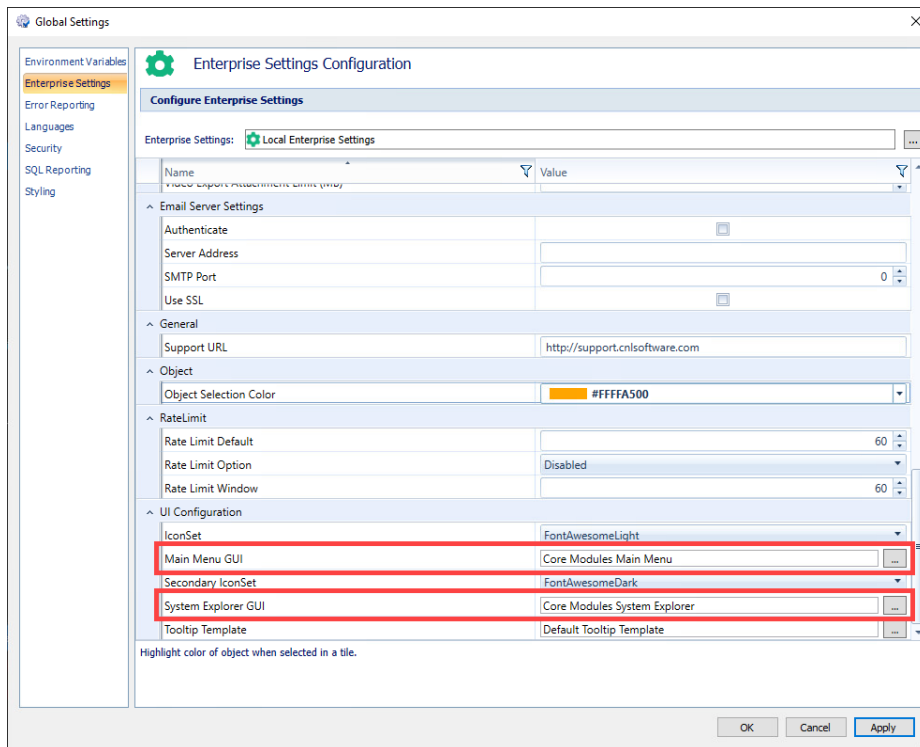


By default, the **Search** function will continue to search through the objects stored on the local server. Additionally, you can search across all Federated Sites or through the contents of a specific Site.

Published System Explorer and Main Menu GUI Controls

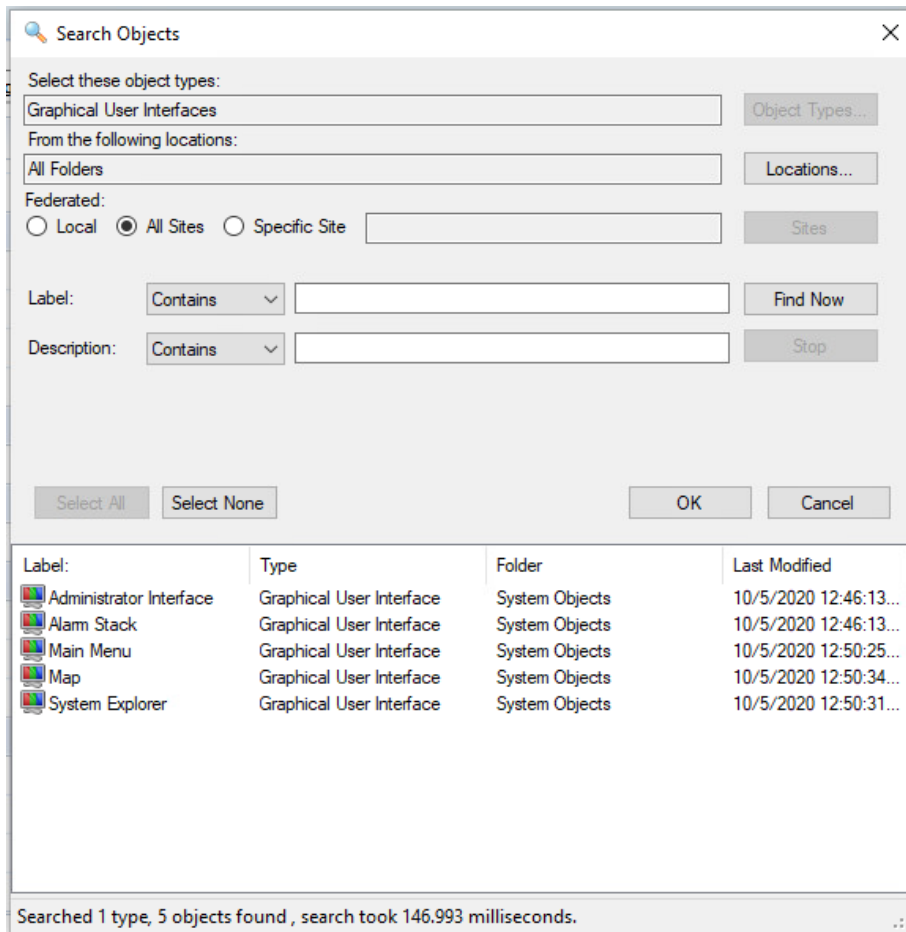
Through Publishing, Control Center can create a centrally defined System Explorer and Main Menu that is controlled at one site and synchronized with remote sites. This enables a high degree of conformity to Alarm Management throughout the organization.

After creating and saving the Main Menu or System Explorer, it is published to each remote site. The **Global Settings** dialog on the remote site can be used to select which Main Menu and System Explorer GUI to use.



Go to **System Configuration > Global Settings > Enterprise Settings**. Navigate to **UI Configuration**. From here you can choose from the available Main Menus or System Explorers.

When selecting an alternative GUI to use, the **Search** box appears. Remember to use the **All Sites** search option to find GUIs from the site that published them.

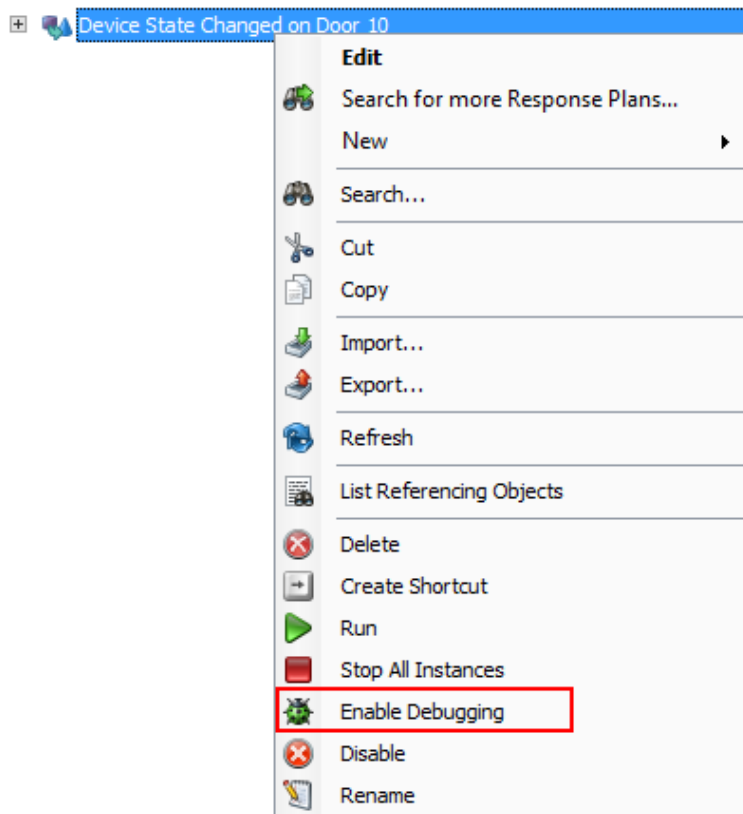


Debugging Published Content

To assist debugging commissioned logic, GUIs, and response plans that are published can be debugged at the receiving site.

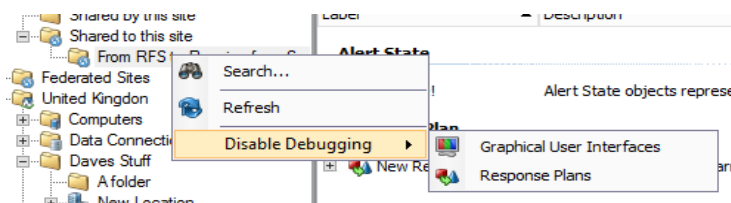
The required break points in a response plan must have been included when the content is published. On the site that receives the response plan, the user can enable or disable debugging via the context menu.

Response Plan



The client that will show the debug information for a response plan will be the client on which the **Enable Debugging** option is set on the response plan.

The user can disable debugging at a folder level by using the folder context menu. This gives the user the ability to disable debugging on GUIs or response plans separately. The application will provide a pop-up notification confirming how many response plans or GUIs were modified.



Publishing and Federating Custom Properties

A commissioning user can create Custom Properties to store additional information for specific object types.

No changes have been made to which objects support Custom Properties or to the types of Custom Properties that may be created.

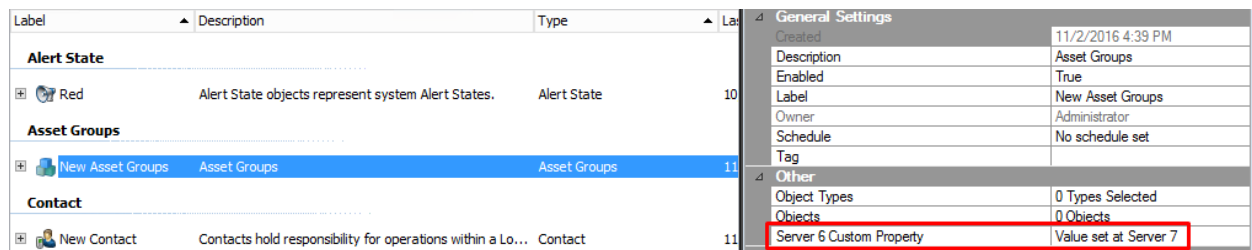
When using Custom Properties in a federated environment additional considerations apply.

The following examples refer to NOC to indicate an instance of Control Center that acts as a receiver of Alarm Data from one or more Sites. It works with the assumption that the NOC owns the Published content which is Published to the Sites.

Any Custom Properties that have been defined at a site will be included when that site publishes content to remote sites. All Custom Property definitions are published even if they are defined for object types which do not get published.

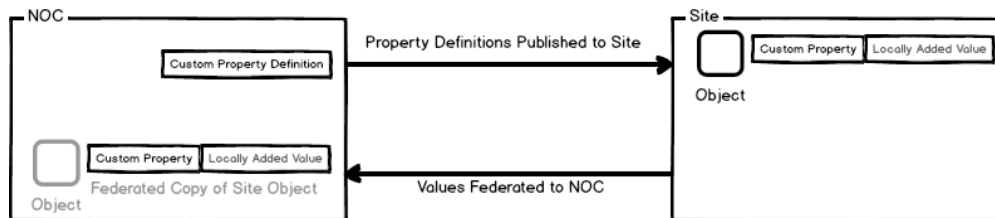
The Object Designer only shows those Custom Properties that have been defined at the local site. It is not possible to edit or change Custom Properties that have been Published to a site.

All Custom Properties available at the site are visible to the user when creating or editing a new object. These Custom Properties may have been created locally or published to the site.

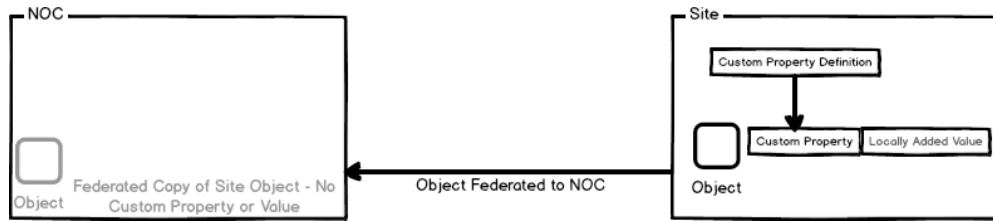


The above figure shows an Asset Group created on Server 7. The highlighted Custom Property was defined on Server 6 and Published to Server 7. After creation of the new Asset Group, the user can set the value of this Custom Property using any of the available methods.

If the Custom Property is defined against for a Federated object type, then the value of the Custom Property will also be Federated to any site configured to receive Federated data.



The above figure shows the correct configuration to receive Custom Property values at a Federated NOC site.



In the above figure, the custom property has been defined at the Site. Neither the property definition nor any locally added values are federated to the NOC.

When using Custom Properties with Federated Sites, care must be taken to ensure that unique Property Names are used across the entire enterprise. If two sites define a Custom Property on the same Object Type with the same Custom Property Name, then a Validation error will occur when the Publish is attempted.

If a published object also contains a Custom Property defined and populated on the NOC, then the Property Definition and Value set at the NOC is published to the remote site. The Custom Property Value cannot be overwritten at the local site as the data will be owned by the NOC.

Alert State

Alert State objects provide additional alerting capabilities in a federated Control Center solution.

In a Federated environment, where a Location Reference is configured, the list of parents to be alerted will continue across the Site Reference to the Federated Site. If you do not wish this behavior, then add the following key to the <appSettings> section of the configuration file for the Core Server and Alarm Types Service on the parent site, that is, the site that contains a Site Reference:

```
<add key="EnableAlertsAboveSiteRef" value="False" />
```

This will prevent Alert State propagation past Location References.

Consider the following scenario where Site 2 is federating to Site 1 and a Location Reference exists between the sites.

Site 1 - Globe

Contains its own locations and links to other instances of Control Center.

- . Location Tree for Globe
 - o Globe (Location Type - Other)
 - Europe (location Type - Region)
 - UK (Location Type - Country)
 - Headquarters (Location Type - Site)
 - Building 1 (Location Type - Building)
 - Building 2 (Location Type - Building)

- Remote Site (Site Reference to Site 2)

Site 2 - Remote Site

Includes a separate instance of Control Center that federates Alarm data to Globe.

- Location Tree for Site 2
 - Site 2 (Location Type - Site)
 - Building 3 (Location Type - Building)
 - Floor 1 (Location Type - Floor)
 - Device 1
 - Device 2

If an Alert State configured to include parents of Location Types Floor is applied to Device 1, then Floor 1 will also have the alert state applied to it.

If an Alert State configured to include parents of Location Types Floor, Building and Country is applied to Device 1 then Floor 1 and Building 3 at Site 2 will be alerted, also alerted will be UK at Site 1.

If multiple Alert States with the same priority are applied to a resource, then the most recent alert state to be applied will be shown.

Methods available for Alert States stay unchanged except for resetting an alerting object resulting in parent objects to also be reset.

Federated Status

The Federated Status functionality enables you to determine the connected state of all remote sites, additional information about the state of the connected sub-systems and perform tests to confirm end-to-end connectivity. The status of each site can be determined from the federated status dashboard displayed on the GUI.

Federated Control Center Prerequisites

Make sure you have configured the following prerequisites as a minimum:

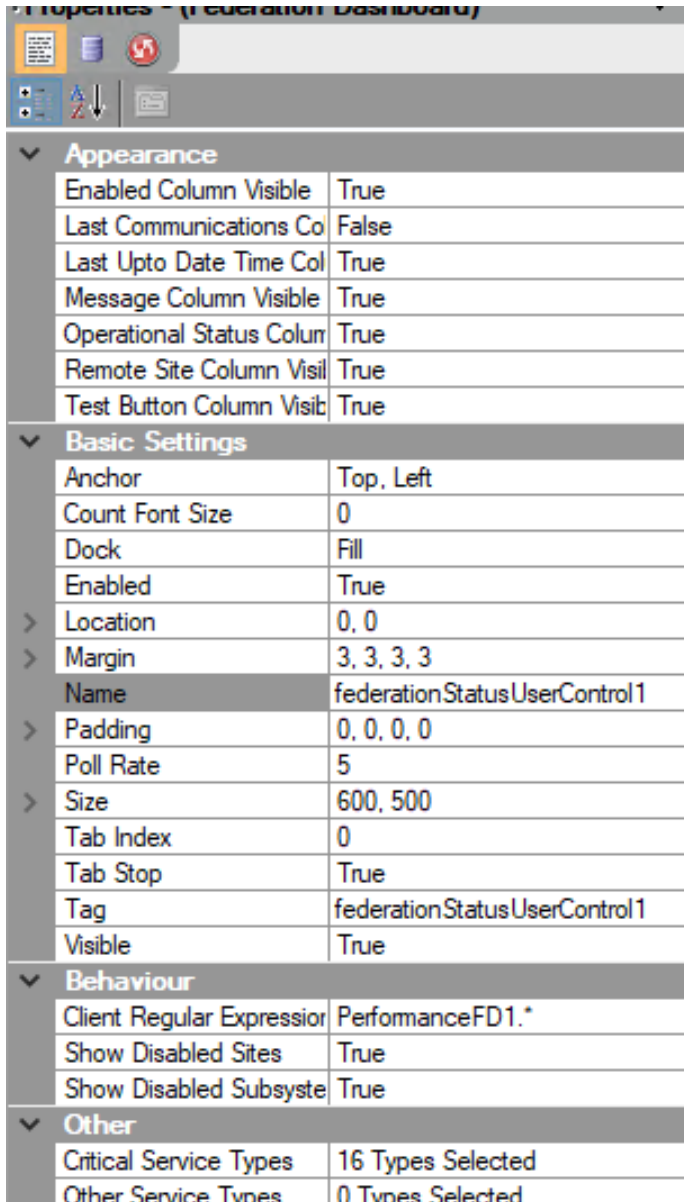
- Install the Federation Service and set up at least one federated solution.
- Configure a working Federated system, wherein you have at least two Control Center Servers and one Control Center Client for each of the servers.

Label based on the apps used. Map sources such as Google Maps and OSM will require an internet connection. If a mapping server is available on the local network, then suitable network connectivity must be in place between the mapping server and all Control Center servers/clients.

Configuring the Federated Status GUI

To configure the Federated Status GUI:

1. Right-click anywhere in the **Overview – System Objects** pane and select **New > Graphical User Interface**.
2. Rename it to **Federated Status** view.
3. Double click on the GUI object to open the GUI editor.
4. From the **Toolbox > Visual** pane, drag the **Federated Status** control and drop it to the design surface.
5. With the GUI selected, configure the following properties on the right.



Properties - (Federation Dashboard)	
Appearance	
Enabled Column Visible	True
Last Communications Co	False
Last Upto Date Time Col	True
Message Column Visible	True
Operational Status Colum	True
Remote Site Column Visib	True
Test Button Column Visib	True
Basic Settings	
Anchor	Top, Left
Count Font Size	0
Dock	Fill
Enabled	True
> Location	0, 0
> Margin	3, 3, 3, 3
Name	federationStatusUserControl1
> Padding	0, 0, 0, 0
Poll Rate	5
> Size	600, 500
Tab Index	0
Tab Stop	True
Tag	federationStatusUserControl1
Visible	True
Behaviour	
Client Regular Expressior	PerformanceFD1.*
Show Disabled Sites	True
Show Disabled Subsystem	True
Other	
Critical Service Types	16 Types Selected
Other Service Types	0 Types Selected

Appearance	
Enabled Column Visible	Show or hide the Enabled column by setting it to True or False.
Last Communications Column	Show or hide the Last Communications column by setting it to True or False. Do not use, superseded by Last Upto Date column.
Message Column Visible	Show or hide the Message column by setting it to True or False.
Operational Status Column Visible	Show or hide the Operational Status column by setting it to True or False.
Remote Site Column Visible	Show or hide the Remote Site column by setting it to True or False.
Test Button Column Visible	Show or hide the Test column by setting it to True or False.
Basic Settings	Lists the Generic Grid Properties found in the other areas of the application. Count Font size: sets the font size of the count displayed in the dashboard
Poll Rate	How often federates status is checked.
Behavior	
Show Disabled Sites Show Disabled Sub Systems	Show or hide disabled sites when you select True or False.

	Show or hide disabled subsystems when you select True or False.
Other	
Critical Service Types	Select the critical object types that should be visible and monitored when displaying a site's local objects. A critical service failure will result in the Site being shown as offline.
Other Service Types	Select the non-critical object types that should be visible and monitored when displaying a site's local objects. A non-critical service failure will result in the Site being shown to be in a warning state.

6. Save the GUI.
7. From the **System Objects** pane, right-click the GUI and select **Generate Tile Layout**.
8. Right-click the new tile layout and select **Display Tile Layout On** or drag and drop the tile layout to display on a display area.



Viewing the State of the Key Remote Services

From the Federated Status GUI, expand a site to view the state of the monitored remote services such as the Control Center Core Service, Connection Manager Service, or specific devices at the sub-system in the main window. If the services are running, you will see a green tick under the Operational Status column. A red cross represents that the services or devices are not operational and needs to be fixed. A green tick under the enabled column depicts the services or devices have been enabled.

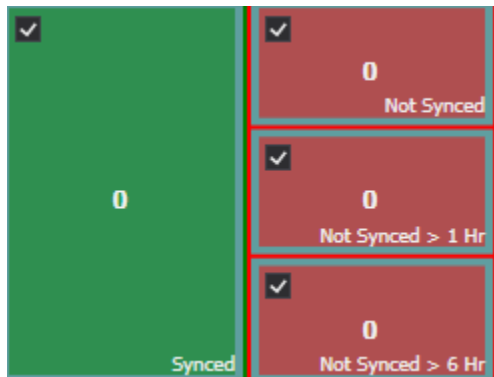
Let's consider a scenario to understand the GUI displayed above.

If the administrator at the NOC wants to view the status of all sites connected to it, the administrator can easily get an insight by the status boxes on the right side of the screen. The green boxes to the left display the sites that are functional and the red boxes on the right displays various stages the sites are in before it eventually becomes functional.

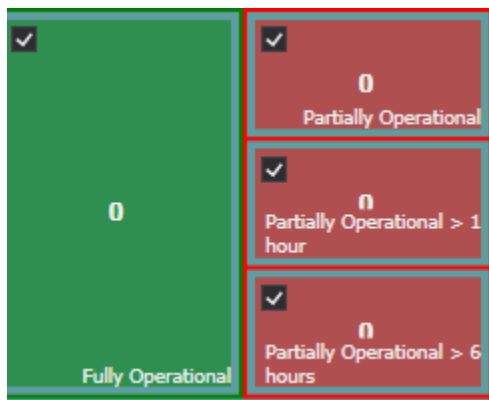
The first set of boxes represent the number of sites that are connected or not connected to the central hub. It is logical to assume that the sum of these two numbers is a typical representation of the total number of sites connected to NOC.



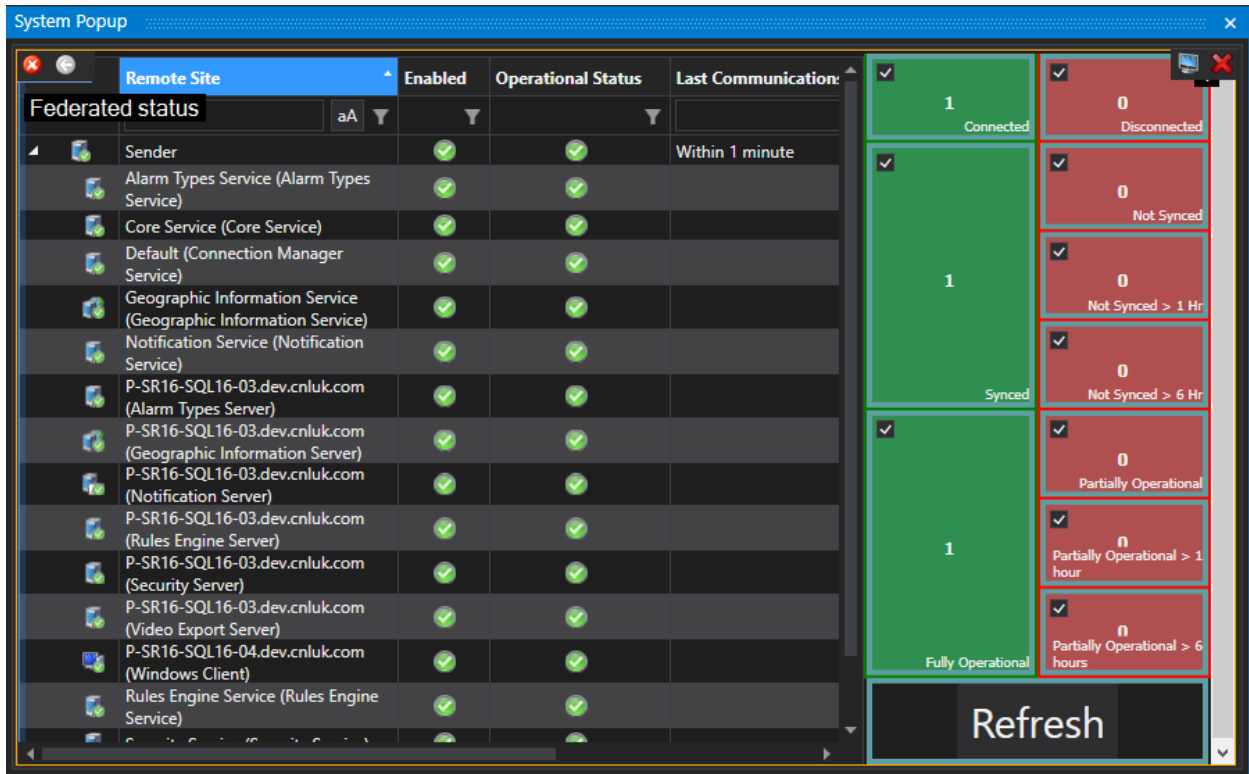
The next set of boxes represent the sites that are synced or not synced to the NOC. In circumstances where the site has lost connectivity to the parent site, it would be in the Not synced box. Once the connectivity is established and the sync is complete, it will be added to the Synced count. The boxes in the right also gives us the indication of the duration for which the site is out of sync with the NOC



The last set of boxes represent the represent the sites that are fully operational or partially operational depending on the operational status of all the services and devices at the site.



A fully connected, synced and operational site is as shown in the figure below. The administrator can click on the refresh button to see the latest status of all sites.

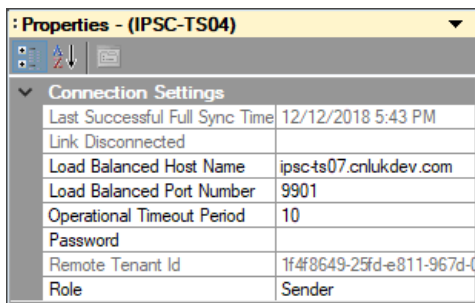


By default, all sites connected will be listed. The user can also look for a site by entering the name in the search bar at the top of each column. On pressing enter, the site along with its status will be displayed.

A site where the remote Federation Service has failed but is not a monitored type, will show all services as offline and the reason stated as 'connection lost'. For a more accurate status message, add the RFS service type to the list of monitored types. If the RFS fails, the reason will now state, correctly, that the RFS has failed.

There is an additional property that can be set, to fire an alarm if a site is non-operational for more than the set time. To do that,

1. Click on the **Federated Sites** option in the **System Configuration** window.
2. Select a site from the list connected in the federation network, to display the properties window on the right.



3. Enter the **Operational Timeout Period** in minutes after which the event needs to be triggered.

10 min is the time for a site to connect back to the NOC after going offline. If this time limit exceeds and the site is still non-operational, then an event is triggered to fire an alarm.

Remote Federated Service				
IPSC-TS07	Remote Federated Service	Remote Federated Service	12/11/2018 2:03:08 PM	Synchronization complete
Events				
Operational Timeout Exceeded	The time since this site was successfully connected a...			
Remote Federated Event	Event from remote site			
Service State Changed	Raised when the online state of the service changes			
Test Remote Site	Event fired when 'Test Site' is pressed on Remote Fe...			
Threat Level Changed	The Threat Level of the system has changed.			
Shortcuts	Shortcuts targeted against this object			

Fully Updated

At a quick glance, sites that have issues might appear to be working as they are in a synchronizing state or temporarily online. The Fully Updated column aims to help users get an appreciation for if there are underlying issues at a site.

Sites continuously update the federated hub with updates. If there is an underlying issue, this could be detected by looking at how long it has been since a hub was fully up-to-date with a site. The *Fully Updated* column shows this.

The value is updated regularly based on the polling value of the federation dashboard GUI control.

To display the new column, edit the federation dashboard GUI and set the property *Last Updated Time Column Visible* to True.

When the RFS state is online and synchronized and changes to any other state, the Last Up-to-Date Time property on the RFS object is updated.

When the RFS state goes offline , the Last Up-to-Date Time is updated.

At any time, the hub and site are synchronized and online, the Fully Updated column should display "Within 1 minute".

If the site is not online and synchronized, the Fully Updated column displays the last time it was, based on the property of the RFS object.

	Enabled	Operational Status	Fully Updated
.cnluk.com Site10	✓	✓	Within 1 minute
.cnluk.com Site11	✓	✓	Within 1 minute
.cnluk.com Site12	✓	✓	Within 1 minute
.cnluk.com Site13	✓	✓	Within 1 minute
.cnluk.com Site14	✓	✓	Within 1 minute
.cnluk.com Site15	✓	✓	Within 1 minute
.cnluk.com Site16	✓	✓	Within 1 minute
.cnluk.com Site17	✓	✓	Within 1 minute
.cnluk.com Site18	✓	✓	Within 1 minute
.cnluk.com Site19	✓	✓	Within 1 minute

Location Dots Indicate Online State Change

The Location dot will show as grey if the Location is offline due to a communication issue between the sites. The following figure shows the Wroughton Office and Newbury Office online, where blue dots on the left indicates that the Federation Service is enabled and grey dots on the right after the Federating Service is disabled.



Import / Export

You can export Control Center objects and import them into another solution.

The Import / Export feature supports all Control Center object types except the following:

- Clients
- Servers
- Services

It is still possible to export objects that reference the above objects. During the import of these objects you can select the local object to be used in place of servers, devices and so on.

Some objects in Control Center are system objects, meaning they are created when the system is installed and cannot be deleted. When exporting and importing, the following rules apply to system objects.

- A system object can only upgrade or overwrite a system object on import.
- A system object can only be imported if it is of type GUI, Extension or Alarm Type
- A system object can only upgrade or overwrite a non-system object on import.

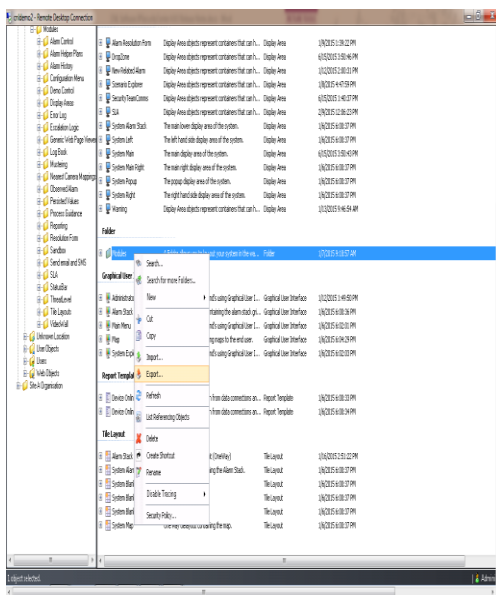
Exporting Control Center Objects

When exporting alarm types, only local alarm types are exported into the file. For example, the highlighted alarm type would not be exported.

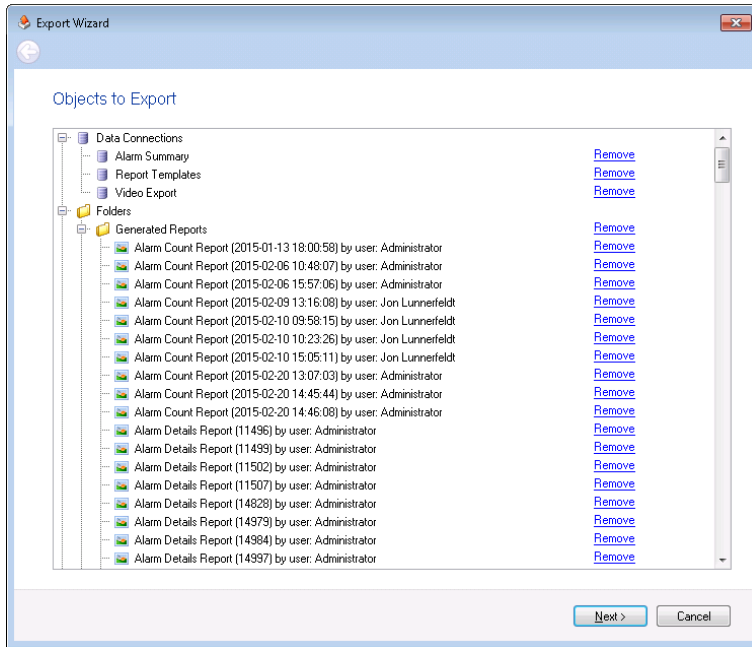
Overview - System Objects						
Alarm Types						
Alarm Types						
Alarm Stack Views						
Alarm Types						
	Label	Enabled	Description	Site Name	Manual	
1	Device Alarm	True		Local	True	
1	Door Alarm	True		Server 007	True	
2	Real Alarm	True		Local	False	
1	Correlated Alarm Types	True		Local	False	

You can export several objects from Control Center. To export objects:

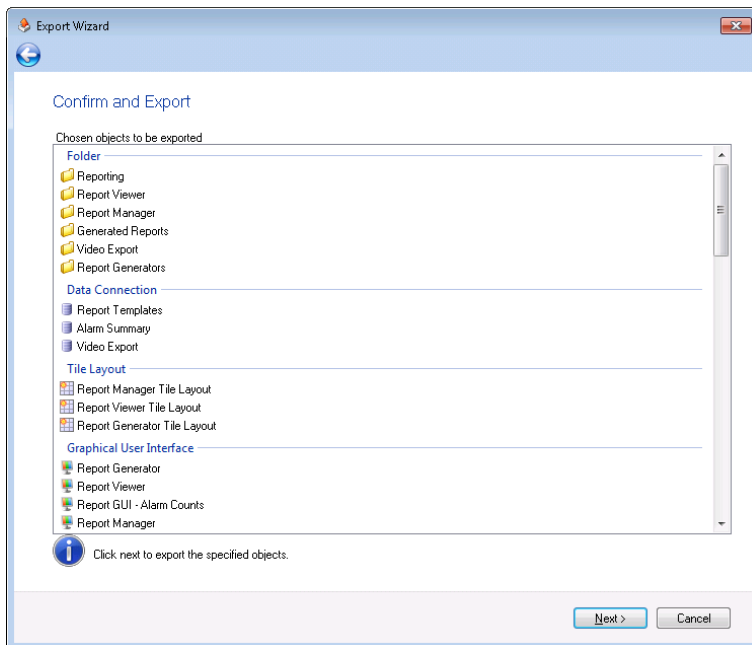
1. Open **System Explorer** and select one or many objects or folders that need exporting.
2. Right-click anywhere and select **Export**.



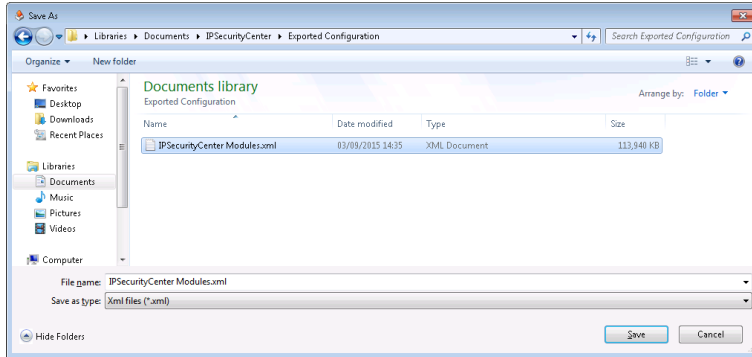
3. The **Export Wizard** is shown. The wizard will review all referenced objects based on the selected objects and include these in the export if required.
4. If an object is not included, click **Remove** link next to the object.
5. Click **Next** to continue.



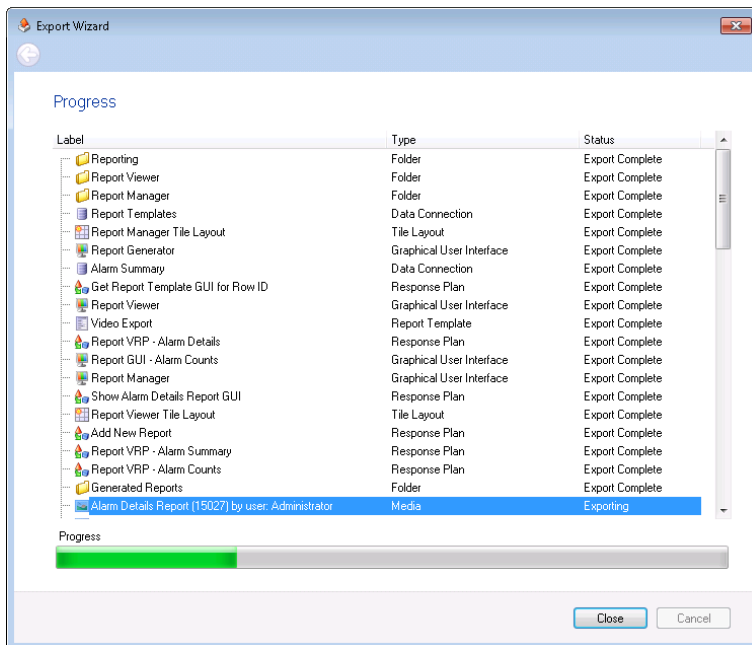
6. A summary screen is shown. Review the objects to be exported and click **Next** to continue.



7. The **Export** wizard will save the export to a file. Select a location and a file name for the file to be exported.



8. The export is started. Progress is shown during the export. Once the export is complete, click **Close** to close the dialog.



Importing to Control Center

You can import objects from, for example, a development Control Center environment to a production Control Center environment.

When importing objects to an Control Center environment, you can either:

- Add the imported objects as new objects in your Control Center environment
- Overwrite your existing objects with the imported objects.

You can also import alarm type objects to an Control Center environment.

When you install Control Center, Control Center creates a default system alarm type object. The default system alarm type object is in **\MyOrganization\System Objects** folder. In a non-federated Control Center environment, you can only have one system

alarm type object. Importing an alarm type object in a non-federated Control Center environment updates the existing system alarm type object.

The default system alarm type object is composed of a combination of individual alarm types, including Alarm Types, Manual Alarm Types, Correlated Alarm Types and Alarm Type Modifiers. There are also other objects within the System alarm type object, such as Alarm Stack Views, Alarm Handling Groups, Alarm Activity Types and Resolution Types.

When importing a system alarm type object to an Control Center environment, for each individual alarm type object, you can:

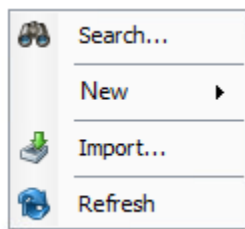
- Add the imported alarm type objects as new alarm type objects
- Overwrite existing alarm type objects with imported alarm type objects
- Merge existing alarm type objects with imported alarm type objects

While importing, individual alarm type objects are evaluated based on the unique identifier (GUID) associated to the Alarm Type in the database.

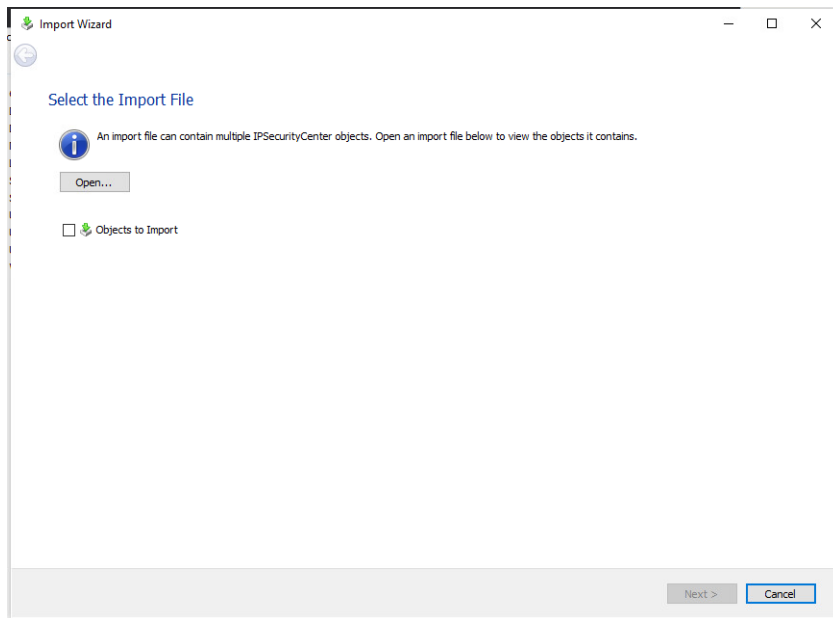
Importing Control Center Objects

To import the exported file into Control Center, follow these steps:

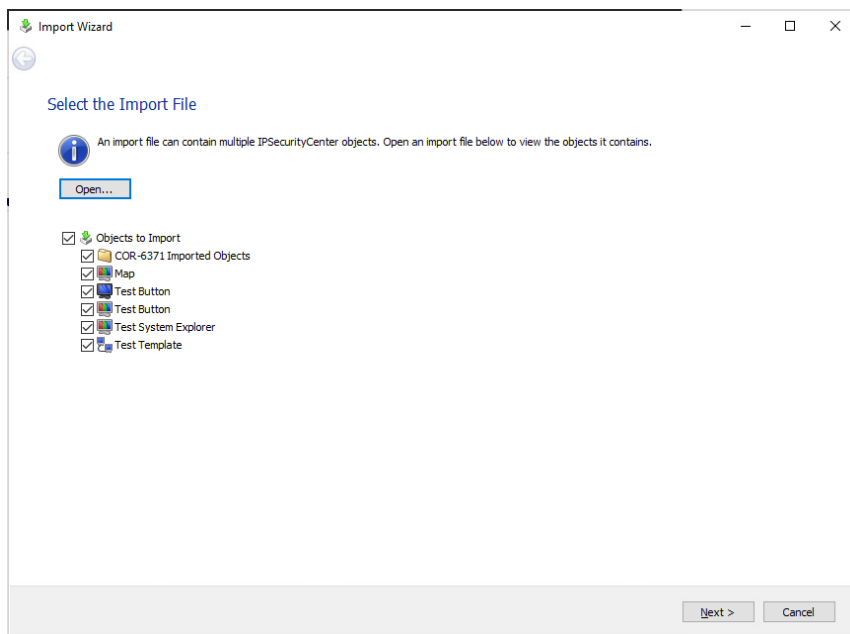
1. Open **System Explorer** and right-click and select **Import...**




2. The **Import Wizard** appears. Click **Open...** to select the file to import from.



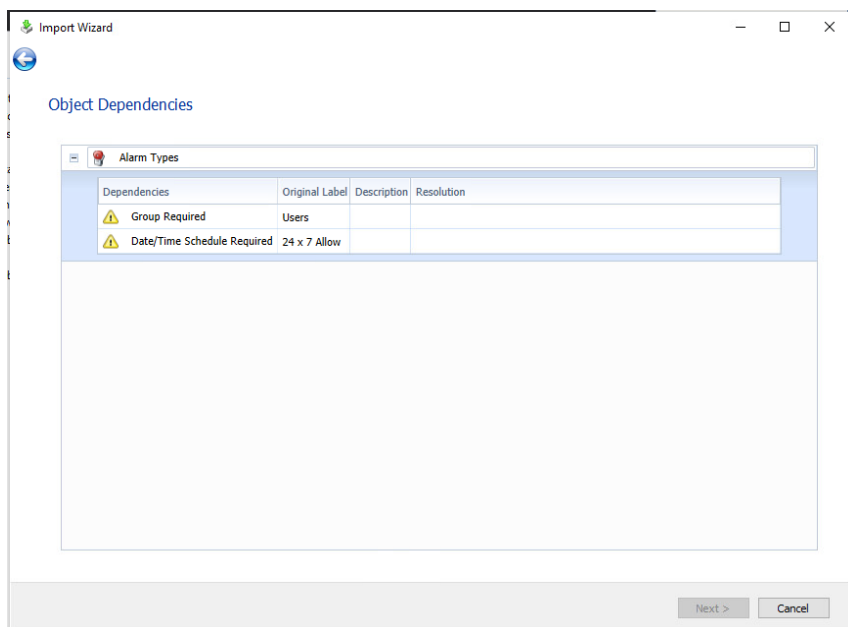
3. The **Import Wizard** shows all objects found in the file. Validate that these are the expected objects.



If a  is shown next to any of the objects, this object cannot be imported. The reason why the object cannot be imported is also given, for example, connector not loaded. Depending on your requirements, you can resolve the issue and perform the import again.

Click **Next**.



- The next step in the wizard shows object dependencies. An exported object can reference another object that has not been exported. If there are no dependencies, a **No dependencies to resolve** message is displayed.



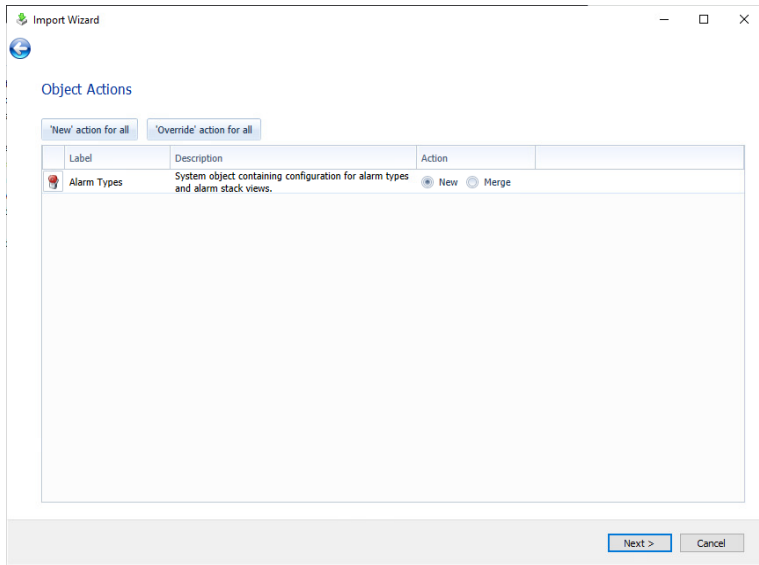
- You can update an object reference to use an existing object. If this is required, right-click on the missing object and select **Search**.

Dependencies	Original Label	Description	Resolution
⚠ Group Required	Users		
⚠ Date/Tir  Search	24 x 7 Allow		

- Use the standard Control Center **Search** dialog to find and select the new object to be used. The **Import Wizard** is updated to show that a replacement object has been selected.

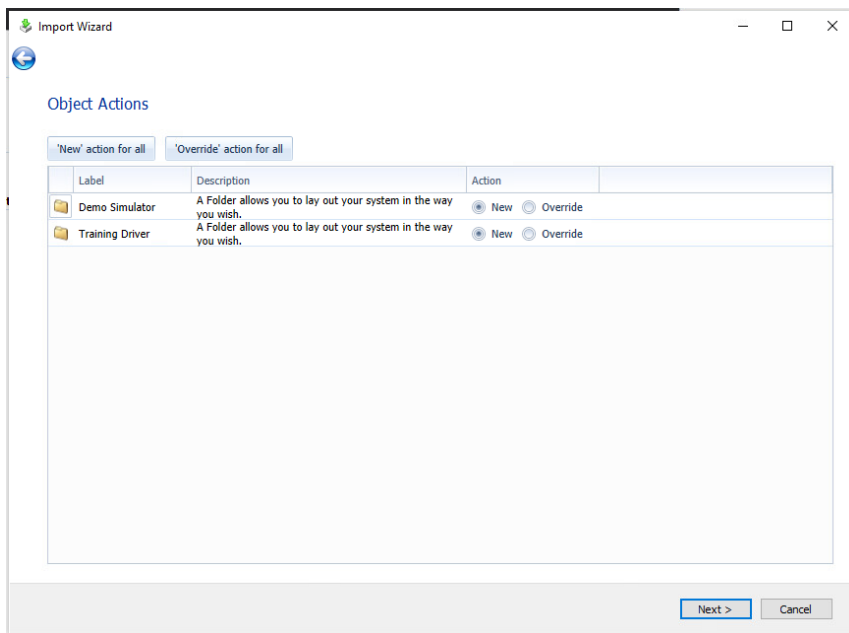
Dependencies	Original Label	Description	Resolution
✔ Group Specified	Users		 Users
✔ Date/Time Schedule Specified	24 x 7 Allow		 24 x 7 Allow

- Select **Next** to move to the next step. If the file to be imported contains objects that already exist in Control Center these are listed on the next screen. If you are importing alarm types, the following screen displays:




If you see this screen, go to [step 9](#).

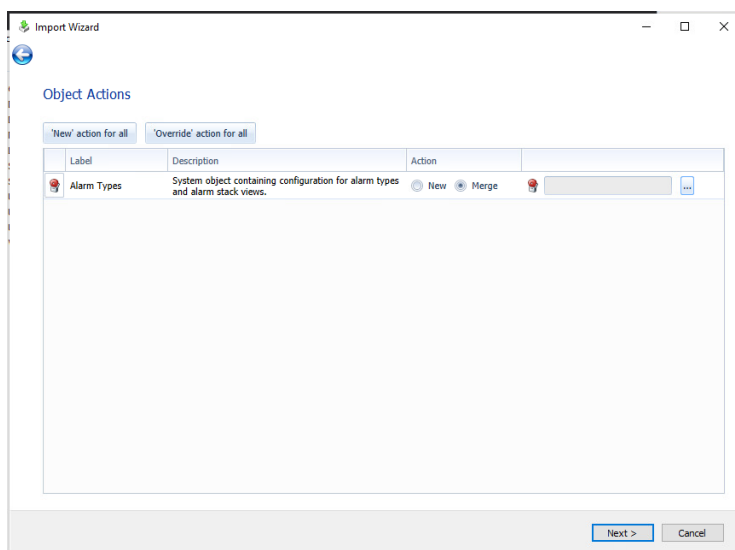
If you are importing any other Control Center objects, the following screen is displayed:



If you see this screen, go to the next step.

8. **If you are importing Control Center objects** (other than alarm type objects) you can, either:
 - import all the objects as new objects. To do this, select **New action for all**.
 - override all the existing objects with the imported objects. To do this, **Override action for all**. By selecting this option, you are effectively merging your existing objects with your imported objects.

- for each object, decide whether to import the objects as a new object or merge the object with an existing object. To do this, for each individual object that already exists, select:
 - **New**, if you want the imported object to be imported as a new object. Go to [step 10](#).
 - **Override**, if you want the imported object to be merged with the existing object.
- a. If you select, **Override** for each individual object or **Override action for all**, for each object, select  to display the Control Center **Search** dialog to select an existing object to merge with the imported object.

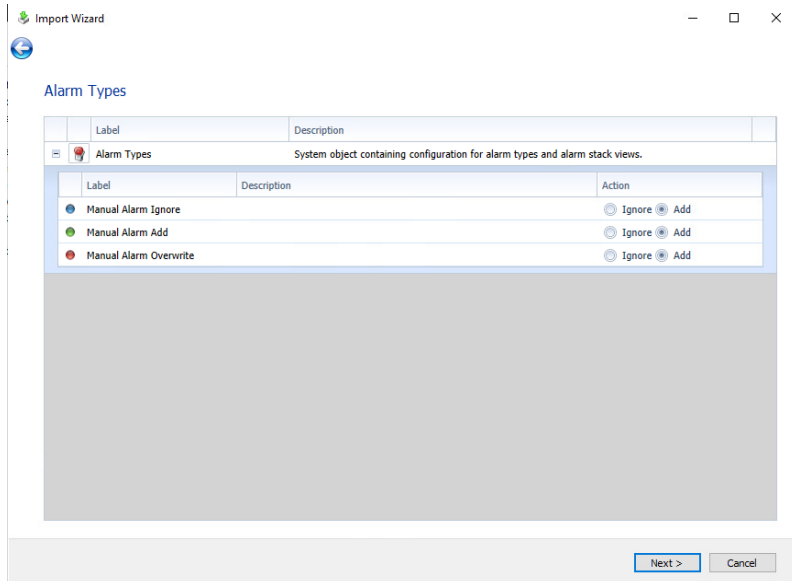



- b. Once you have completed this for each individual object, select **Next**. Go to [step 10](#).

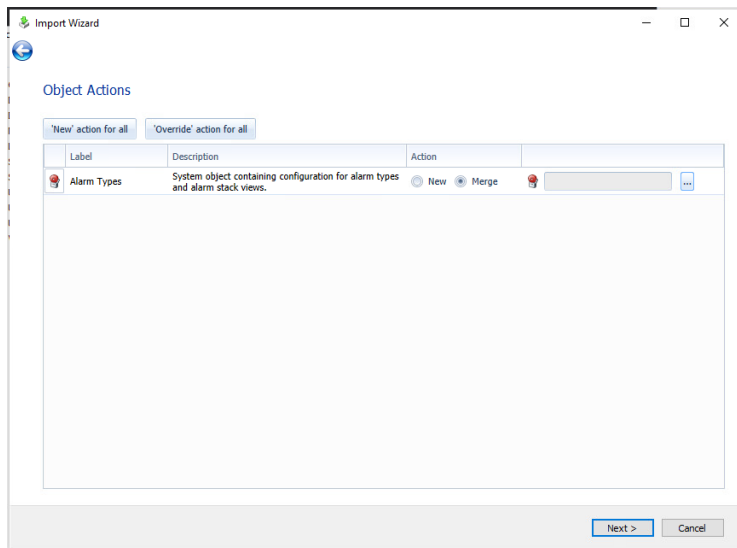
9. If you are importing alarm type objects, you can, either:

- import all the alarm type objects as new objects. To do this, select **New action for all**.
- override all the existing alarm type objects with the imported alarm type objects. To do this, select **Override action for all**. By selecting this option, you are effectively merging your existing alarm type objects with your imported alarm type objects.
- for each alarm type object, decide whether to import the objects as a new object or merge the object with an existing object. To do this, for each individual object that already exists, select:

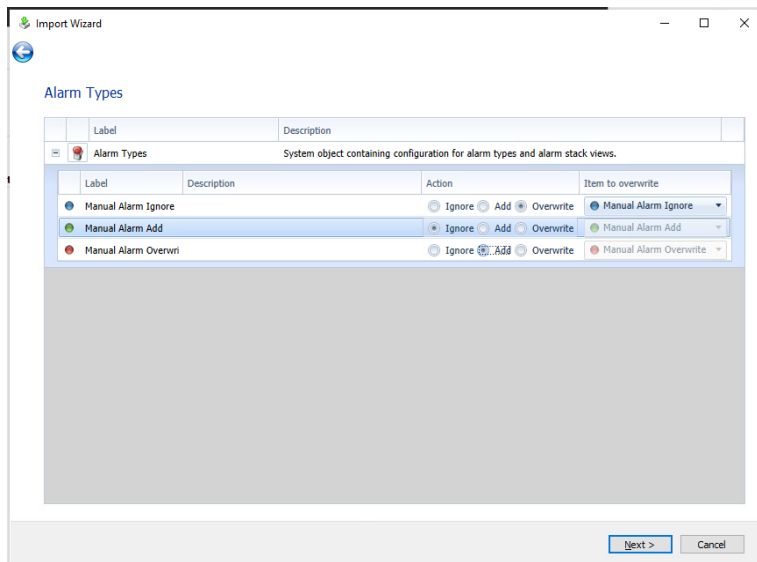
- **New**, if you want the imported object to be imported as a new object.
 - a. For each of the individual alarm type object, you can choose whether to:



- **Ignore**. Select this if you want to ignore the imported object. In other words, the existing object remains the same.
 - **Add**. Select this if you want to add the imported object as a new object.
- b. Once you have completed this for each individual object, select **Next**. Go to [step 10](#).
- **Merge**, if you want the imported object to be merged with the existing object.
 - a. If you selected, **Merge** for each individual object or **Override** **action for all**, for each object, select  to display the Control Center **Search** dialog to select an existing object to merge with the imported object.



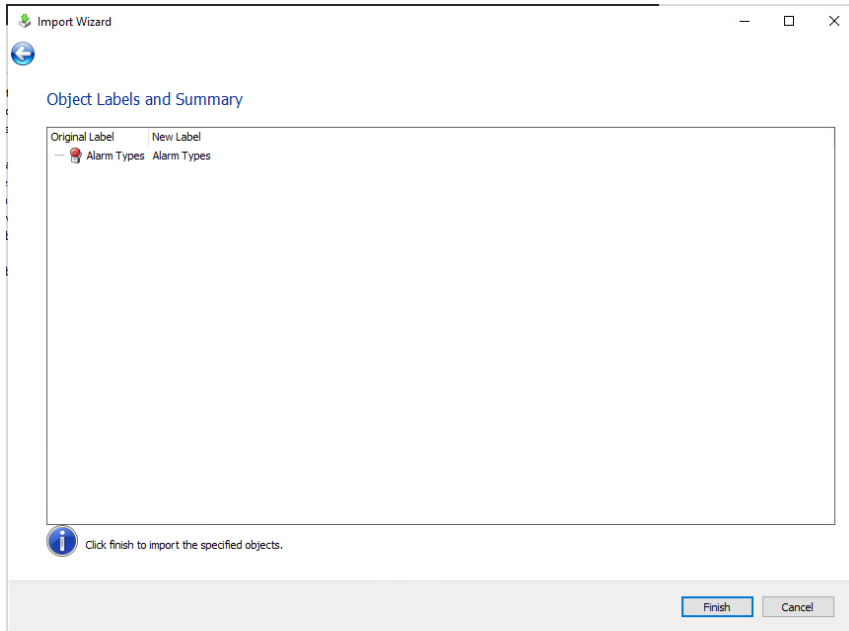
- b. For each of the individual alarm type objects, you can choose whether to:



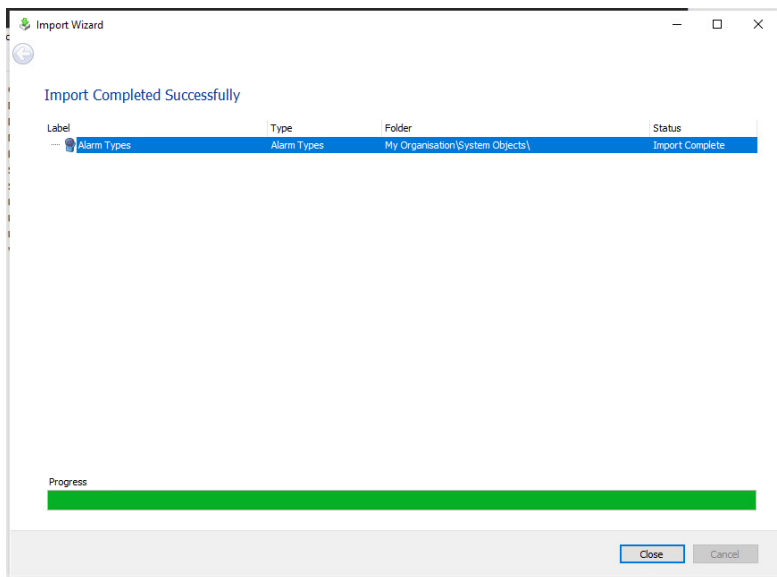
- **Ignore.** Select this if you want to ignore the imported object. In other words, the existing object remains the same.
- **Add.** Select this if you want to add the imported object as a new object.
- **Overwrite.** If you select **Overwrite**, from the **Item to overwrite** drop-down list, select the item you want to overwrite with the imported alarm type object.

- c. Once you have completed this for each individual object, select **Next**.

10. From the summary screen, validate and click **Finish** to start the import process.



11. Click **Close** once the import has completed to close the dialog.



Disaster Recovery

Control Center has been designed to facilitate a DR (Disaster Recovery) process in the case of complete systems failure. The design provides for an awareness of the environment in which Control Center is operating. The environments supported include:

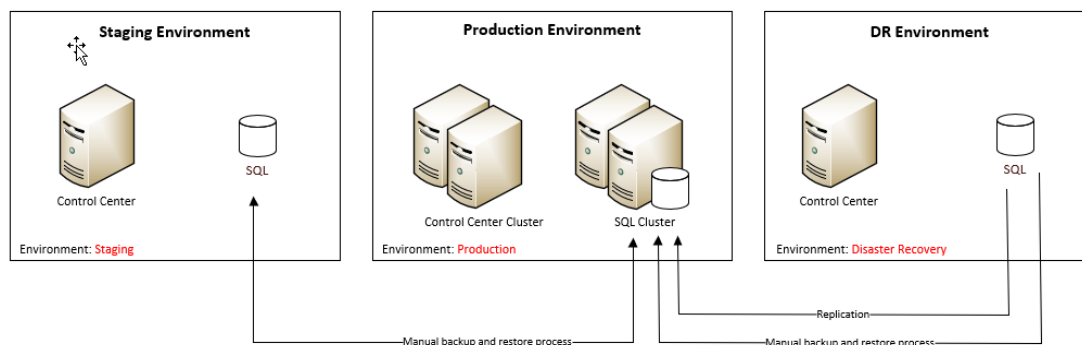
- Production
- Staging
- Disaster Recovery

Certain objects in the system will be assigned an environment. This awareness of different environments will then allow Control Center to initialize and re-home assets accordingly when starting up.

Configuring the Environment

The diagram below shows an example where replication has been setup between a SQL cluster in a production environment and a single instance on SQL in a DR environment. The databases in the DR environment will continually replicate those in the production environment. Should the production environment suffer an irrecoverable failure then the DR environment can be manually initialized to resume operations with no loss of data. Following the failure of the production environment, SQL replication would be terminated and therefore manual intervention is required to re-establish the production environment, restore the databases and then setup replication.

The combination of clustering and single servers shown in the following diagram is used as an example only. Control Center imposes no restrictions on the combination of single servers, dual servers with failover, or clusters between environments.



To enable automatic recovery of the solution, every object will be assigned an environment as indicated in the diagram above. While this is available on all objects, it is primarily related to servers, clients, devices, and placeholders. The following things happen:

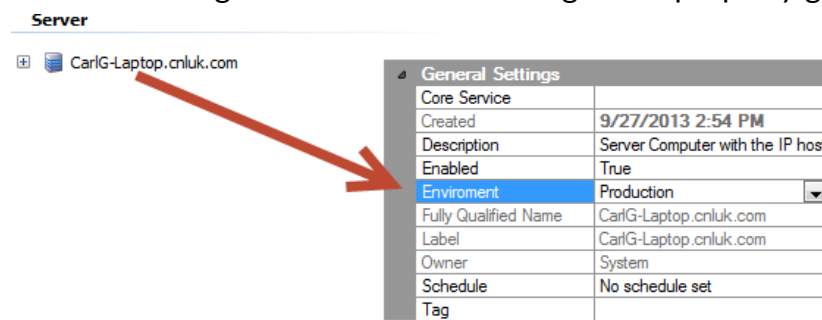
Assets in either the staging or production environments will only initialize and be available in the corresponding environment.

The disaster recovery environment will automatically take ownership of all assets marked as production, which means re-homing devices onto the DR connection managers.

Control Center Configuration

To configure a Control Center solution to support disaster recovery, you must:

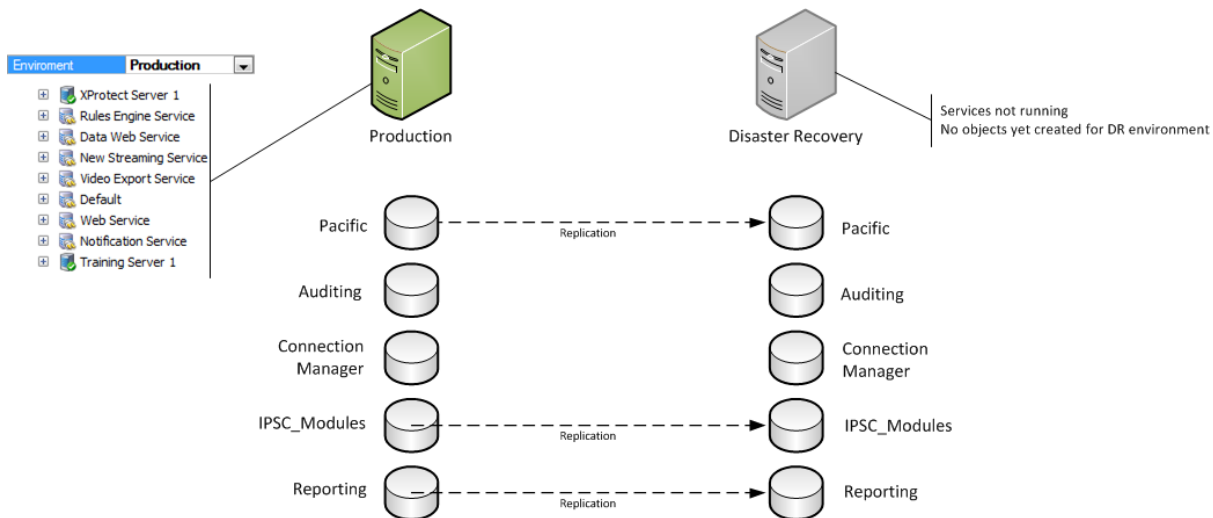
1. Install Control Center and configure the solution in the production environment. As each object is added into the solution, the environment setting for certain objects such as servers and services will default to Production. Existing objects created prior to the release and installation of Control Center 4.7.7 will also default to production. This setting can be checked by selecting the object and checking the Environment setting in the property grid.



2. Install Control Center in the staging environment but do not start the services
3. Setup replication to publish from the production pacific database to the DR database
 - o Replication is not required for any other Control Center databases.
 - o Supplementary databases such as IPSC_Modules will need to be replicated.

The license used must include sufficient server allocation to allow for the DR server to be created without any licensing implications

The solution should now be configured so that the production environment contains all required objects for the solution, with the environment set to Production, and the pacific database, together with any supplemental databases, are replicated to the DR SQL instance; this is illustrated below.



The Auditing and Connection Manager databases should not be replicated.

Disaster Recovery Process

When the production system suffers a complete loss, and cannot be recovered, then the Control Center solution can be failed over to a disaster recovery solution.

The process to failover to DR is minimal but does require user intervention. This process should only be carried out in extreme circumstances as the process to restore back to the production environment is more intensive.

Assuming the solution has been configured as per the previous section, if production environment fails, the disaster recovery process is as follows:

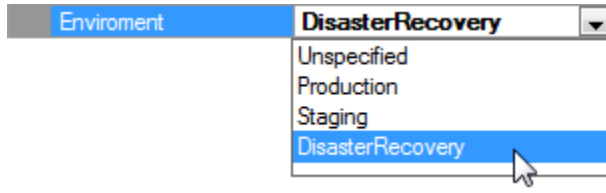
1. Ensure that all measures to recover the production environment have been exhausted, otherwise ensure that all Control Center services in the production environment are not running.
2. Disable replication.
3. Disconnect the replication link between the environments to isolate the DR environment.
4. Start all DR services.
5. Start the Control Center Server service with the start parameter **Environment:DisasterRecovery**. This will create the necessary server and service objects whilst setting the environment to **DisasterRecovery**. The server will then automatically rehome all devices from the production connection manager service(s) over to the disaster recovery connection manager service(s).
6. Log every client into the DR server. This will update the list of known servers so that users can easily log in without manually specifying the DR server address.

For more information on creating a response plan to automate this process, see [Automated Client Log In/Out Process](#).

Manual Failover

If you started the Control Center Server service in a Disaster Recovery environment without the **Environment:DisasterRecovery** start parameter, then you must perform the process manually.

First, set the **Environment** property on all objects corresponding to the DR environment to **DisasterRecovery**. This will include all corresponding servers, services and clients.



In addition, ensure to manually rehome all devices from System Configuration in Control Center.

To rehome devices from one Connection Manager to another, simply right-click a device (typically the parent server), select **Rehome Device** from the context menu and then specify the new connection manager.

This will update all connected devices, therefore rehomeing the parent server will also rehome all child devices.

Automated Client Log In/Out Process

When switching to a Disaster Recovery server, the connected clients would have never connected to the server previously. This means that when wanting to log in, each user would have to manually enter the server details to connect. The following response plan show an example where a response plan can be used to automatically log each client in and out of the DR server. This will then update the list of known servers on each client so that the user can simply log in without specifying a server address.

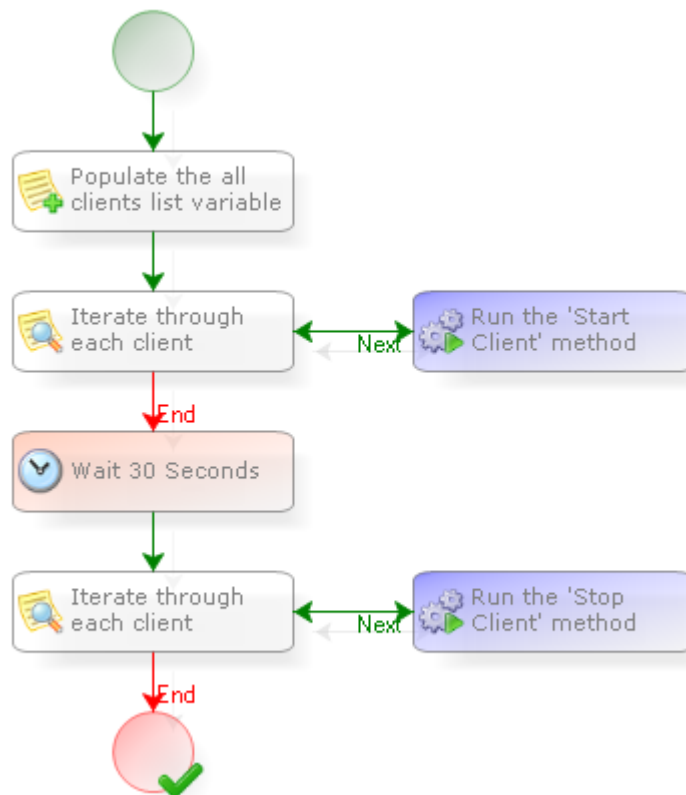
This requires an account which allows multiple log ins. Security should also be considered as users may be able to operate the workstation during this process using the designated account therefore permissions should be restricted.

The following steps describe creating a response plan which can be used to automatically log in and out all clients. This can then be used from main menu for example.

1. Create a response plan with the following variables:

Page - Hidden	
AllClients List Of 'Windows Client'	Hidden
CurrentClient Windows Client	Hidden
Page - Required	
Password Text	Required
ServerAddress Text	Required
UserName Text	Required

2. Add the following:
 - o Add to List
 - o Iterate Collection
 - o Dynamic Action
 - o Wait Iterate Collection



- o Dynamic Action

- Configure the **Add to List** shape to populate the client list variable with all clients using the **Computers** (or otherwise) folder.

Optional	
Include Child Folders	True
Required	
Folders to search	1 Object
List Variable	AllClients
Objects to Add	0 Objects

- Configure both **Iterate Collection** shapes to iterate through the client list variable.

Optional	
Reference	
Required	
Current Value	CurrentClient
List Variable	AllClients

- Configure the first **Dynamic Action** shape to call the Start Client method on the CurrentClient variable.

Start Client

Run the Start Client function

Starts the Control Room Client on this PC

Specify required information to run the function

To run the requested function the following information is required. Please fill in the properties below and click OK to continue.

Start Client	
Hide Server Details	False
Name of User	Username
Password	Password
Server	ServerAddress
Server Port	9001

Hide Server Details
Hides the advanced section on the client login dialog.

OK Cancel

6. Configure the **Wait** shape to pause the response plan for a suitable duration to allow the clients to fully log in before logging them out.
7. Configure the second **Dynamic Action** shape to call the **Stop Client** method on the **CurrentClient** variable.

Failover Clustering

Windows Server Failover Clustering is a feature of the Windows Server platform that helps improve system availability. Wherein, if one server fails, another server begins to provide service in its place.

Microsoft defines a failover cluster as follows:

A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover). Users experience a minimum of disruptions in service.

(Microsoft.com, 2011)

For comprehensive documentation on Failover Clustering, please refer to the Microsoft website:

[http://technet.microsoft.com/en-us/library/cc732488\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc732488(W.S.10).aspx)

Control Center supports the Windows Failover Clustering (WSFC) features so that a second instance of Control Center can be started with no user intervention, if a server or Control Center fails.

While Control Center is restarting, a message is displayed informing the users that the Control Center Client is attempting to reconnect.

During this time, the user can continue to view the video devices.

Once the connection is re-established, the client resumes normal operation.

Microsoft Windows Failover Clustering can be used to improve the availability of Control Center. Failover clustering provides automated recovery in the event of the following incidents:

- Hardware failure
- Operating system failure
- Control Center Server termination

Configuring Failover Clustering

The following is required:

- A Microsoft SQL Cluster should be available for Control Center deployed in accordance with Microsoft SQL best practices. Control Center requires a permanently available database connection, that is, if SQL Server is not available, Control Center will not be available.
- All machines should be members of a domain.

- Shared storage for clustering. Shared storage will be available and preferably an always available SAN.
- MSMQ to be setup as a high availability resource group.

Control Center Services

The following Control Center services need to be deployed in the MSMQ Resource Group:

- AlarmTypes
- Audit
- Federated
- GIS
- Notification
- Report Server
- Rules Engine
- Security
- Server

The following Control Center services are not deployed in a cluster:

- Video Export
- Monitoring Service
- Connection Manager

The Connection Manager provides a native failover. See [Connection Manager Failover](#) for more information.

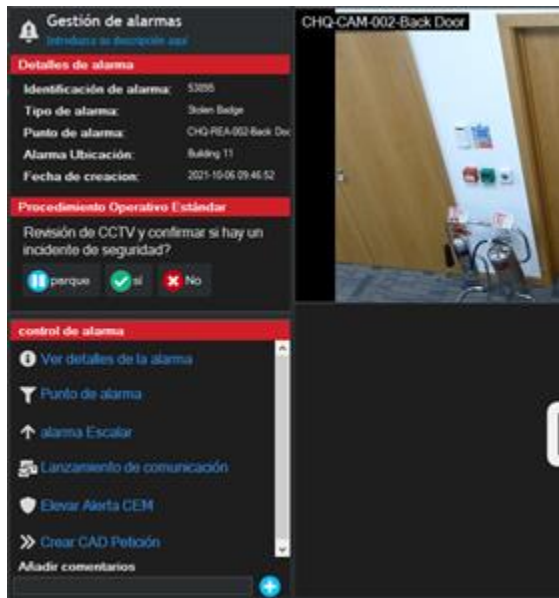
When Control Center Services are deployed in a clustered environment, the Load Balanced Host Name will be the address of the cluster, not the node.

Internationalization

Control Center supports using multiple languages in graphical user interfaces such as Process Guidance. Translations apply to the content, but not to standard product language strings, such as system menu items, tooltips, and the login screen.

In addition, the login screen and system menus also support Arabic language. However, the screen alignment is left-to-right.

Various tools and processes are included with Control Center to facilitate the import and export of text.



Internationalization Prerequisites

Ensure that the following prerequisites are met in SQL Server Management Studio before extracting language references from the solution for translation:

- Enable the Include column headers when copying or saving the results option. This option is located under **Tools > Options > Query Results > SQL Server > Results to Grid**.
- Enable the Quote strings containing list separators when saving .csv results option in Microsoft SQL Server Management Studio. This option is located under **Tools > Options > Query Results > SQL Server > Results to Grid**.

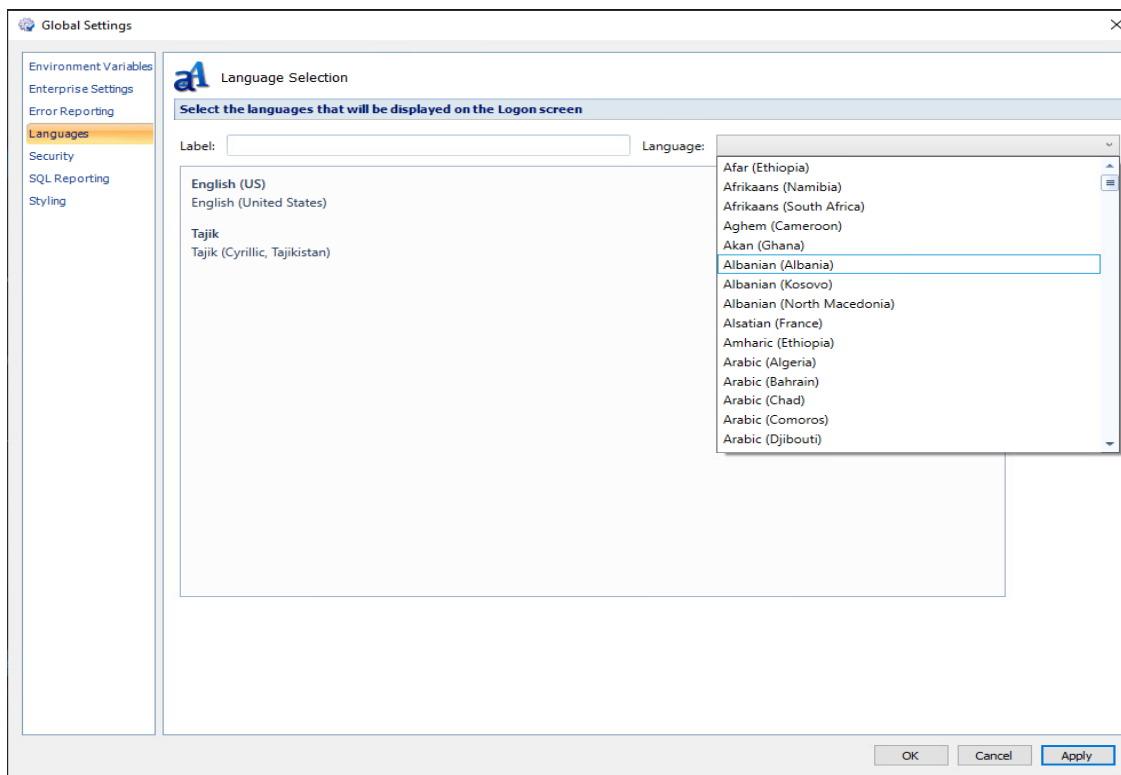
Configuring Internationalization

Control Center is installed with English (US) as the default language. Additional languages can be introduced into a solution which will then show up throughout the system in the user interface.

Only English (US) and Arabic (Saudi Arabia) are currently supported in Control Center.

To specify additional languages into a solution, create a new entry in the **Languages** tab of **Global Settings** by following these steps:

1. From the **System Configuration** dialog, click the **Global Settings** toolbar button.
2. From the menu on the left of the dialog, select **Languages**.
3. Enter a label for the new language entry into the textbox labeled **Label**.
4. Specify a language from the **Language** drop-down list, for example, Arabic (Saudi Arabia).
5. Click **Add** and then click **OK**.



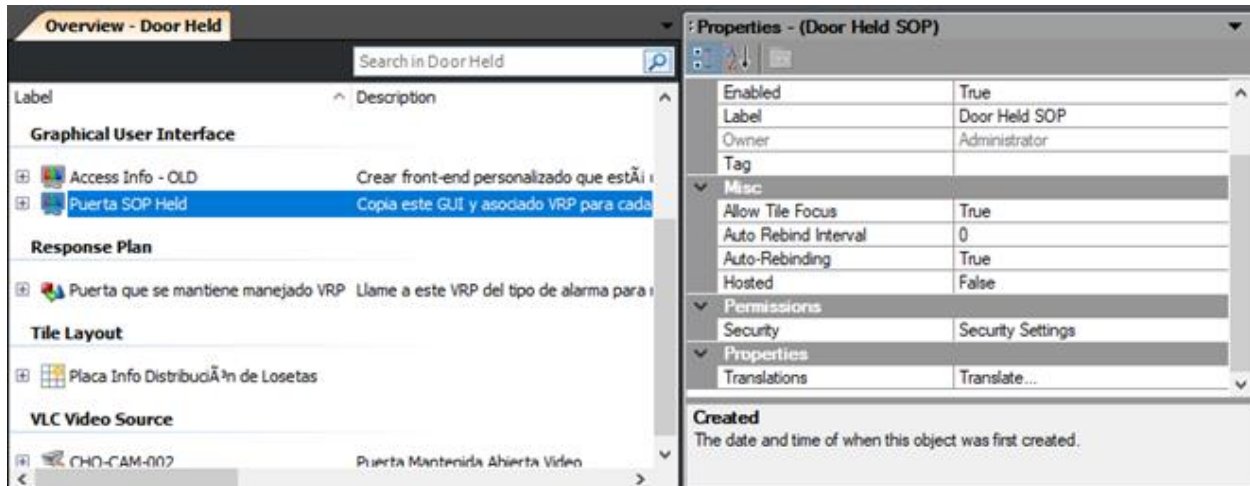
Additional languages are then shown as available language options on the login dialog. The user can select their preferred language and then login to see the user interface in their selected language.

All dynamic text must be translated prior to the solution being used, for example, dynamic solution data; GUI labels or menu button labels.

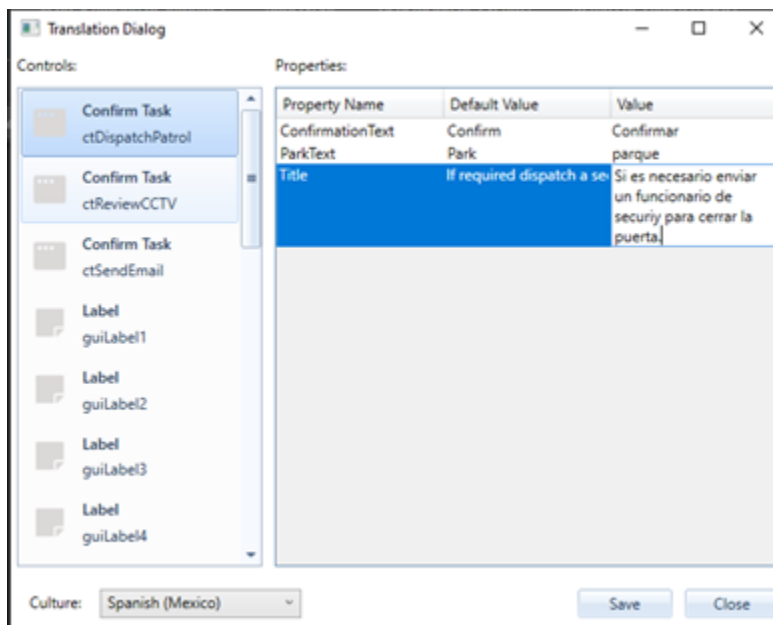
Translating a Graphical User Interface

To translate a graphical user interface to a different language:

1. In **System Configuration**, navigate to the graphical user interface you want to translate.



2. Select the graphical user interface.
3. From **Properties**, select **Translate ...**. The **Translation Dialog** is displayed.



4. In **Translation Dialog**, from **Culture** drop-down list, select the culture you want to translate to.
5. Select the user control you want to translate.
6. Select the property you want to translate.

7. In **Value**, type the translation.
8. Select **Save** to save and close the **Translation Dialog**.

Exporting Dynamic Text Ready for Localization

For mass translation, you can export all configured UI content so that it can be translated and imported.

Control Center comes packaged with localized text for all static text values in the product. However, all dynamic text in the solution must also be translated.

This is split into two separate areas. The first area is the object labels and descriptions, which includes alarm type activity and resolution types. The second area is the GUI control text. Each area must be exported separately, translated, and imported back into the solution.

Exporting Object Labels and Descriptions for Localization

Use the following steps to export the dynamic text into a .CSV file ready for translation.

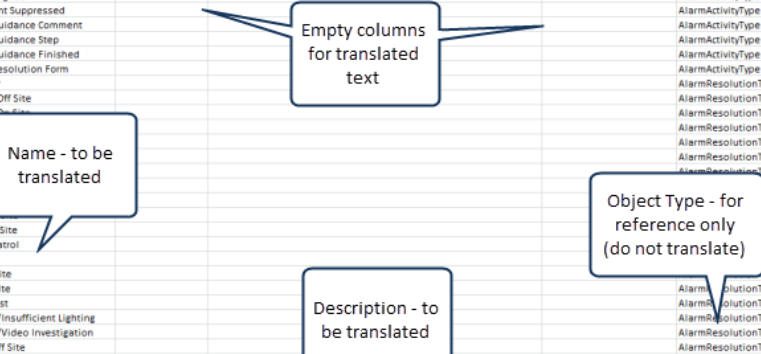
1. Open the SQL Server management Studio.
2. Connect to the SQL Server instance containing the Control Center pacific database for the configured solution.
3. Expand **Databases**.
4. Right-click on the pacific database and then click **New Query**.
5. Enter the following SQL and then
6. press F5.

```
EXEC IPSC.Translations_List '<culture>'
```

where *culture* is a combination of a language and country code, for example, **ar-SA** for Arabic (Saudi Arabia). (A complete list of all country ISO codes is described in the ISO 3166 international standard and a complete list of all language codes is described in ISO-639 Language Codes.)

7. Right-click in the results window and then click **Save Results As...**
8. Save the results as a CSV file.
9. The name and description columns (columns B and D) must then be translated into their neighboring columns (C and E) ready to import back into Control Center.

ID	A	B	C	D	E	F
ID	Name	TranslatedLabel	Description	TranslatedDescription	ObjectType	
2	2BDB3FE5-9568-E211-981E-F078CBA9C05A	SLA Elapsed				AlarmActivityType
3	2CDB3FE5-9568-E211-981E-F078CBA9C05A	Alarm Handled				AlarmActivityType
4	2DDB3FE5-9568-E211-981E-F078CBA9C05A	Alarm Parked				AlarmActivityType
5	2EDB3FE5-9568-E211-981E-F078CBA9C05A	Alarm Resolved				AlarmActivityType
6	2FDB3FE5-9568-E211-981E-F078CBA9C05A	Alarm Assigned				AlarmActivityType
7	30DB3FE5-9568-E211-981E-F078CBA9C05A	Alarm Point Suppressed				AlarmActivityType
8	31DB3FE5-9568-E211-981E-F078CBA9C05A	Process Guidance Comment				AlarmActivityType
9	32DB3FE5-9568-E211-981E-F078CBA9C05A	Process Guidance Step				AlarmActivityType
10	33DB3FE5-9568-E211-981E-F078CBA9C05A	Process Guidance Finished				AlarmActivityType
11	34DB3FE5-9568-E211-981E-F078CBA9C05A	Initiate Resolution Form				AlarmActivityType
12	35DB3FE5-9568-E211-981E-F078CBA9C05A	Contractor				AlarmResolutionType
13	36DB3FE5-9568-E211-981E-F078CBA9C05A	Engineer Off Site				AlarmResolutionType
14	37DB3FE5-9568-E211-981E-F078CBA9C05A	Engineer On Site				AlarmResolutionType
15	38DB3FE5-9568-E211-981E-F078CBA9C05A	Environ				AlarmResolutionType
16	39DB3FE5-9568-E211-981E-F078CBA9C05A	False Al				AlarmResolutionType
17	3ADB3FE5-9568-E211-981E-F078CBA9C05A	Fire Al				AlarmResolutionType
18	3BDB3FE5-9568-E211-981E-F078CBA9C05A	Fire Bri				AlarmResolutionType
19	3CDB3FE5-9568-E211-981E-F078CBA9C05A	Intrude				AlarmResolutionType
20	3DD3FE5-9568-E211-981E-F078CBA9C05A	Membe				AlarmResolutionType
21	3ED3FE5-9568-E211-981E-F078CBA9C05A	Police O				AlarmResolutionType
22	3FD3FE5-9568-E211-981E-F078CBA9C05A	Police On Site				AlarmResolutionType
23	40DB3FE5-9568-E211-981E-F078CBA9C05A	Security Patrol				AlarmResolutionType
24	41DB3FE5-9568-E211-981E-F078CBA9C05A	Staff Error				AlarmResolutionType
25	42DB3FE5-9568-E211-981E-F078CBA9C05A	Staff Off Site				AlarmResolutionType
26	43DB3FE5-9568-E211-981E-F078CBA9C05A	Staff On Site				AlarmResolutionType
27	44DB3FE5-9568-E211-981E-F078CBA9C05A	System Test				AlarmResolutionType
28	45DB3FE5-9568-E211-981E-F078CBA9C05A	Unknown/Insufficient Lighting				AlarmResolutionType
29	46DB3FE5-9568-E211-981E-F078CBA9C05A	Unknown/Video Investigation				AlarmResolutionType
30	47DB3FE5-9568-E211-981E-F078CBA9C05A	Vehicle Off Site				AlarmResolutionType
31	48DB3FE5-9568-E211-981E-F078CBA9C05A	Vehicle On Site				AlarmResolutionType
32	D141AF44-CE6E-E211-A307-005056C00008	Video Wall 3	Client Computer with the IP hostname of VW3.CNLUK.COM			Client
33	221D6C4C-CE6E-E211-A307-005056C00008	Video Wall 2	Client Computer with the IP hostname of VW2.CNLUK.COM			Client
34	1C1B8754-CE6E-E211-A307-005056C00008	Workstation 1	Client Computer with the IP hostname of WS1.CNLUK.COM			Client
35	6A6AE986-A968-E211-981E-F078CBA9C05A	Standard Web Client	Standard Web Client			Client
36	F9FE1426-856C-E211-856F-F078CBA9C05A	Video Wall 1	Client Computer with the IP hostname of VW1.CNLUK.COM			Client
37	606AE986-A968-E211-981E-F078CBA9C05A	Online State Data Connection	For device online state reports			DataConnection
38	536AE986-A968-E211-981E-F078CBA9C05A	24 x 7 Allow	This default Date Time Schedule permits operation at any time.			DateTimeSchedule
39	546AE986-A968-E211-981E-F078CBA9C05A	System Maintenance	This default Date Time Schedule denotes when the system maintenance will be executed.			DateTimeSchedule
40	63695D48-D76E-E211-A1CD-005056C00008	Drop Zone	Display Area objects represent containers that can host Tile Layouts. Display Areas allow the same			DisplayArea
41	9550A83-D96E-E211-A1CD-005056C00008	Video Wall	Display Area objects represent containers that can host Tile Layouts. Display Areas allow the same			DisplayArea
42	646AE986-A968-E211-981E-F078CBA9C05A	Main Menu	Main Menu Display area is the default monitor to use			DisplayArea
43	656AE986-A968-E211-981E-F078CBA9C05A	System Explorer	System Explorer Display area is where the System Explorer is displayed.			DisplayArea
44	676AE986-A968-E211-981E-F078CBA9C05A	System Main	The main display area of the system.			DisplayArea



Exporting GUI Control Text for Localization

The English text for all the GUI controls must be exported into a CSV file so these can also be translated.

Each GUI lists all the control text in the database which can be localized. This occurs when the GUI is saved. Therefore, any logic which has been imported or existed in the solution before the Internationalization feature was introduced will not contain the relevant GUI control text entries in the database. To ensure the database contains all the relevant GUI control text for translation, open and save every GUI before exporting the data.

Open and save all GUIs which require translation to ensure the database contains all the relevant text.

To export all GUI control text:

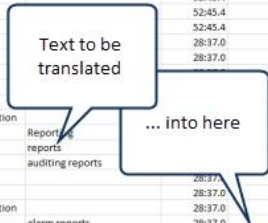
1. Open SQL Server Management Studio.
2. Connect to the SQL Server instance containing the Control Center pacific database for the configured solution.
3. Expand **Databases**.
4. Right-click on the pacific database and then click **New Query**.
5. Enter the following SQL and then press F5.

```
SELECT* , 'as TranslatedText
FROM IPSC.GraphicalUserInterfaceControlLC
```

WHERE CultureId='Default'

6. Right-click anywhere in the **Results** window and then click **Save Results As...**
7. Save the results as a .CSV file.
8. The text in **Text** column (F) must then be translated ready to be added back into the relevant GUIs via the **Translations** property.

ID	A	B	C	D	E	F	G	H
1		GraphicalUserInterfaceID	CultureId	ControlName	PropertyName	Text	LastModified	TranslatedText
2	4FD932D0-6C70-E211-8883-F07BCBA9C05A	78082323-6870-E211-8883-F07BCBA9C05A	Default	guiButton2	Text	Clear	52:45.4	
3	50D932D0-6C70-E211-8883-F07BCBA9C05A	78082323-6870-E211-8883-F07BCBA9C05A	Default	guiButton2	Confirmation Text		52:45.4	
4	51D932D0-6C70-E211-8883-F07BCBA9C05A	78082323-6870-E211-8883-F07BCBA9C05A	Default	guiButton1	Text	Load	52:45.4	
5	52D932D0-6C70-E211-8883-F07BCBA9C05A	78082323-6870-E211-8883-F07BCBA9C05A	Default	guiButton1	Confirmation Text		52:45.4	
6	53D932D0-6C70-E211-8883-F07BCBA9C05A	78082323-6870-E211-8883-F07BCBA9C05A	Default	guiSearchControl1	Title		52:45.4	
7	54D932D0-6C70-E211-8883-F07BCBA9C05A	78082323-6870-E211-8883-F07BCBA9C05A	Default	guiSearchControl1	Description		52:45.4	
8	68C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_0_label		28:37.0	
9	6CC3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_0_Group_0_label		28:37.0	
10	6C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_0_Group_0_item_0_label			
11	6EC3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_0_Group_0_item_0_description			
12	6FC3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_0_Group_0_item_0_tooltip			
13	70C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_0_Group_0_item_0_tooltipdescription			
14	71C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_label	Reporting reports		
15	72C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_label	auditing reports		
16	73C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_0_label			
17	74C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_0_description		28:37.0	
18	75C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_0_tooltip		28:37.0	
19	76C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_0_tooltipdescription		28:37.0	
20	77C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_1_label	alarm reports	28:37.0	
21	78C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_1_description		28:37.0	
22	79C3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_1_tooltip		28:37.0	
23	7AC3BA9E-8270-E211-8883-F07BCBA9C05A	CA7F1244-D4D2-4DCA-9D21-786973550688	Default	guiRibbon1	Tab_1_Group_0_item_1_tooltipdescription		28:37.0	
24	1004F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtFirstName	Text		22:45.7	
25	1104F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtFirstName	Title	First Name	22:45.7	
26	1204F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtFirstName	Description		22:45.7	
27	1304F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtLastName	Text		22:45.7	
28	1404F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtLastName	Title	Last Name	22:45.7	
29	1504F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtLastName	Description		22:45.7	
30	1604F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtPhoneNumber	Text		22:45.7	
31	1704F89B-8B6C-E211-856F-F07BCBA9C05A	151499AD-856C-E211-856F-F07BCBA9C05A	Default	txtPhoneNumber	Title	Phone Number	22:45.7	



Importing Localized Object Labels and Descriptions

You can import translated text into Control Center by importing the data from the translated CSV into a temporary database table in pacific database called dbo.translations, and then finalize by running a stored procedure to update the various pacific tables with the imported data.

1. Open SQL Server Management Studio.
2. Connect to the SQL Server instance containing the Control Center pacific database for the configured solution.
3. Expand **Databases**.
4. Expand the pacific database > tables node.
5. Delete the table dbo.translations if it exists.
6. Right-click the pacific database, point to **Tasks**, and then click **Import Data...**
7. Click **Next** on the **Welcome** page. On the **Data Source** page, choose **Flat File Source** from the drop-down.
8. Specify the file name by clicking the **Browse** button, locating the .CSV file containing the translated text and then clicking **Open**.
9. Select the Column names in the first data row option.
10. Click the **Advanced** option on the left-hand menu.

11. Select each column in turn and set the **OutputColumnWidth** value to **250** for all columns.
12. Click **Next** to continue to the destination page.
13. Ensure that the specified server name is correct.
14. Specify valid authentication details.
15. Ensure the specified database is **pacific**, and then click **Next** to continue.
16. Ensure that the destination table is called `[dbo].[translations]`, then click **Next** to continue.
17. Ensure that the **Run immediately** option is checked, then click **Next** to continue.
18. Click **Finish** to begin the data import. Once the data has been imported into the translation database table, follow the steps below to copy the translated data into the relevant database tables in **pacific**.
19. Right-click in the **pacific** database and then click **New Query**.
20. Enter the following SQL and then press F5:

```
EXEC IPSC.Translations_Translate '<culture>'
```

where *culture* is a combination of a language and country code, for example, **ar-SA** for Arabic (Saudi Arabia). (A complete list of all country ISO codes is described in the ISO 3166 international standard and a complete list of all language codes is described in ISO-639 Language Codes.)

21. The translation table can be deleted as the stored procedure that was executed previously would have copied the data through the database into the relevant tables.

Servers and Services

An example using the above terminology would be where multiple machines are used to run the Rules Engine service. The Rules Engine service in this example is running on machines IPSC-RE-SVR-1 and IPSC-RE-SVR-2. These objects are automatically created in the Computers folder.

Rules Engine Server

- + IPSC-RE-SVR-1
- + IPSC-RE-SVR-2

A service object is created automatically in the Services folder. There should only ever be one instance of a service to which all server objects point to.

Rules Engine Service

- + Rules Engine Service Rules Engine Service

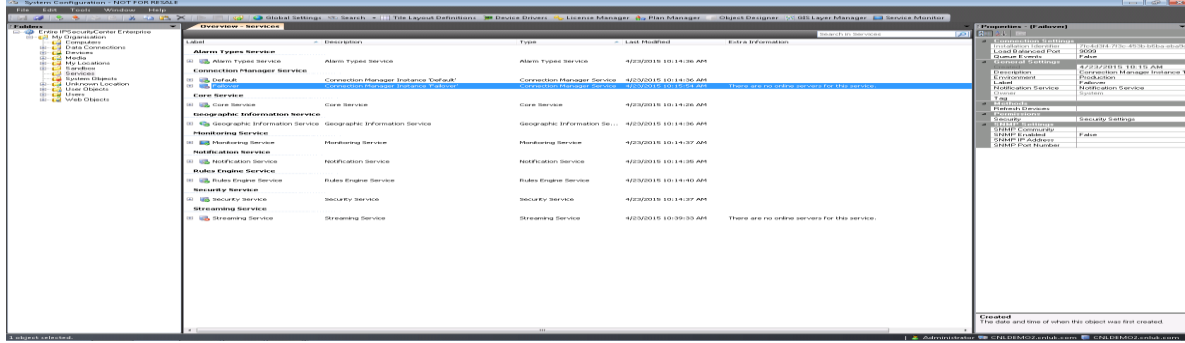
Each server object is configured to target the corresponding service object. In the following example, the Rules Engine Service property in the Rules Engine Server objects are set to point at the object called Rules Engine Service.

The screenshot shows the 'Properties - (IPSC-RE-SVR-2)' window. The 'General Settings' section is expanded, displaying a table of properties. The 'Rules Engine Service' property is highlighted with a red box, showing its value as 'Rules Engine Service'.

Properties - (IPSC-RE-SVR-2)	
General Settings	
Created	9/27/2013 2:55 PM
Description	Server with the IP hostname of C
Enabled	True
Environment	Production
Fully Qualified Name	CarlG-Laptop.cnluk.com
Label	IPSC-RE-SVR-2
Owner	System
Rules Engine Service	Rules Engine Service
Schedule	No schedule set
Tag	

Certain service objects also include event viewers which can be used to monitor the event passing through the system. The different event viewers are described in the following sections.

If a Control Center service is not in an operational state, the System Configuration interface provides any additional information available about the cause of the issue.

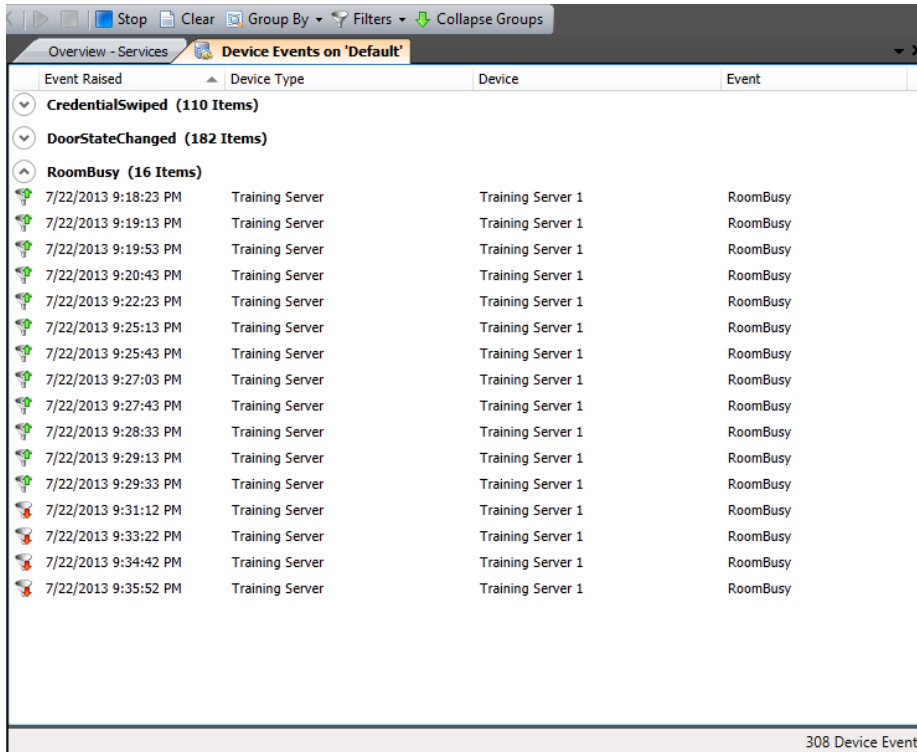


Connection Manager Event Viewer

The Connection Manager Device Event Viewer lists all events raised by the different devices under the control of a connection manager. The event viewer will list the events as they are received and subsequently processed by Control Center.

To open the Event Viewer, double-click a Connection Manager or right-click and select the Connection Manager Device Event Viewer.

The event viewer appears and will automatically start listing the events as they are received.



A toolbar associated with the event viewer provides the following options:

Option	Description
--------	-------------

Stop/Start	Stops and starts the logging of events. Events will not be cleared from the list when stopping or starting the logger.
Clear	Clears all events from the event viewer.
Group By	Provides options to group events by: None Events Device Type Device
Filters	Show All Filters - Displays the Event Filters dialog. See Connection Manager Event Filtering for more information. Clear All Filters - Clears all currently applied filters. View Filtered Events - Displays the filtered events.
Expand/Collapse Groups	Expands or collapses all groups when the results are grouped by one of the options above. The name of the button will change when clicked.

The Event Viewer also includes a total number of events logged on the status bar. A total will be shown for each group of events when events are grouped together.

Connection Manager Event Properties

The properties for each event can be viewed by simply selecting an event. The corresponding properties for the event will then be shown in the property grid.

Event Properties	
Date	10/7/2013 4:51 PM
DeviceIdentifier	81ba02f2-bd06-41d9-adc5-c40bc8c
Door	4
DoorLabel	Door 4
Email	andy.aracri@cnlsoftware.com
FirstName	Andy
Identifier	4
LastName	Aracri
Picture	http://+:56789/TrainingDriver/4.jpg
Reader	11
ReaderLabel	Reader 11
Result	Granted
ResultValue	1
Telephone	01483 4800004
Misc	
EventId	4a5157c2-702f-e311-be1b-005056c
SenderEventId	1c9e9d26-4ff0-43ae-ad78-fa4921ad
SenderId	276710be-2ae3-4329-82ed-6867a1f

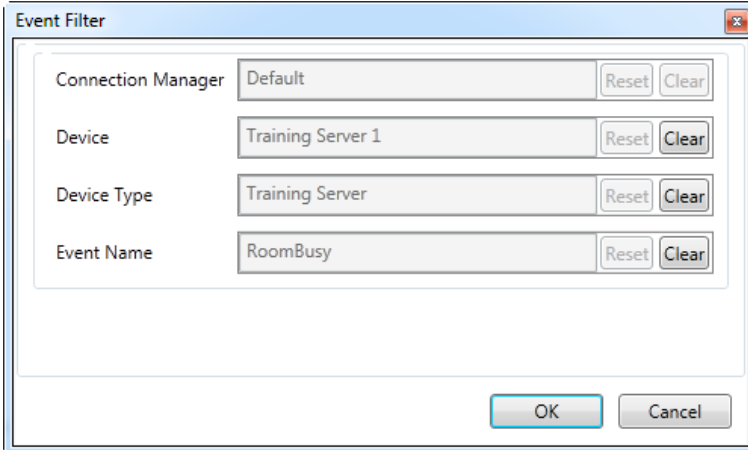
Connection Manager Event Filtering

Filters can be applied to the events being received by the connection manager. This can be used to drastically reduce the load on the services when lots of unwanted events are being received and processed.

To filter events for a Connection Manager:

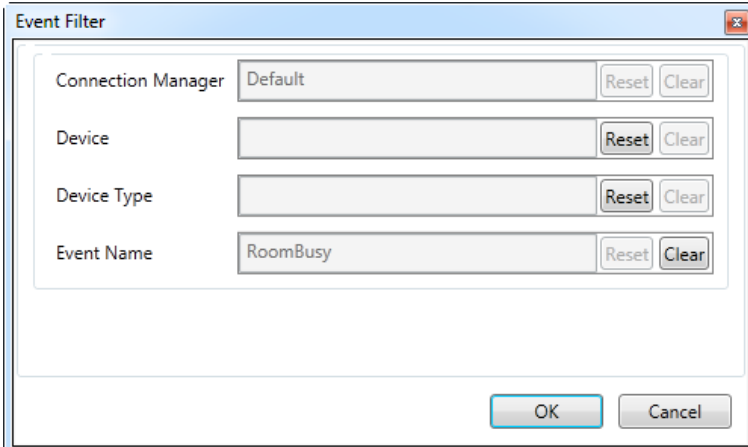
1. From **System Configuration** window, click **Services**. The **Overview - Services** dialog opens.
2. Double-click the **Connection Manager** for which you want to filter events. The **Device Events** for the selected **Connection Manager** are displayed.
3. Right-click anywhere in the event view and select **Filter**. The **Event Filter** dialog appears.

The **Event Filter** dialog shows the different options available for filtering, which includes filtering by device, device type or event name. By default, all filters include the Connection Manager, therefore the Connection Manager field cannot be cleared.



Use the **Reset** and **Clear** buttons to reset and clear events respectively. The following figure shows a filter on events based on the event name, Room Busy. Click **OK** to apply the filter.

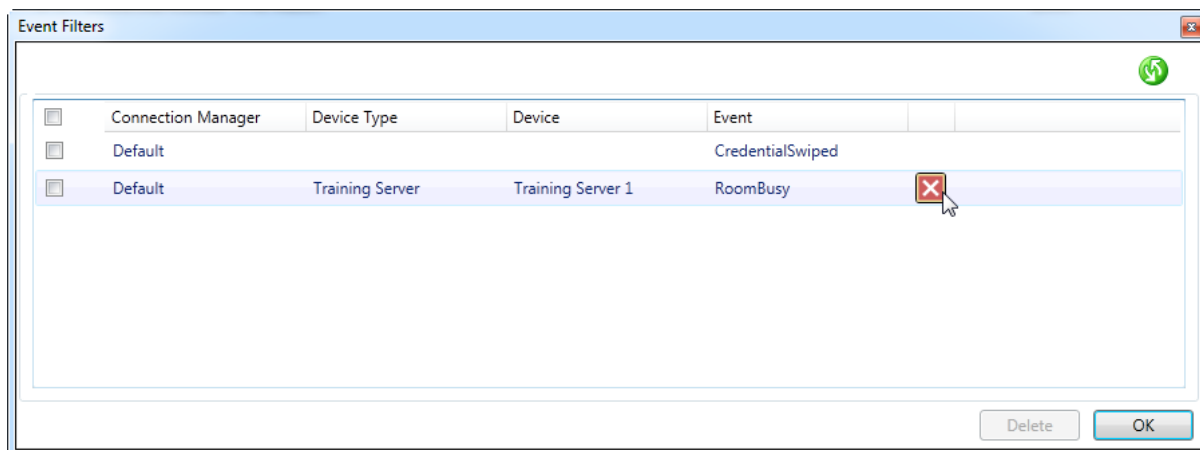
Ensure to restart the Connection Manager service for the filter to take effect.



All new events which are received by the Connection Manager, but subject to the applied filters, will not be forwarded onto other Control Center services for further processing. This includes logging the event in the pacific database and evaluating the event against triggers or alarm types. The event viewer will show an icon to indicate which events are filtered or not.

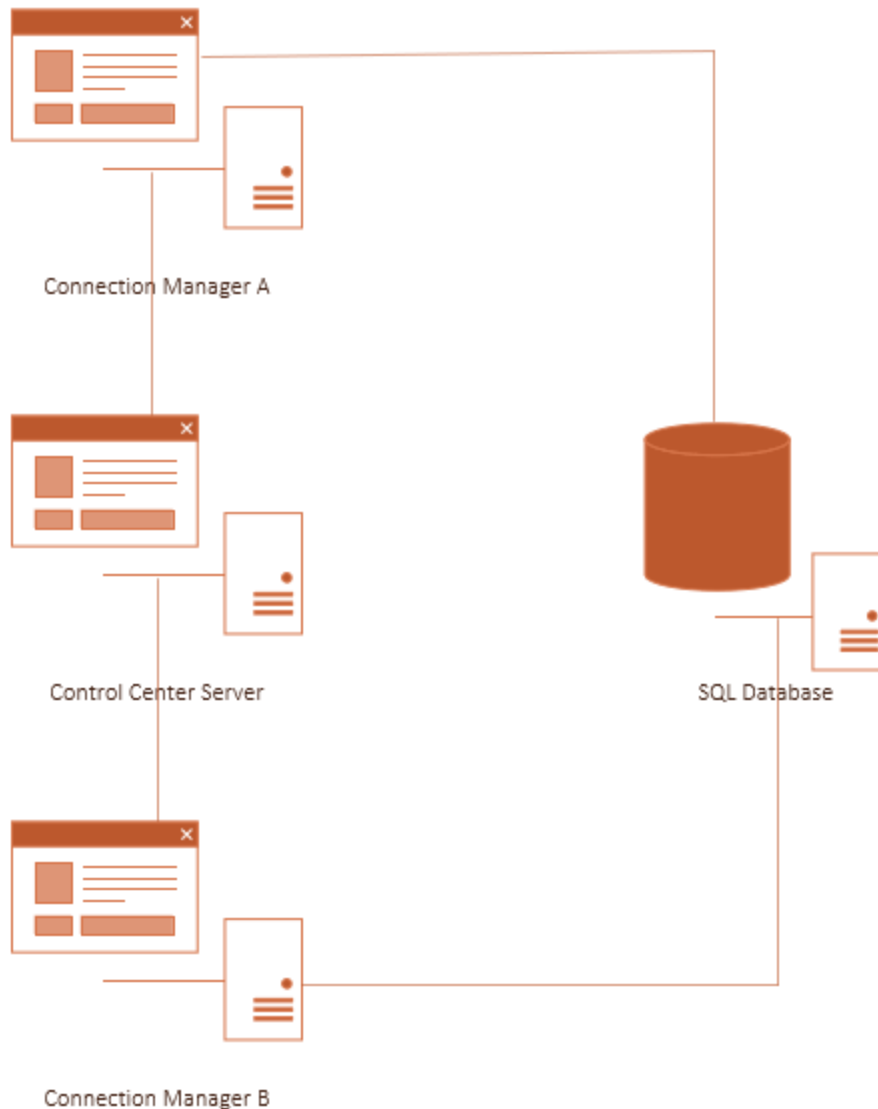
Not Filtered				
	7/22/2013 9:29:33 PM	Training Server	Training Server 1	RoomBusy
	7/22/2013 9:31:12 PM	Training Server	Training Server 1	RoomBusy
Filtered				

A list of all the currently applied filters is also available via the **Filters** toolbar item. Selecting the **Show All Filters** option will display the **Event Filters** dialog. You can delete any existing filter by clicking the delete button. Note that the Connection Manager service must be restarted following any changes to the filters.



Connection Manager Failover

Control Center supports the use of multiple Connection Manager (CM) instances to implement failover. Therefore, if one instance of the CM becomes unavailable another CM can resume the operations.

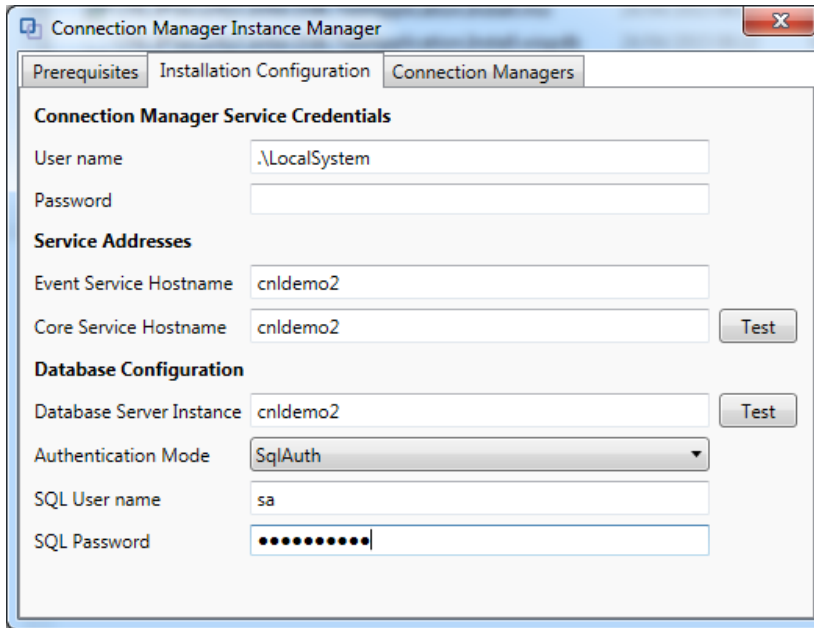


To configure two Connection Managers in failover mode, first install the Connection Manager on two separate servers.

It is recommended to give both the Connection Managers the same name.

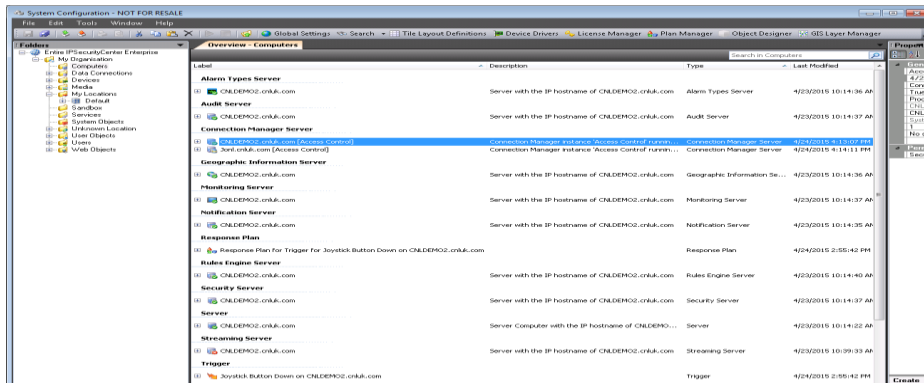
In the CM installer, use the **Installation Configuration** tab to set the **Event Service Hostname** and **Core Service Hostname** properties to point to the relevant services. The names shall be entered using IP or machine names, do not use localhost.

Also, set the **Database Instance Name** to point to the Control Center configuration database. This is the same for all Connection Managers.



Once the Connection Managers are installed and started, the following new objects will appear in System Configuration:

- Two CM servers in the Computers folder
- One CM Service in the Services Folder



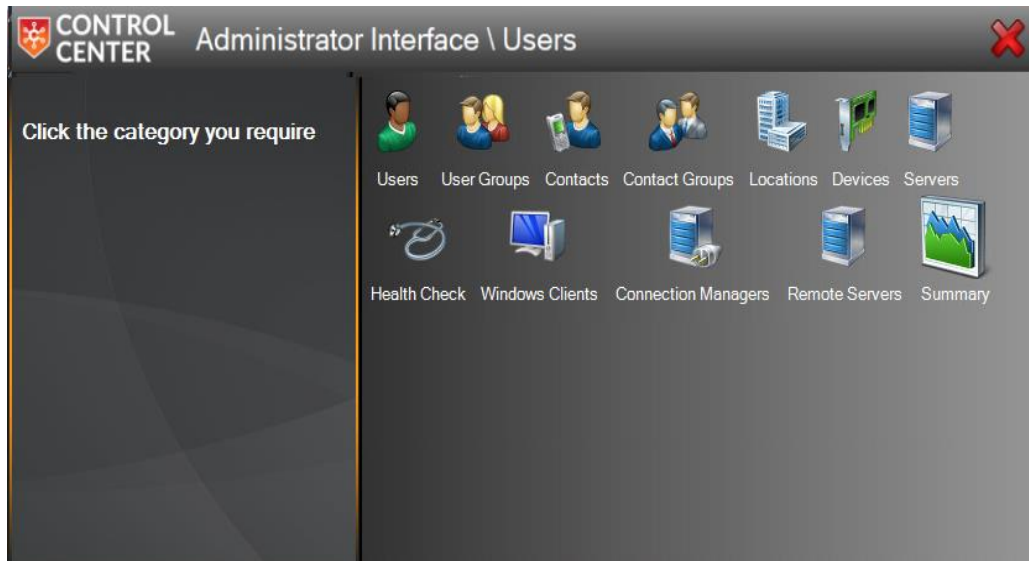
- Select the Connection Managers in the Computers folder. Observe that the property Connection Manager Service points to the same service for both CM servers. This is because the service now uses both Connection Manager servers but only one at a time.

Only one of the Connection Manager servers can be active at any one time. This is illustrated by the Online icon overlay. The remaining CM servers are pending. If a CM server is not running or if the Control Center server cannot contact the CM, the object is marked as failed in System Configuration and the reason for failure is shown in the Extra Information column.

Use the Server State Changed event to monitor the state of the servers (if required). Additional functionality is also available in the Administrator Interface. This can be used to monitor the status of Connection Managers and to restart Connection Managers.

To monitor status of Connection Managers through the Administrator Interface:

1. Open the **Admin Interface**.
2. Select **Connection Managers > Status**. The status of the Connection Managers is shown.



To restart the Connection Manager through the Administrator Interface:

1. Open the **Admin Interface**.
2. Select **Connection Managers**.
3. Double-click on the Connection Manager that needs to be restarted.

Connection Manager Priority

An installation can consist of physical servers with different specifications where one server performs better than others. It is then desirable to give the highest performing CM server a higher priority. This will have the effect that Control Center makes this the active CM when available.

To change the priority of the Connection Manager, set the Priority property of the CM Server object. 1 is the highest priority.

Calculated Device States

The online state of all devices that are connected to the Connection Manager is only refreshed when the Connection Manager is online. If the Connection manager is offline, the devices will be assumed to be offline and unavailable.

Rules Engine Event Viewer

The Rules Engine Event Viewer lists all events processed by the selected Rules Engine server.

The Rules Engine Event Viewer is available on a per-server basis. This will report all events processed at a machine service level rather than at the overarching Control Center service level.

To open the event viewer either double-click a rules engine server or right-click and select **Rules Engine Event Viewer**. The event viewer will be shown and will automatically start listing the events as they are processed.

Sensor Service

The Sensor Service can be used to monitor and respond to data received from sensor devices. These sensors can be in standalone devices or embedded in many types of device already supported by Control Center.

Once installed and enabled the service will process sensor readings from supported devices. The service can support thousands of sensor readings per second.

Existing Device Connectors will need to be updated to provide sensor data in the format required by the Sensor Service.

All sensor readings are stored in the Control Center database and can be viewed by finding the device in System Configuration, System Explorer, or on a scene, then right clicking and selecting **View Recent Events**:

Received Date Time	Description	Alarm Point	Location	Event Count
2/9/2023 4:57:22 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:57:17 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:57:12 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:57:07 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:57:02 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:56:57 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:56:52 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:56:47 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:56:42 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:56:37 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:56:32 PM	Device Event	Server Room Temp	Building 11	1
2/9/2023 4:56:27 PM	Device Event	Server Room Temp	Building 11	1

Property	Value
Description	Server Room Temperature Sensor
SpatialReferenceIdentifier	0
SensorType	Temperature
UnitOfMeasure	DegC
SensorValue	24
ScalingFactor	1
DeviceIdentifier	61ef32c0-a380-4cad-b731-e98efeadc7c6
Date	2/9/2023 4:57:17 PM
DeviceLabel	Server Room Temperature Sensor
EventReceivedTime	2/9/2023 4:57:17 PM

Threshold Rules

The sensor service will evaluate each reading against a set of user-configured rules called Threshold Rules.

When a sensor reading is received with a value that corresponds to one of the configured rules, a **Threshold Breached** event is raised by the Sensor Service.

This event can be used to trigger various actions within Control Center. For example it could trigger a response plan that notifies a user about a sensor reading that is higher than expected, or create an alarm if a sensor reading is at a dangerous level.

Creating a Threshold Rule

1. Open **System Configuration** and navigate to the **Services** folder.
2. Double click on the **Sensor Service** to open the Threshold Configuration Rules window.

Device Name	Operator	Threshold Value 1	Threshold Value 2	Criticality
Server Room Temperature Sensor	LessThan	20	0	0
Server Room Temperature Sensor	Between	20	30	1
Server Room Temperature Sensor	Between	30.01	50	2
Server Room Temperature Sensor	GreaterThan	50	0	3

3. Use the button on the toolbar, or right click in the window and select **Add New Rule**, to open the Threshold Configuration window.

Threshold Configuration

Device:

Operator:

Threshold Value 1:

Threshold Value 2:

Criticality:

Ok Cancel

4. Use the available parameters to configure the threshold rule as required:

Parameter	Description	Value
Device	This is the device that the sensor service will evaluate against this threshold.	Any device in Control Center.
Operator	Defines the evaluation to be made between the sensor value and threshold value.	EqualsTo GreaterThan LessThan Between

Threshold Value 1	The value to which the sensor reading will be compared. If using the Between operator, this is the minimum value that will be considered as part of the threshold.	Any decimal value
Threshold Value 2	If using a Between operator this is the maximum value that will be considered as part of the threshold.	Any decimal value
Criticality	This field can be used to assign a priority to the threshold rule which can later be used to take different actions in Control Center.	Free text

5. Click **Ok** to save the threshold rule.

Currently, Threshold rules can only be configured for an individual device. It is not possible to configure a rule for a type of sensor or specific location.

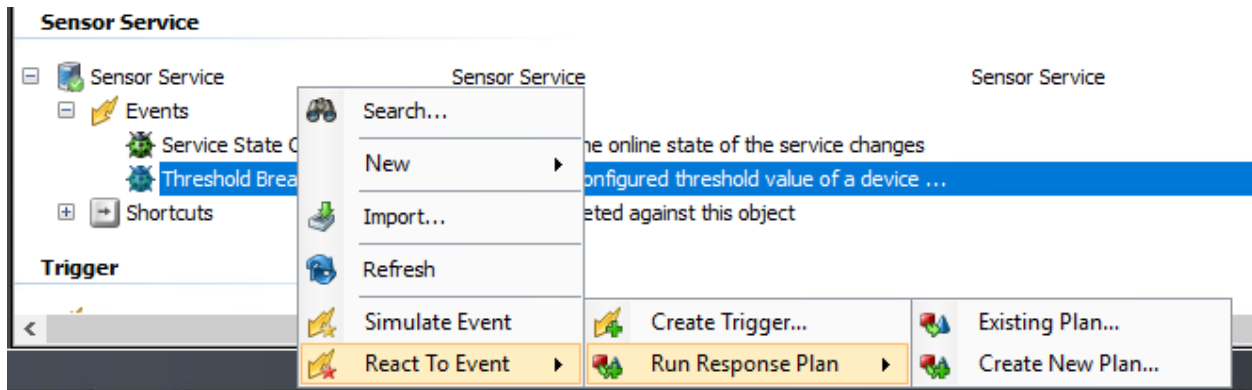
Users can also edit or delete a rule by right clicking on the rule in the Threshold Configuration window.

Using Threshold Rules

Running a Response Plan

See the Response Plans section for detailed information on creating a new response plan.

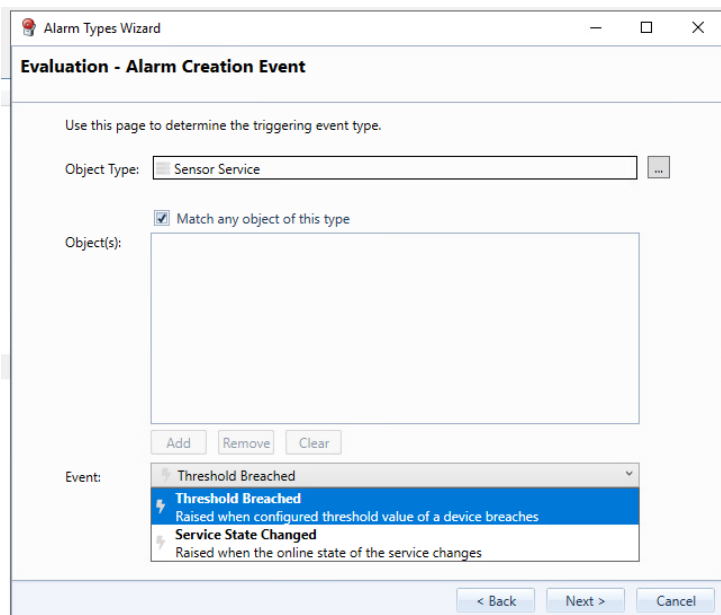
1. Open **System Configuration** and navigate to the **Services** folder.
2. Right click on the **Sensor Service**, then select **React To Event, Run Response Plan**, and select either **Existing Plan** or **Create New Plan**.



Creating an alarm

See the Alarm Types section for detailed information on creating a new alarm.

- To create alarms when a Threshold Rule is breached, search for and select the **Sensor Service** as the **Object Type** on the **Alarm Creation Event** page and select **Threshold Breached** as the **Event**.



- On the **Alarm Creation Event Conditions** page, you can use event properties to narrow down the threshold rules that will trigger the creation of the alarm. For

example, you can specify that the threshold must have a certain criticality value:

Source	Operator	Destination
<input checked="" type="radio"/> Event Property <input type="radio"/> Object Property Criticality	Equals	<input type="radio"/> Event Property <input type="radio"/> Object Property <input checked="" type="radio"/> Constant Value Major

- On the Alarm Point screen, you can select **Use Event Property** and then select **Device** to use the sensor device that provided the reading as the alarm point. This is useful if you want to apply an alert state to the device to be displayed on a scene.

Use Event Property

Property:

Currently, any alarms created using this property must be handled and resolved manually. Alarm Type Modifiers will not affect alarms created this way.

Secondary Authorization

Secondary Authorization provides the ability for an authorizer to authorize an activity before it is performed, for instance adding or changing a contact or user. The affected areas where permissions are changed will require a second authorized user to authorize the changes. When a request comes through, a notification is shown on the Client. The number of outstanding requests is also shown in the status bar.

The Config Authorization Interface, available as a GUI Control and accessible from the System menu displays all requests awaiting authorization, such as requests to access System Configuration, renaming of the folder, and so on. It is where you approve or reject requests.

The Config Authorization changes affect the following areas in Control Center.

- . Admin Interface
 - . Users
 - . User Groups
 - . Contacts
 - . Contact Groups
 - . Locations
 - . Enable/Disable Devices
- . System Configuration

- . **Access to System Configuration:** Users requiring authorization to be able to access System Configuration based on the authorizers listed in the Security Policy. When the authorizer approves the request, the user will be granted access to System Configuration. If the authorizer rejects the request, the user will be denied access. The user will be informed whether the request was denied, or the request timed out.
- . **Create / Delete / Change Object**
- . **Changing Settings**
- . **Executing Actions**
- . Any User Function configured to use Secondary Authorization

Secondary Authorization Prerequisites

- At least two clients configured to the same server (one as an administrator and the other as a user).
- More than one user and user group

Global Settings Configuration

There are four Configuration options for managing the Secondary Authorization settings:

- Authorization for accessing System Authorization Configuration request timeout
- Authorization required for accessing System Configuration
- Enable Configuration Authorization
- Enable Location Based Configuration Authorization

These settings help the administrator to enable/disable the access to System Configuration and Admin Interface to users/user groups. The options are as explained below:

The screenshot shows the 'Enterprise Settings Configuration' window. On the left is a sidebar with 'Enterprise Settings' selected. The main area is titled 'Configure Enterprise Settings' and shows 'Local Enterprise Settings' selected. Below this is a table with columns 'Name' and 'Value'.

Name	Value
Authorization	
Authorization for accessing System Configuration request timeout	0
Authorization required for accessing System Configuration	<input type="checkbox"/>
Enable Configuration Authorization	<input checked="" type="checkbox"/>
Enable Location Based Configuration Authorization	<input type="checkbox"/>
Request Archiving Period (days)	10

Option	Value
Authorization for accessing System Configuration request timeout	Default is set to 30 sec. This means that if a request is not authorized by the authorizer within 30 secs, the request will be rejected.
Authorization required for accessing System Configuration	Enabled/Disabled. If this is enabled, the user must request authorization to gain access to System Configuration. This setting requires 'Enable Configuration Authorization' to also be enabled for request notifications to apply.
Enable Configuration Authorization	Enabled/Disabled. If this is enabled, the user must request authorization to perform administrative tasks in System Configuration or in the Admin Interface, including creating or changing objects, devices, disabling devices etc.
Enable Location Based Configuration Authorization	Enabled/Disabled. If this is enabled, it means that no two clients within the same location can authorize each other's request.
Request Archiving Period (days)	Secondary Authorization requests are continuously replicated to the Archive database. Request Archiving Period defines how long requests are stored for before they are deleted from the primary pacific database tables.

Users must re-login after the 'Enable Configuration Authorization' setting has changed.

Configuring Security Policies for Configuration Authorization

You can configure the following security policies for configuration authorization:

- **Configuration Authorization Required** – Specify which users and groups are required to have their configuration changes authorized (Root user, Administrator etc.).
- **Configuration Authorizers** – Specify which users and groups can authorize configuration changes (Root user, Administrator etc.).

The policy can be turned on or off and would apply to all Control Center clients connected to the server.

Enabling Configuration Authorization Required policy

Once configured, this policy lists all the users that need authorizing of one of the following requests:

- Users that require Secondary Signoff
- Users that do not require Secondary Signoff

To set the Configuration Authorization Required policy:

1. From the **System Configuration** window, right-click on the Users folder and select **Security Policy**.
2. Expand **Security Policies > User Policies**. The available policies are displayed on the right.
3. Double-click the **Configuration Authorization Required** policy. The **Configuration Authorization Required** dialog appears.
4. Select the **Define Policy** check box and then click Users and Groups to add users and groups whose configuration changes need authorization from another user (for example, an Administrator).
5. Click **OK**.

When a user attempts to launch System Configuration, a dialog box appears notifying that a request has been created for another user to grant them access.

This setting will be only effective if there are multiple accounts configured as authorizers.

Enabling Configuration Authorizers Security Policy

Once configured, this policy lists all the users that can authorize one of the following requests:

- Users that require Secondary Signoff
- Users that do not require Secondary Signoff

To configure authorizers:

1. From **System Configuration**, access the Security Policies in the same way as the previous section.



2. Double-click the Configuration Authorizers policy. The **Configuration Authorizers Properties** dialog appears.
3. Select the **Define Policy** check box and then click **Users and Groups** to add users and groups that can authorize configuration changes (for example, an Administrator).
4. Click **OK**.

Authorizing Requests

The users attempting an action that requires authorization will require a second user to authorize the action.

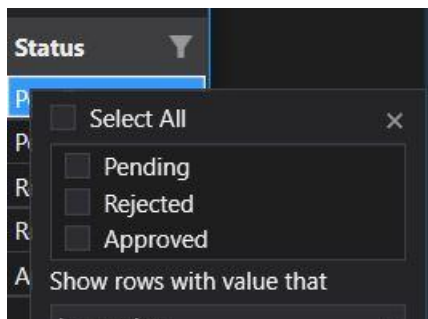
For example, you can require that an attempt to add a user requires authorization. To demonstrate this scenario:

From the Admin Interface, add a new user. To do this:

1. Click on the **Users** tab and then  button which will take you to the **Add Users** window.
2. Enter the user details and click **OK**.
3. Enter the comment in the **Configuration Authorization Request** box.
4. Press .
5. The authorizing client will receive a notification at the bottom right corner of the screen.
6. Click on this to go to configuration **Authorization** window.

Mark All		Unmark All		Reject	Approve
Full Text Search					
	Description	Requested User	Requested Date	Requested Client	Status
<input type="checkbox"/>	Add Test user	Limited Admin User	12/12/2018 2:16:05 PM	DEVnetClient174.CNLUKDE	Pending
<input type="checkbox"/>	Add djskdj	Limited Admin User	12/12/2018 1:31:32 PM	DEVnetClient174.CNLUKDE	Pending
<input type="checkbox"/>	Open System Configuration DEVnetClient174.	Limited Admin User	12/11/2018 12:08:17 PM	DEVnetClient174.CNLUKDE	Rejected
<input type="checkbox"/>	Open System Configuration DEVnetClient174.	Limited Admin User	12/11/2018 11:41:31 AM	DEVnetClient174.CNLUKDE	Rejected
<input checked="" type="checkbox"/>	Add test user	Limited Admin User	12/11/2018 10:59:42 AM	DEVnetClient174.CNLUKDE	Approved

7. Click the **Status** tab on the menu to open the drop-down menu and select **Approved** to approve a request.



You can also access the **Config Authorization** dialog by clicking on the status bar at the bottom of the main display area. Any changes that need approval or rejection and the existing declined/approved requests will appear here. However, only the requests awaiting approval or rejection will have the check box enabled.

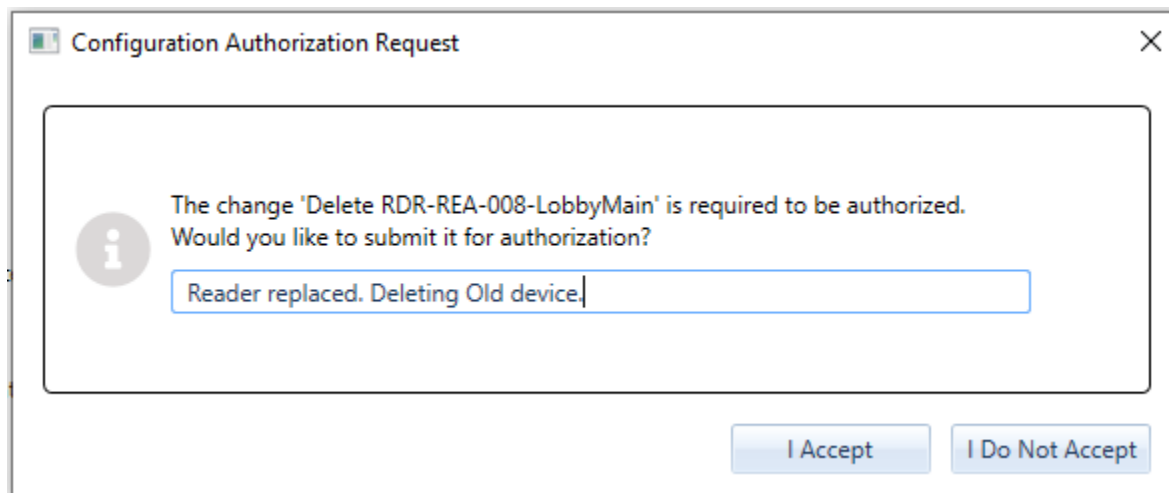
Authorization for Accessing System Configuration Request Timeout

There is a time limit that can be set in the Enterprise Settings of the authorizer, which says that if the request is not honored in that time frame, then it will automatically be rejected.

Secondary Authorization in System Configuration

Configuration Authorization for Creating, Updating and Deleting Objects

When Configuration Authorization is enabled, a number of changes to specific object types requires Secondary Authorization. An attempt to create, update or delete these objects will result in the Authorization Request dialog being shown and the user prompted to complete a request.



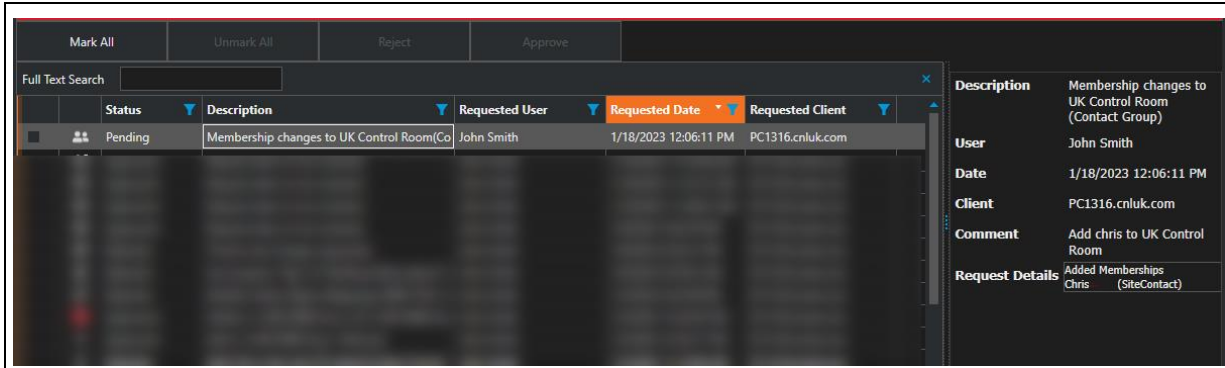
The change will be shown within the Secondary Authorization grid with a short description. Selecting the request row shows more information in the information panel

at the right side of the grid. The additional information available depends on the object and change.

Description	Requested User	Requested Date	Requested Client	Status
Delete RDR-REA-008-LobbyMain	John Smith	24/11/2022 17:25:55	PC1316.cnluk.com	Pending

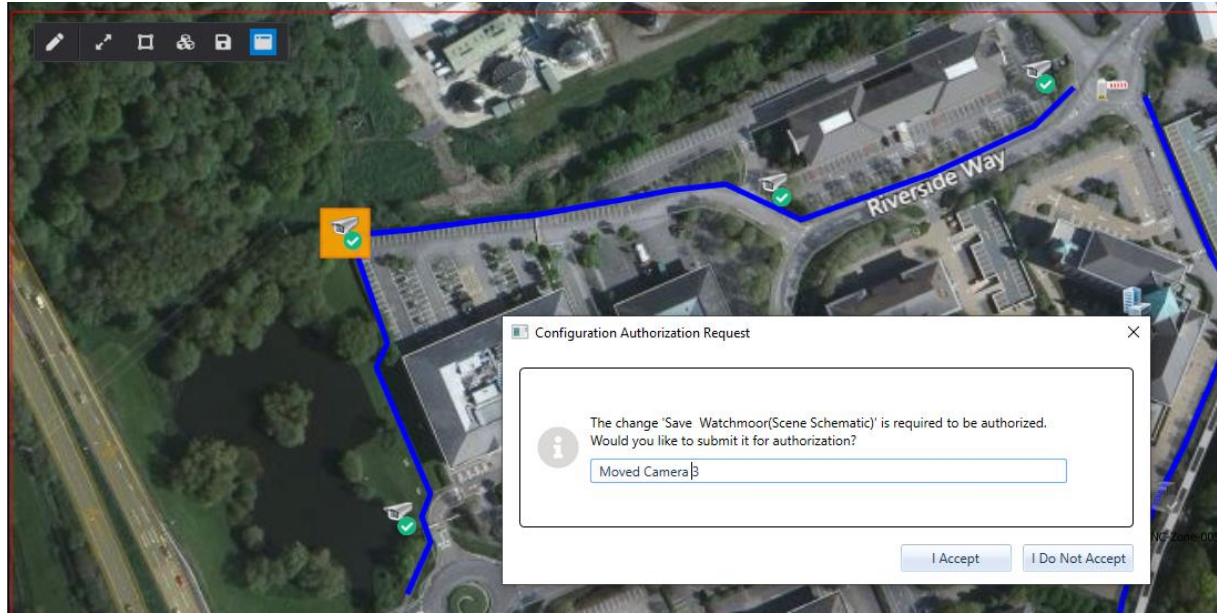
The following object types and changes are governed by Secondary Authorization.

Object Type	Change Requiring Secondary Authorization
Alarm Types	Enable / Disable / Delete Default SLA Changes
Alert State	Create Property Change Delete Disable / Enable Rename Note: Alert Object and Reset Alert functions provide limited information in request details when multiple objects are selected.
Contact	Create Property Change Delete Disable / Enable Rename Change 'Member Of'
Contact Group	Create Property Change Delete Disable / Enable Rename Change Members

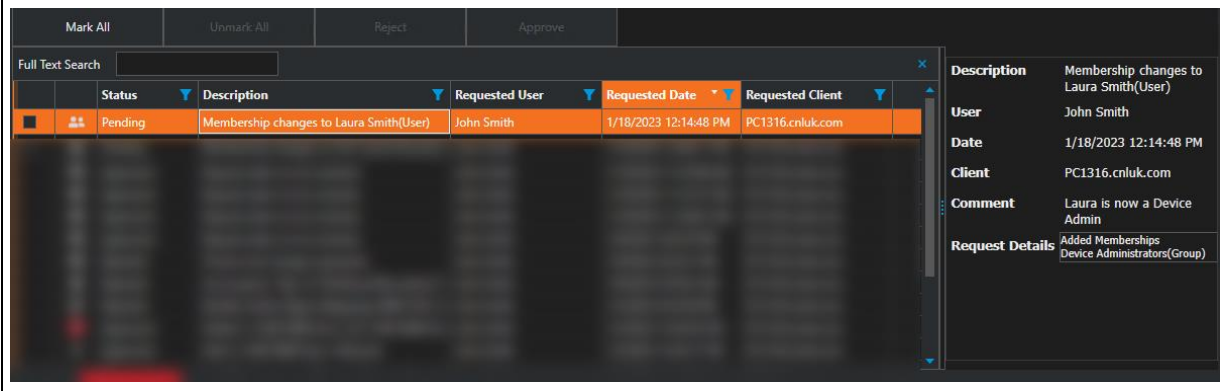


Device	<ul style="list-style-type: none"> Create Delete Disable / Enable Rename
Group	<ul style="list-style-type: none"> Create Property Change Delete Disable / Enable Rename Change Members
Media	<ul style="list-style-type: none"> New Media Update Media Create Property Change Delete Disable / Enable Rename
Placeholder	<ul style="list-style-type: none"> Create Property Change Delete Create from device...
Scene	<ul style="list-style-type: none"> Create Property Change

	<p>Delete</p> <p>Disable / Enable</p> <p>Edit Scene</p>
--	---



User	<p>Create</p> <p>Property Change</p> <p>Delete</p> <p>Disable / Enable</p> <p>Rename</p> <p>Change 'Member Of'</p>
------	--



Lock Down Non-Compliant Objects

Not all object types and functions within System Configuration are compliant with secondary authorization. Before a Control Center solution is deployed in a production environment requiring secondary authorization for System Configuration, these object types and functions must be locked down by preventing user access using Type Permissions. Set the locked-down Type Permission object to be in use in production.

Reverting to another Type Permission object requires Secondary Authorization.

The following object types are not compliant with Secondary Authorization within the System Configuration user interface.

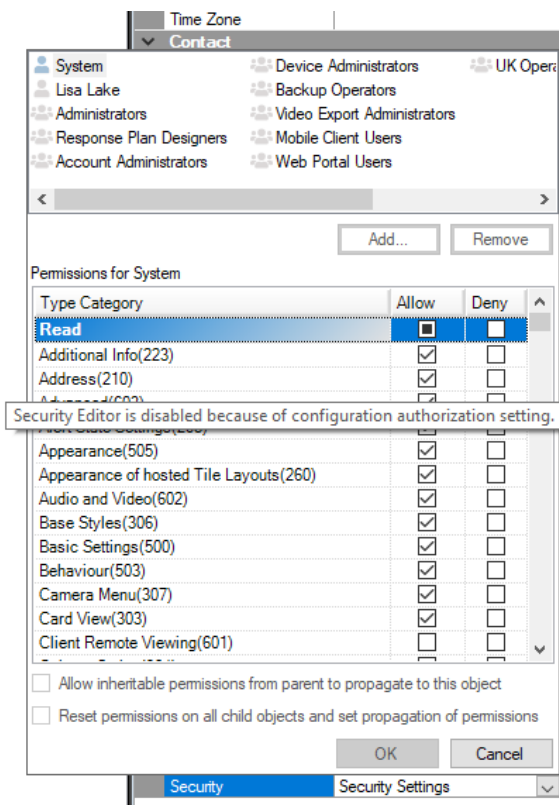
- Asset Group
- Dashboard
- Data Connection
- Date/time Schedule
- Display Areas
- Enterprise settings
- GUI
- Hot key mappings
- Icon Set
- Location Reference
- Modern Client Theme
- Object Style Template
- Remote Federation Service
- Response plans
- Sequence
- Shortcut
- Tile Layout
- Timer
- Tooltip Template
- Trigger
- Type Permissions
- Connectors & Extensions
- Icon Manager
- GIS Layer Manager
- Object Designer
- Device Manager
- License Manager
- Plan Manager
- Operator Actions

System Functionality Disablement

While Configuration Authorization is enabled, a number of functions are locked down to prevent users from making changes that are not compliant with Secondary Authorization, but risks compromise the integrity of the system when in production.

Object Security

On enabling Config Authorization, changing Security settings of all objects is disabled.

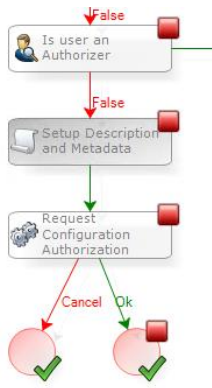


Secondary Authorization within Response Plans

Control Center supports the configuration of end-user functions that are not built-in and natively covered by Secondary Authorization. For instance, a user interface can be created that allows users to change the current Threat Level. You can implement Secondary Authorization in any configured end-user functionality by using the Request Configuration shape in Response plans.

A typical authorization sequence would be configured as follows, using Changing Threat Level as an example.

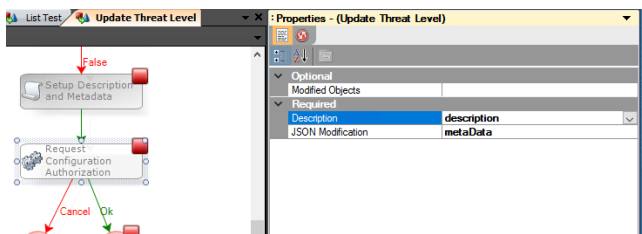
1. From the GUI, a link shape is used to run the Update Threat Level response plan.
2. In the Response Plan, data about the request is stored in a text variable using JSON



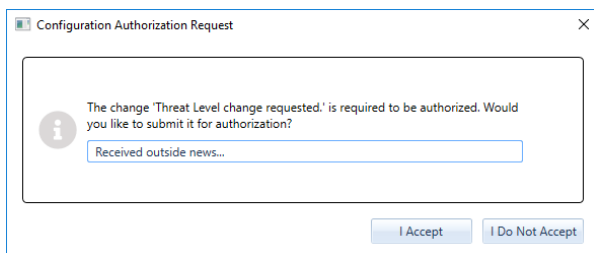
```

My.PageVariables.description = "Threat Level change requested."
My.PageVariables.metadata = My.PageVariables.metadata.SetJsonValueByKey("concurrencyAction", "threatlevel")
My.PageVariables.metadata = My.PageVariables.metadata.SetJsonValueByKey("action", My.PageVariables.Action)
My.PageVariables.metadata = My.PageVariables.metadata.SetJsonValueByKey("key", My.PageVariables.Key)
  
```

3. The shape is executed, passing in a description to show the user, and the metadata containing information about the change request.



4. The user is prompted to complete the request. User fills in a comment and clicks 'I Accept'.



5. The Response Plan will complete down the OK route from the shape. At the same time, Approvers receive the new request which is visible in the Authorization Grid.

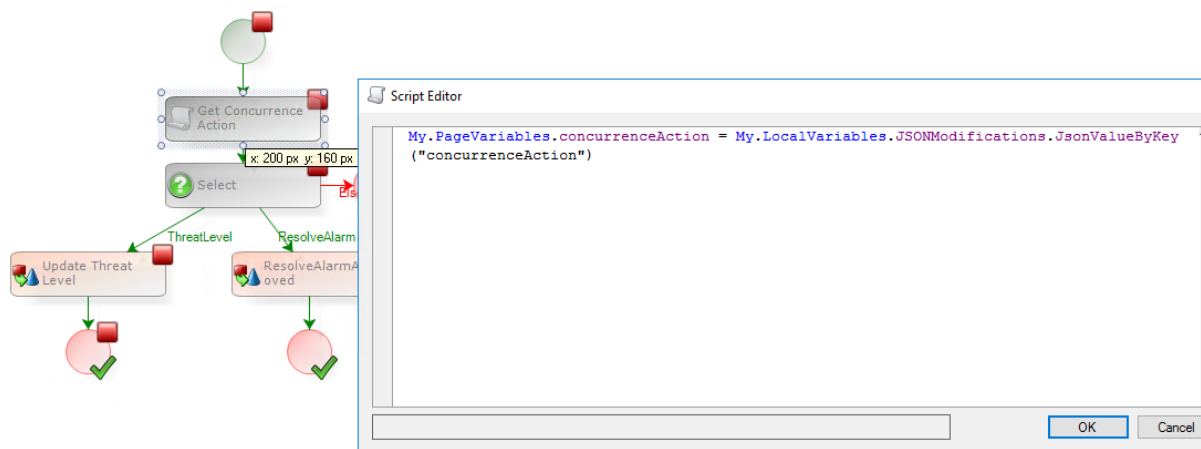
Status	Description	Requested User	Requested Date	Requested Client
Pending	Threat Level change requested.	Lisa Lake	1/18/2023 2:06:23 PM	WIN-4SABEFUB03U

- The Approver approves the request. A new event is raised from the Server object. This is linked to a Response Plan that handles all request approvals.

Server

- WIN-4SABEFUB03U Server Computer with the IP hostname of Demo-Brix-... Server
- Events
 - Application Exited Event raised when an Application executed on the Se...
 - Custom Configuration Approved** Event raised when a custom configuration is approved.

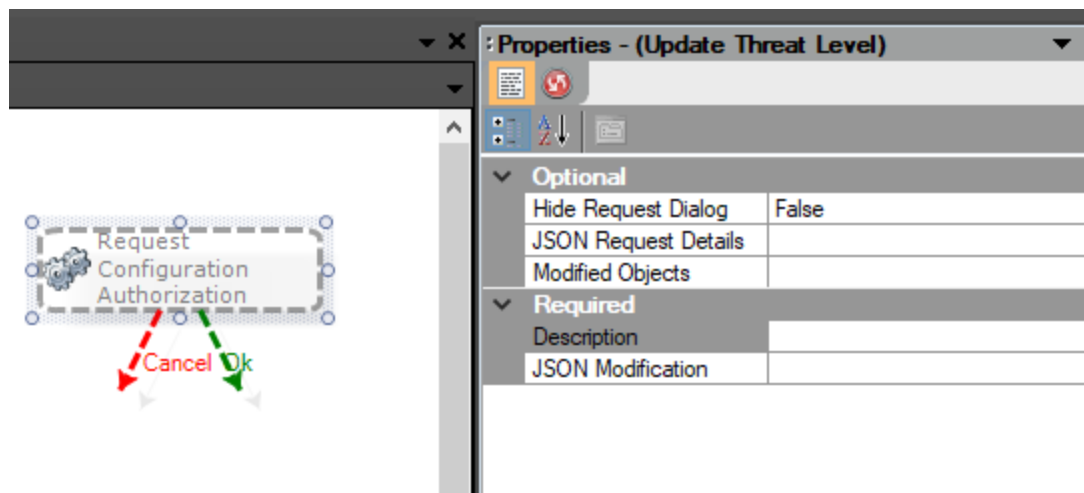
Custom Configuration Approved [Master Page]



- The JSON metadata is used to determine the type of request and which action to take next.
- The Update Threat Level response plan is run using the parameters from the request, and the threat level is updated.

Request Configuration Authorization

The Request Configuration Authorization shape is used to prompt the current user to request authorization.



The shape displays the request dialog and if the user submits a request, will go down the OK route. If the user cancels the request, it will go down the Cancel route.

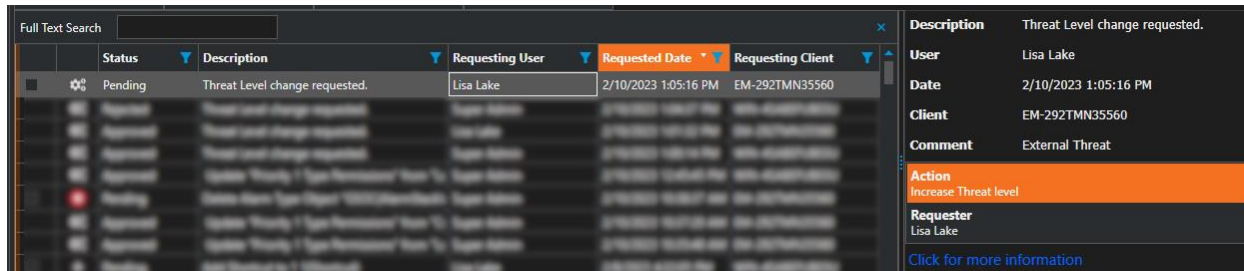
When a user submits a request, the request will appear in the Authorization Request grid for approvers to approve.

Property	Description
Hide Request Dialog	If True, Submits the request without prompting the user for a Check-in comment. The comment in the request will be blank.
JSON Request Details	Additional detail to be shown in the Request detail panel. Submitted as key-value pair where the Key will be shown as the title and the Value the description.
Modified Objects	List of Modified objects to be passed to the Approve, Reject and More Info events.
Description	Description shown to user in the Check-In dialog and in the Description section of the approval request grid.
JSON Modification	JSON describing changes, included in the Approve, Reject and More Info events and used when configuring the resulting Response Plans.

The shape must be used in a Response Plan initiated by a user, e.g., by linking to it from a GUI. If the shape runs in a Response Plan executed by System – there is no user that can submit the request.

Providing Additional Request Details and More Information

Custom Configuration requests can be supplied with additional request details to explain the content of the request to the approver.



Prepare the additional detail by creating a JSON string with a key-value pair for every additional detail. In this example, the Action and Requester are added.

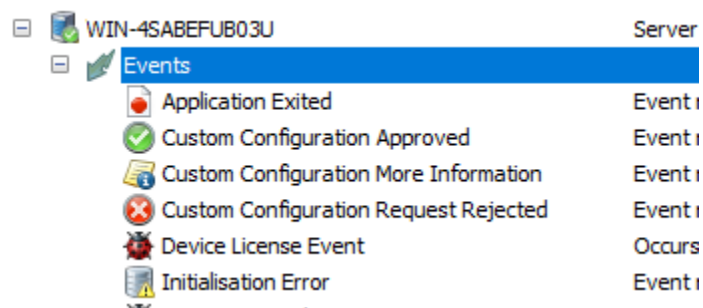
```
My.PageVariables.requestDetails = My.PageVariables.requestDetails.SetJsonValueByKey("Action", "Increase Threat level")
My.PageVariables.requestDetails = My.PageVariables.requestDetails.SetJsonValueByKey("Requester", My.PageVariables.requestingUser.Label)
```

Additional details are shown in the request detail panel to the right of the Secondary Authorization grid.

A link for more information is shown below the additional information screen. When the link is clicked, the Custom Configuration More Information Event is raised by the Server object.

Approved, More Information and Rejected Events

When a request is approved or rejected, or a user clicks on More Information, a matching event is raised by the Server object.



This is used to configure, for instance, the display of more information to the user about the request.

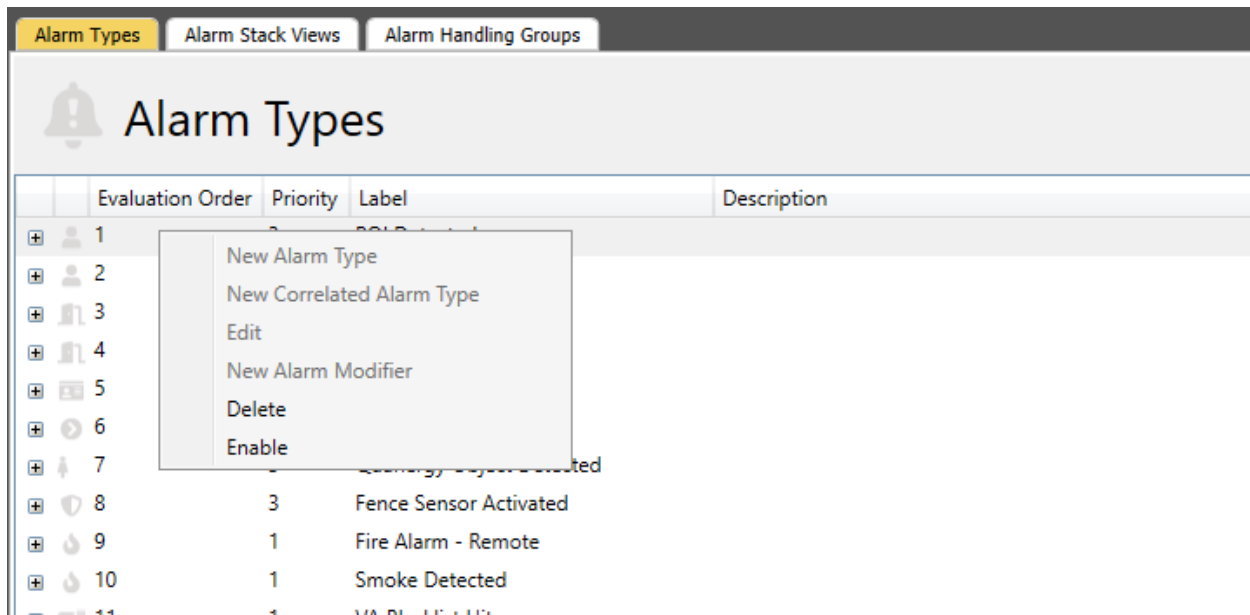
The More Information link is always shown for Custom Configuration requests, so it is recommended to always respond to the click event.

Secondary Authorization for Alarm Types

Most Alarm Type features are locked down when Secondary Authorization is enabled but some are available for administration purposes. The following Alarm Type changes are available and comply with Secondary Authorization when enabled:

- Enable / Disable Alarm Type
- Enable / Disable Correlated Alarm Type
- Delete Alarm Type
- Enable/Disable Alarm Type Modifier
- Delete Alarm Type Modifier
- Delete Alarm Stack View
- Edit Default Service Levels

While Secondary Authorization is enabled, all other modifications to Alarm Types are locked down.



Changes to SLA requires clients to re-login before they apply.

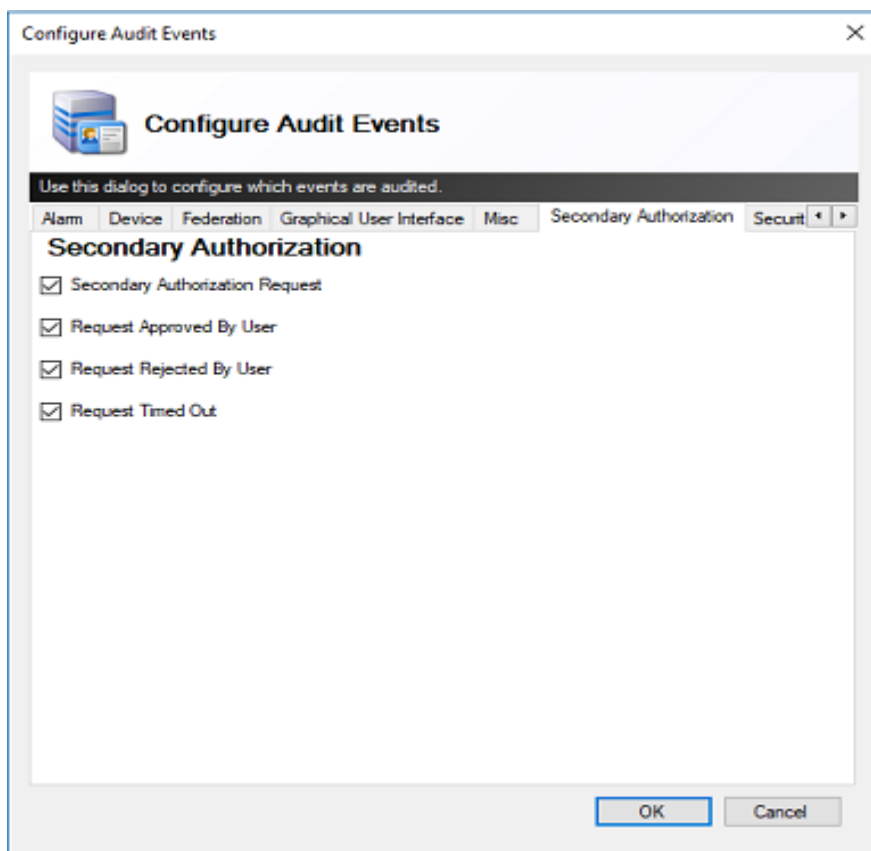
If an alarm is created for an alarm type that has been requested to be deleted, it will not be deleted once a approved since there is now a reference to an alarm.

Moving an alarm stack view to another Alarm Stack View group does not require Secondary Authorization.

When an Alarm Stack View Deletion is approved, users have to re-open the Alarm Type Object to see the update.

Audit Events from Secondary Authorization

The events that you want to be audited can be configured in the **Audit Events** dialog. The available events to choose from are as shown in the figure below.

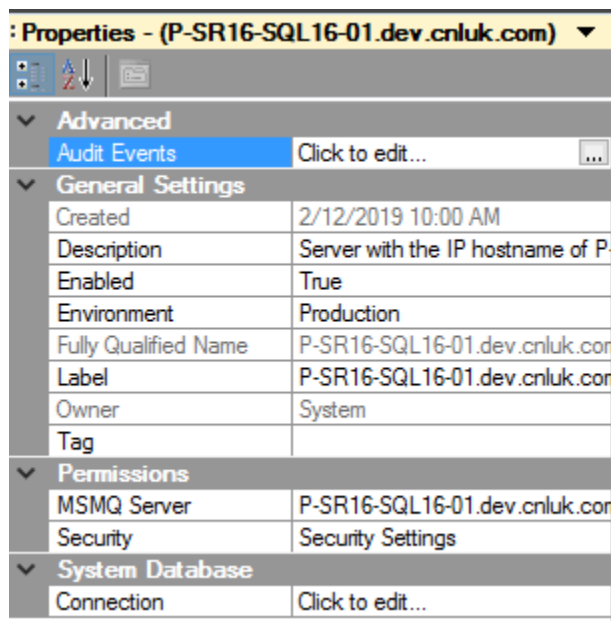


Option	Description
Secondary Authorization Request	If enabled, lists when the secondary authorization is created.

Request Approved By User	If enabled, lists all requests, approved by the user along with the username who authorized it and the workstation name.
Request Rejected By User	If enabled, lists all requests, rejected by the user along with the username who rejected it and the workstation name.
Request Timed Out	If enabled, lists all requests, rejected due to the request being timed out for authorization. In this scenario, the username is listed as System and the Event type as TimedOut in the audit report generated from the database.

To get to the **Audit Events** dialog, you need to:

1. Go to **System Configuration > My Organization > Computers**.
2. Select **Audit Server**.
3. In the **Properties** window in the right pane, select **Audit Events**. The **Configure Audit Events** window displays.



4. Select **Secondary Authorization** tab.
5. Enable the events you would like to audit. By default, all the options are enabled.
6. Select **OK**.

Location Based Configuration Authorization

when the Enable Location Based Configuration Authorization property is enabled in the Global Settings. the authorizer was able to approve/reject the request, only if they are not present in the same location as the requester. The popup notification will only be displayed on the client of the authorizer sitting remotely to the requester. If this property is not enabled, then the authorizer can Approve and Reject regardless of the location.

However, the authorizer on the same location can still go to the configuration authorization window and reject the request. He will not have the rights to approve though, unless seated remotely to the requester. An error message will be displayed, and the user will be restricted to approve the request if placed in the same location.

The screenshot shows the 'Configuration Authorisation' window with a table of requests and an error dialog box overlaid.

Description	Requested User	Requested Date	Requested Client	Status
Add user089	Limiteduser2	6/21/2019 5:07:50 AM	SR16-SQL16-07.dev.cnluk.c	Pending
Add user50	Limiteduser2	6/21/2019 4:04:03 AM	SR16-SQL16-07.dev.cnluk.c	Approved
Add user001	Limiteduser2	6/21/2019 4:03:35 AM	SR16-SQL16-07.dev.cnluk.c	Approved
Add user50	Limiteduser2	6/21/2019 4:01:04 AM	SR16-SQL16-07.dev.cnluk.c	Rejected
Add user15	Limiteduser2	6/21/2019 3:56:40 AM	SR16-SQL16-07.dev.cnluk.c	Approved
		1/2019 3:54:58 AM	SR16-SQL16-07.dev.cnluk.c	Rejected
		1/2019 3:50:47 AM	SR16-SQL16-07.dev.cnluk.c	Approved
		1/2019 3:44:56 AM	SR16-SQL16-07.dev.cnluk.c	Rejected
		1/2019 3:16:27 AM	Win10-07.dev.cnluk.com	Rejected
		1/2019 3:15:42 AM	Win10-07.dev.cnluk.com	Rejected
		1/2019 3:14:46 AM	Win10-07.dev.cnluk.com	Rejected
		1/2019 3:11:54 AM	SR16-SQL16-07.dev.cnluk.c	Rejected
Add user11	Limiteduser2	6/21/2019 3:11:40 AM	SR16-SQL16-07.dev.cnluk.c	Approved
Open System Configuration SR16-SQL16-07.d	Limiteduser2	6/21/2019 3:04:04 AM	SR16-SQL16-07.dev.cnluk.c	Rejected

Error Dialog Box:

Failed to approve 1 request because the requesting client of the change request and approving client are in the same folder

OK

Request Details:

- Description: Add user10
- User: Limiteduser1
- Date: 6/21/2019 2:55:13 AM
- Client: Win10-07.dev.cnluk.com
- Comment: sss

Threat Level



In Control Center, threat levels are supported by alarm types and can be visually represented using a GUI control. The threat level is simply a numerical value which runs from 1 to 5. The threat level GUI control, as shown in the figure, shows how titles and descriptions can be associated with each level to provide more context visually.

A typical example is where the threat level is set based on the types of alarms in the system which could then in turn determine how other alarms are created and handled. The following sections detail how to determine the threat level, control system behavior based on the threat level and how to show the threat level control.

The threat level can also be used externally to Control Center using system events and response plan shapes. For example, the access mode of an access control system could be changed from Card Only to Card and Pin when the threat level reaches a certain level.

Setting the Threat Level

The threat level in Control Center is simply a whole number between 1 and 5, with 1 being the default and 5 being the maximum. The mechanism to set the threat level uses a stack model whereby, threats are entered in the stack by alarm types (when an alarm is created) or by a response plan shape. The threat level in the system will then be based on the highest threat in the stack. The threat level is then updated accordingly as threats

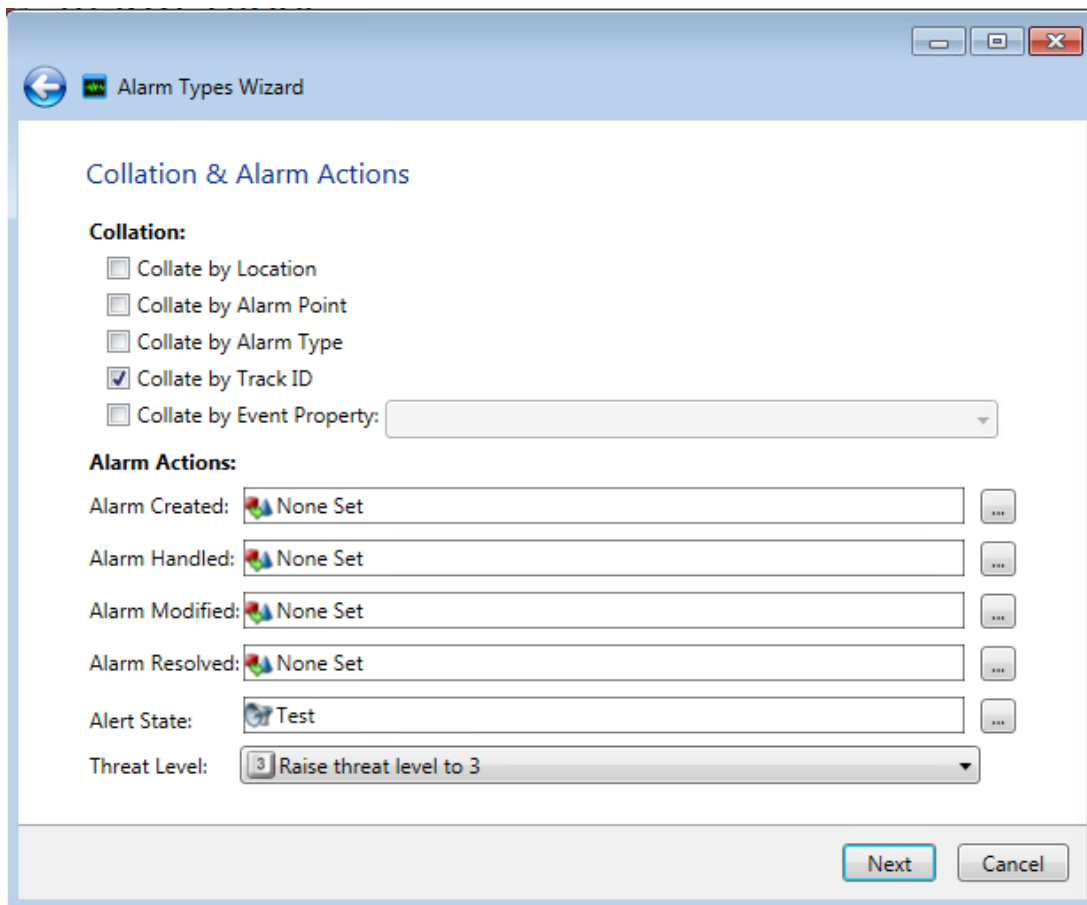
are removed from the stack (either when an alarm is resolved, or a manual threat is removed using a response plan).

Each threat registered on the stack must have a corresponding key. In the case of alarms then each threat is keyed by the alarm ID which is managed automatically. In the case of manual threats, then a key must be specified when adding and removing threats.

Using Alarm Types in Threat Levels

The system threat level can be determined based on unresolved alarms in the system. The Alarm Types wizard includes an option on the Collation and Alarm Actions page to set the threat level when an alarm of that type is created.

The threat specified will determine the minimum threat applied. If an alarm exists which specifies a higher threat level, then the higher value will be used.



The options available for the threat level are:

- No change
- Raise threat level to 2
- Raise threat level to 3

- Raise threat level to 4
- Raise threat level to 5

There is no option to raise to level 1 as this is the minimum and default level.

Manually Setting Threat Levels

In addition to alarms controlling the threat level, manual entries can also be created using response plan shapes. This provides additional control over the threat level from other parts of the solution. For example, a button can be provided on the main menu to register a manual threat. Note that the threat specified will determine the minimum threat level. If alarms or other manual threats exist with a higher threat level, then no change will occur.

In the screenshot below, a response plan has been created to add a threat level of 4. Note that the threat key of FromUser has been specified which must be equally specified when removing the threat.

The screenshot displays the 'Set Threat to High' response plan shape in the Everbridge Control Center. The main canvas shows a flowchart with a green circle at the top, an 'Add Threat (FromUser : 4)' shape in the middle, and two red circles at the bottom labeled 'Fail' and 'Success'. A red arrow points from the 'Add Threat' shape to the 'Properties' panel on the right. The 'Properties' panel shows the following configuration:

Optional	
Error String	err
Required	
Threat Key	FromUser
Threat Level	4

Threat Level Example

A sample solution has been configured with the following alarm types:

- Door Held Open – Threat level setting equals No change
- Fire Alarm – Threat level setting equals Raise threat level to 4
- Perimeter Breach – Threat level setting equals Raise threat level to 3

The solution also has the following buttons on the main menu

- Raise Threat to High – Runs a response plan using the Add Threat shape passing in the values of
 - Threat Key = MainMenu
 - Threat Level = 4
- Revert Threat Level – Runs a response plan using the Remove Threat shape passing in the values of Threat Key = MainMenu

The following table lists example activities using the alarm types and menu buttons detailed above. The left column shows the activity, the center column represents all threats registered in the solution, and the last column shows the current threat level which is the highest of all threats.

Activity	Threat Stack (ID, Threat)	Threat Level
Start	[empty]	1
Perimeter Breach alarm created (ID = 1)	1, 3	3
Door Held Open alarm created (ID = 2)	1, 3	3
Perimeter Breach alarm created (ID = 3)	1, 3 3, 3	3
Fire Alarm created (ID = 4)	1, 3 3, 3 4, 4	4
Alarm 3 resolved	1, 3 4, 4	4
Main menu button Raise Threat to High clicked	1, 3 4, 4 MainMenu, 4	4
Alarm 4 resolved	1, 3 MainMenu, 4	4
Alarm 1 resolved	MainMenu, 4	4

Main menu button Revert Threat Level clicked	[empty]	1
Alarm 2 resolved	[empty]	1
Perimeter Breach alarm created (ID = 5)	5, 3	3
Alarm 5 resolved	[empty]	1

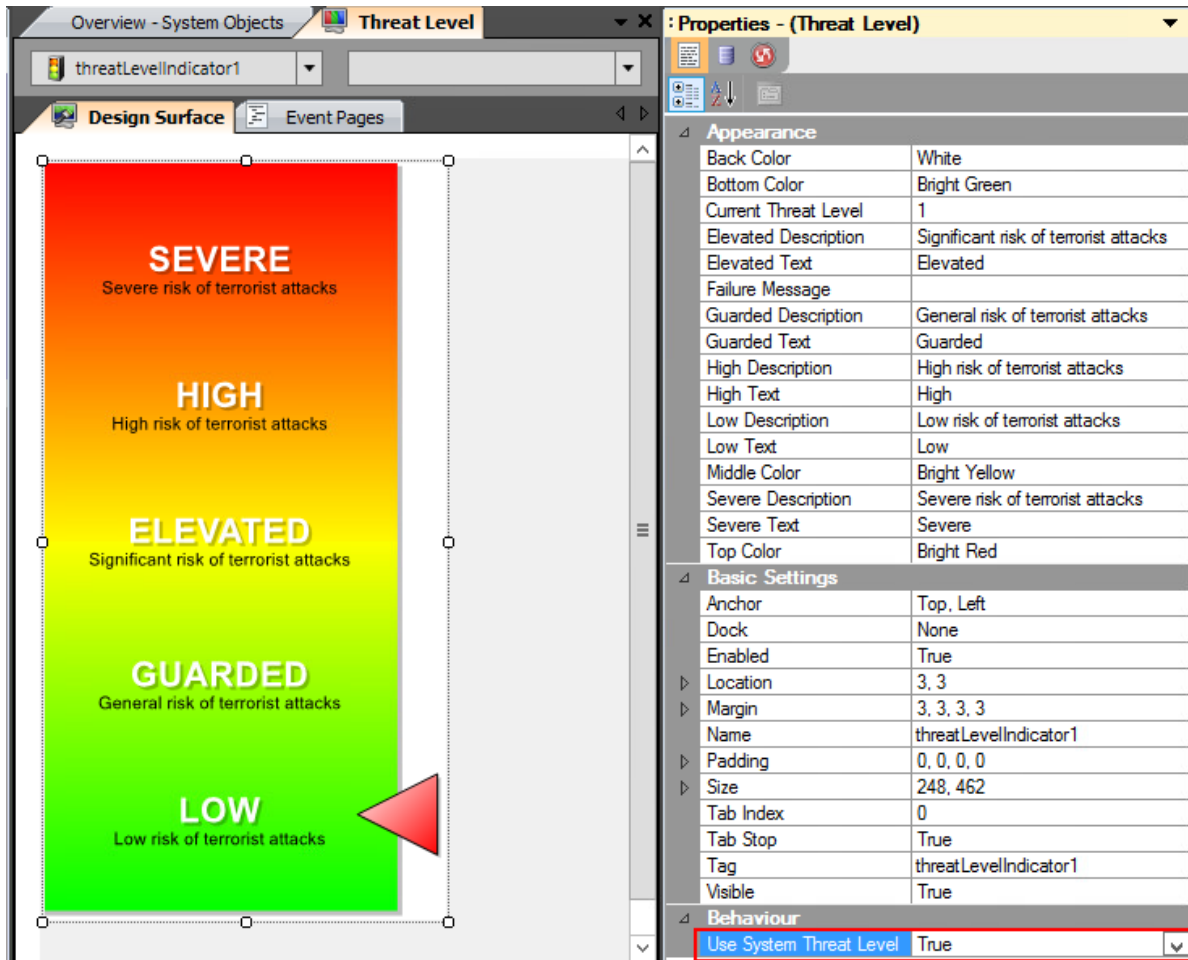
Using the Threat Level

The threat can be used in various parts of a solution as it changes. This includes:

- A GUI control to visually show the threat
- Options in alarm types to determine the creation of alarms
- An event on the alarm types service
- Response plan shapes

Threat Levels With a GUI

The quickest and easiest way to visualize the threat level is using the Threat Level Indicator GUI control. The threat level indicator includes a property called Use System Threat Level which when set to True will automatically update to show the current threat level. Simply create a GUI with the Threat Level Indicator control, set Use System Treat Level to True, save the GUI and then display. The GUI will then automatically update as the threat level changes.



Threat Levels With Alarm Types

The evaluation of an alarm type can also include a check of the current threat level. The Evaluation page of the Alarm Types wizard includes an option to filter alarm creation based on a specified condition. These include:

- **Any**-The alarm will be created at any threat level.
- **Equals**- The current threat level must equal the specified value (1 – 5) for the alarm to be created.
 - **Higher than** - The current threat level must be over the specified value to create the alarm.
 - **Less than** - The current threat level must be below the specified value to create the alarm.

In the figure below, an alarm type has been configured to only create alarms if the threat level is higher than 3 (only when the current threat level is 4 or 5).

Physical State:

Threat Level:

Threat Level Changed Event

When using the threat level outside of Control Center, an event on the Alarm Types Service can be used to detect changes to the threat level and perform actions on external systems as in the example below.

Alarm Types Service

[-] Alarm Types Service	Alarm Types Service
[-] Events	
Forced Park	Raised when an alarm is forcibly parked by a correlat...
Forced Resolve	Raised when an alarm is forcibly resolved by a correl...
Service State Changed	Raised when the online state of the service changes
Threat Level Changed	The Threat Level of the system has changed.
[+] Shortcuts	Shortcuts targeted against this object

The event will then provide values based on the old and new threat level which can be configured to populate response plan variables.

Local	
Date_Time Date/Time	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Optional
Event Service Event Id Text	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Optional
Folder Folder	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Optional
Location Location	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Optional
NewThreatLevel Whole Number	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Optional
OldThreatLevel Whole Number	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Optional
Sender Alarm Types Service	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Optional

Local		
	Date_Time Date/Time	Optional
	Event Service Event Id Text	Optional
	Folder Folder	Optional
	Location Location	Optional
	NewThreatLevel Whole Number	Optional
	OldThreatLevel Whole Number	Optional
	Sender Alarm Types Service	Optional

Get Threat Level Shape

The response plan shapes palette includes a shape to get the current threat level. This can be used to populate a whole number variable to get the current threat level. This can be useful when used in conjunction with the Threat Level Changed event. For example, this shape can be used to get the initial value when starting up a solution and the event can be used for ongoing changes.

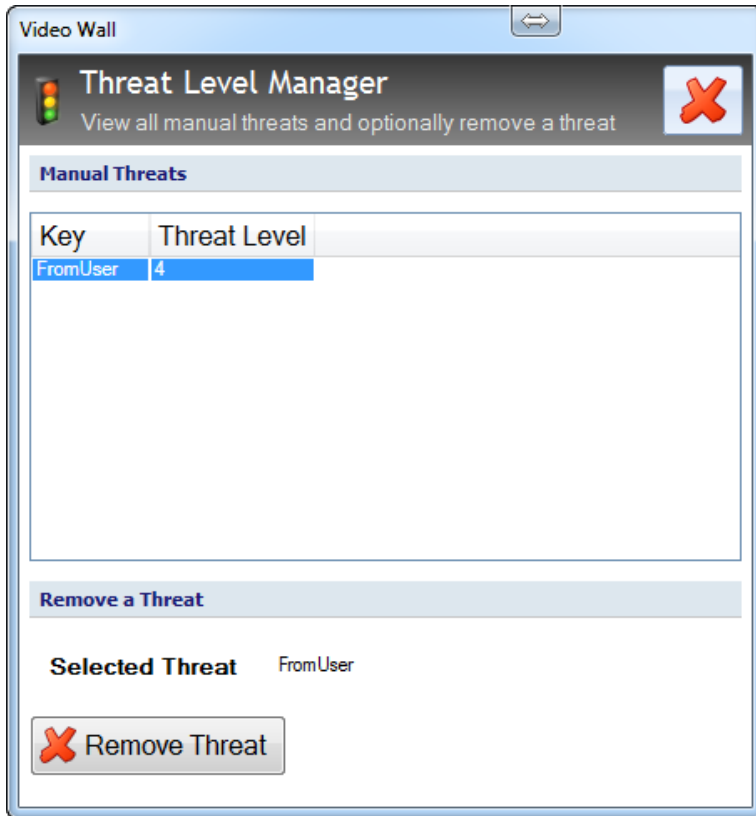


Manual Threats

A GUI control called Threat Level Grid is available to view all manual threats in the system. This shows all manual threats in the system which have been added using the Add Threat shape.

The grid will not show any threats for alarms.

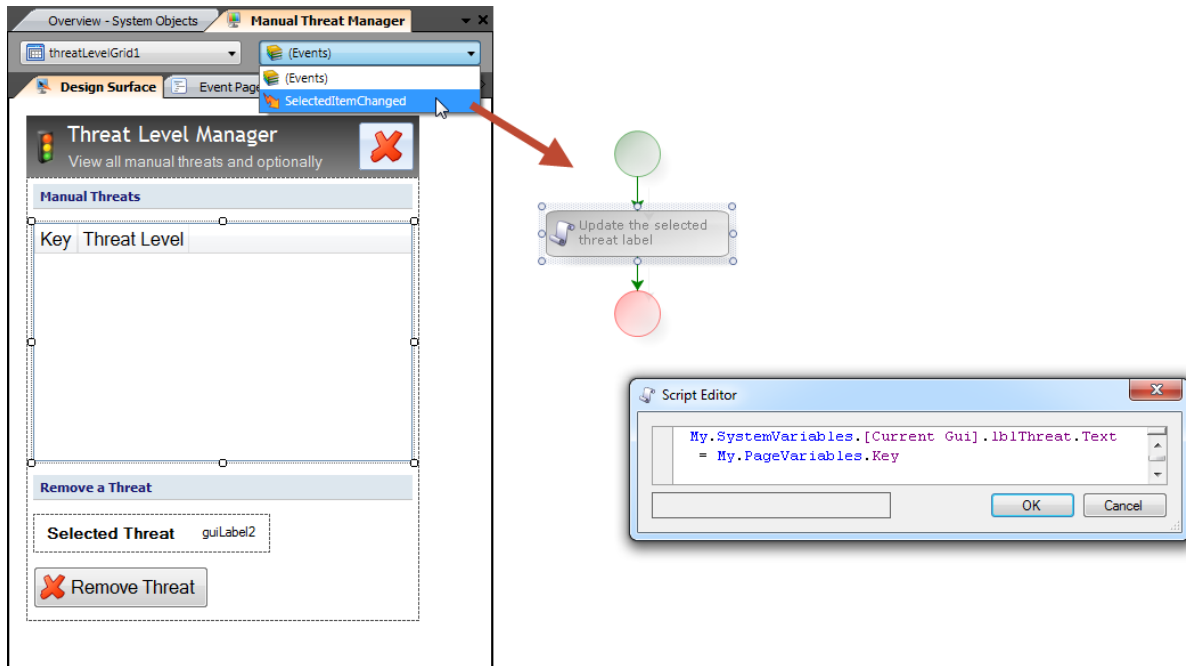
The following screenshot shows how the grid has been used within a GUI to show manual threats and provide the user with the option to remove a threat.



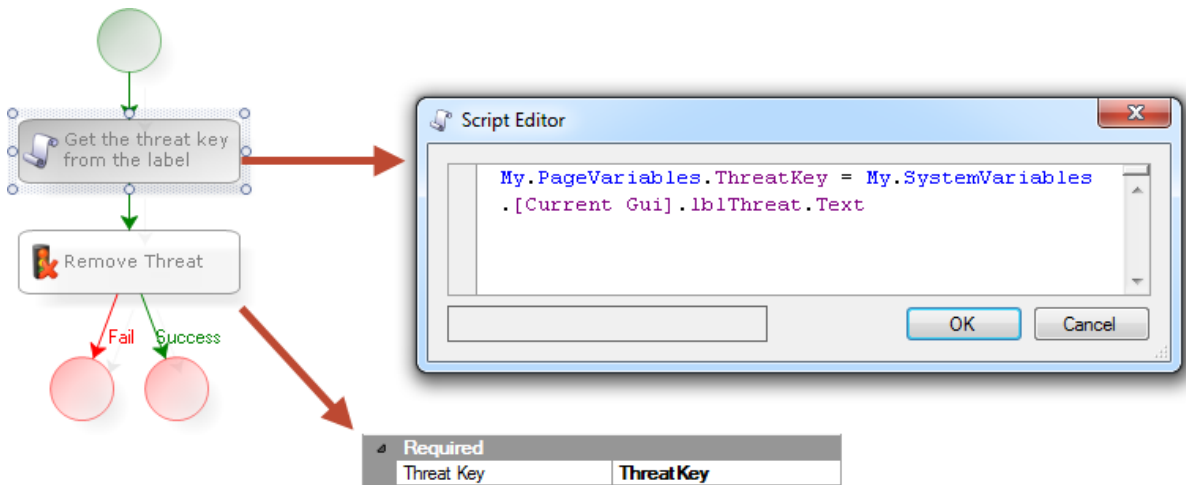
When the user selects an entry in the grid, the GUI will update the selected threat label with the selected key. The user can then click the Remove Threat button to remove the threat.

Manual Threats and GUI Logic

The logic for the GUI includes an event page on the grid SelectedItemChanged event which populates the label.



The button clicked event is also configured to get the selected threat key from the GUI label and then uses the Remove Threat shape to remove the threat.



Modify Alarm Shape

The modify alarm shape allows for the threat level of an existing alarm to be modified. Simply use the shape for an alarm specifying a threat level from 1 to 5. If the alarm previously specified a threat, then it will be updated to reflect the new value. If no threat previously existed for the alarm, then a new threat will be registered on the threat stack. Specifying a new threat level for an alarm will only update that instance of the alarm. Existing alarms for the same type and any new alarms for the corresponding type will not be affected.

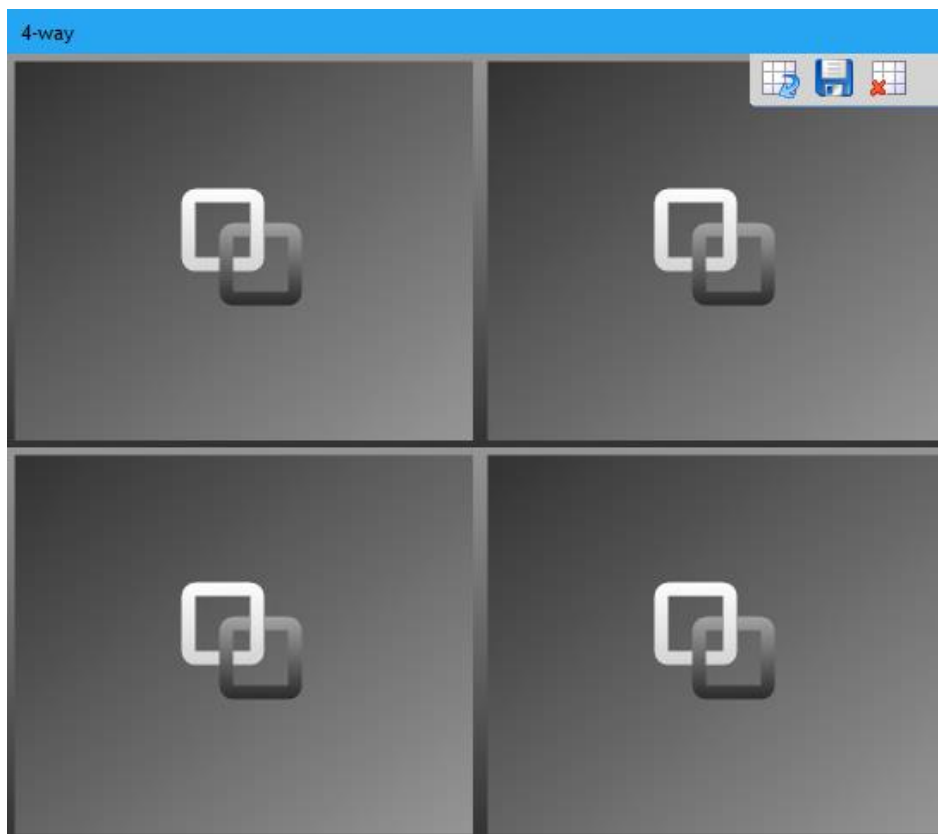
Tile Layouts

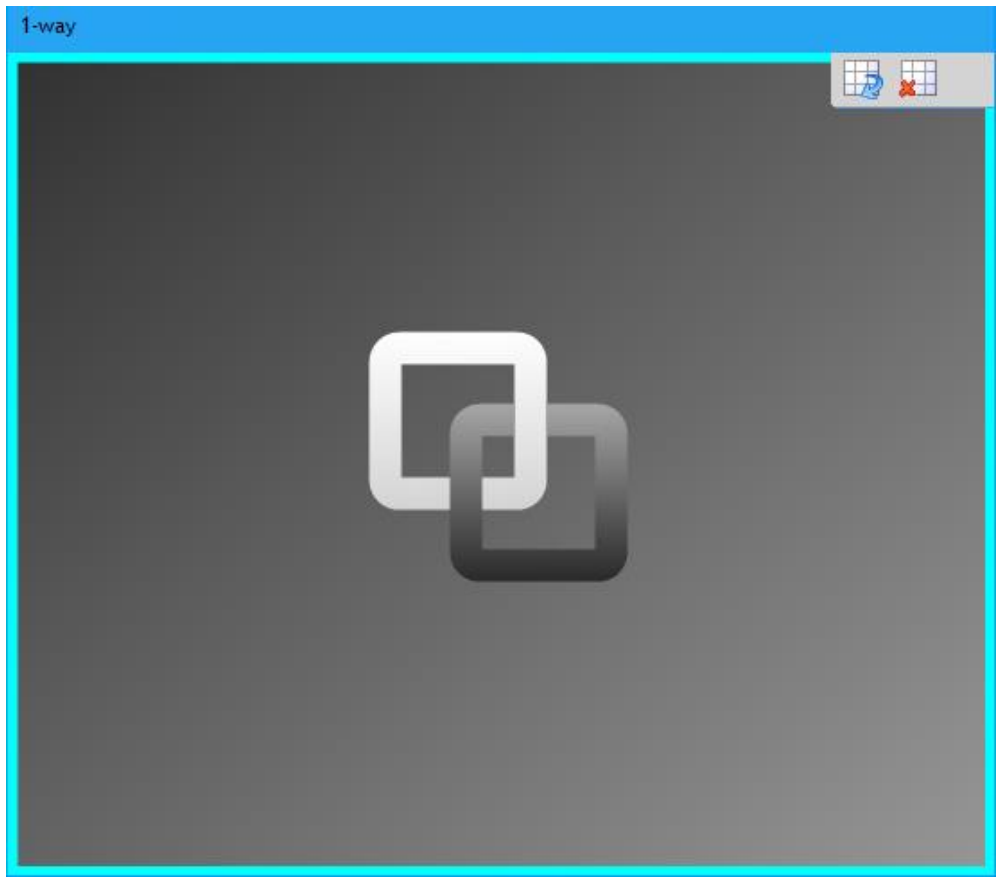
Control Center provides a Tile Layout feature, where a camera view for a customized layout can be saved in the system and expose this to the end-user so that operators can create, view, and modify their own layouts.

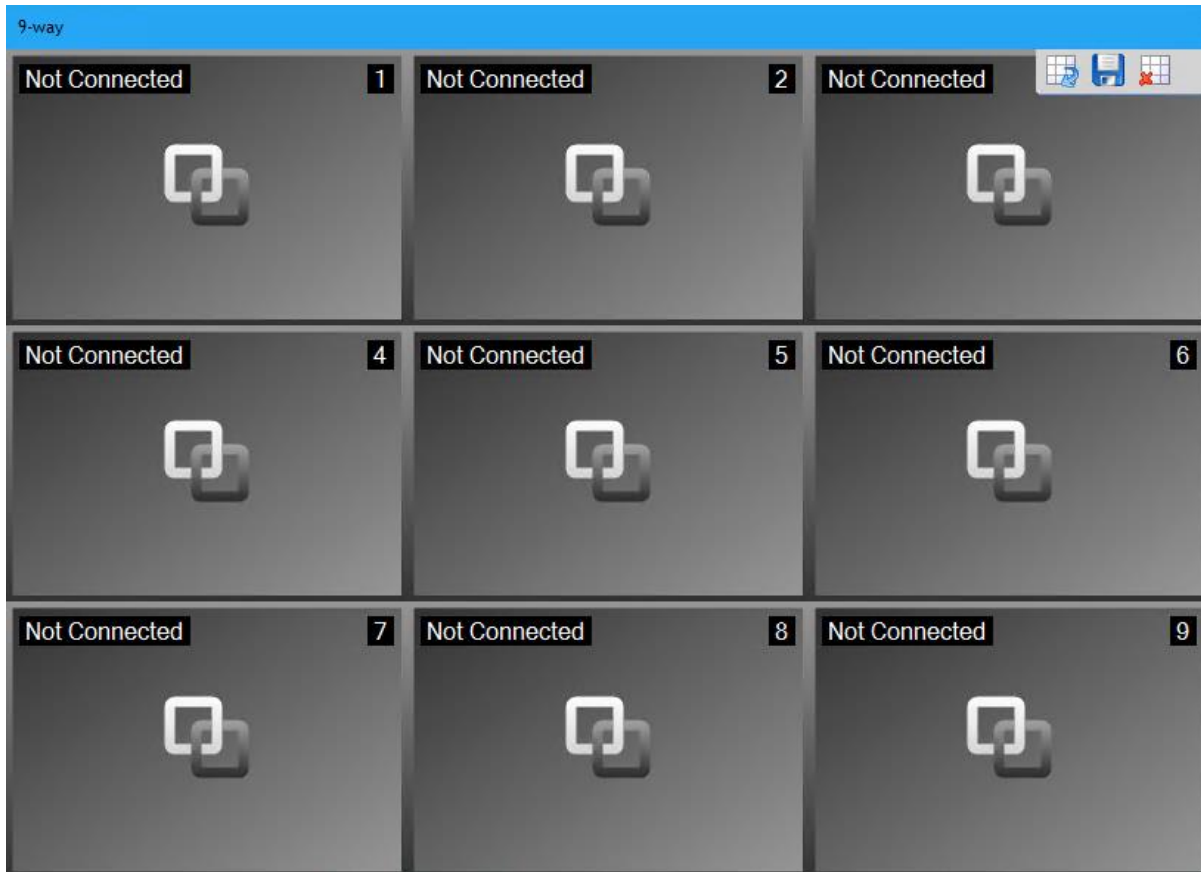
Tile Layouts can be either saved as available for all users or only for the creator of the layout. This introduces the concept of user folders where content can be saved in the system within hidden folders for each user. Functionality added in the future can utilize the same model to further extend content structuring.

A tile is a user interface element in Control Center for displaying content to a user. The content can be output from a device, a commissioned GUI or a Sequence. A Tile Layout is a grid of tiles that can be laid out in multiple ways. The Tile Layouts feature allows the user to create and maintain a unique set of Tile Layouts.

Example Tile Layouts





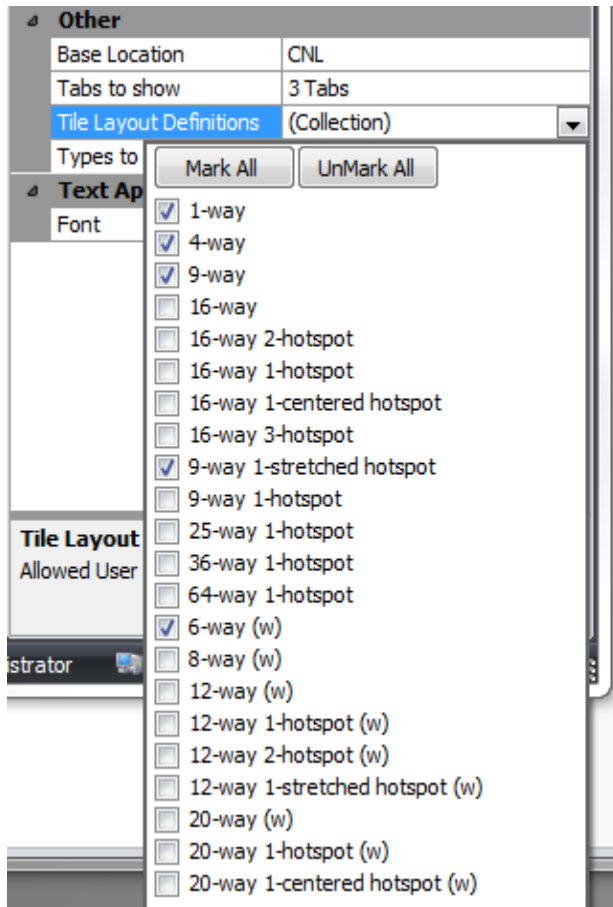


Allow Users to Create Tile Layouts

Defining which system Tile Layouts are available in the Tile Layouts tab determines what Tile Layouts are available to users.

First configure the Tile Layout definitions to enable users to create their own Tile Layouts using the Tile Layout Definitions drop-down.

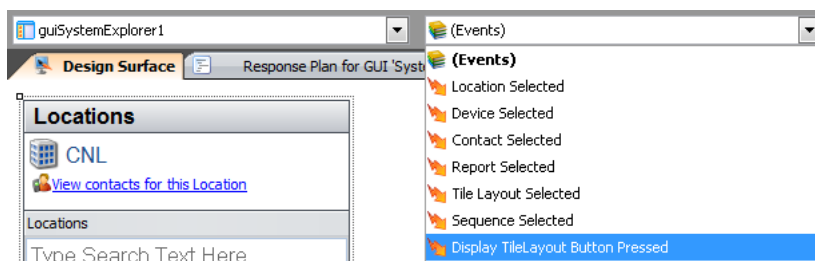
The list of Tile Layout definitions appears displaying all the definitions configured in Control Center. Definitions selected here are made available to the end user to create their own Tile Layouts.



Display Tiles on Video Wall

The toolbar in the System Explorer Tile Layouts tab includes a button to display the selected tile layout to another machine. To use this functionality, configure the **Display TileLayout Button Pressed** event on the System Explorer GUI to show the selected tile layout to the target machine.

1. Edit the System Explorer GUI and select the **Display TileLayout Button Pressed** event on the System Explorer Control. This will create a new event page with an event specific variable for the selected tile Layout.



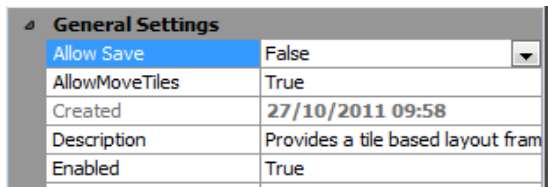
2. Add any required logic into the event page to display the tile layout.

3. Make any changes and click **Save**. Changes are automatically updated in System Explorer Control.

Configure Layouts to be Saved by a User

Using the **Allow Save** property in tile layouts, you can save global or personal tile layouts, if permitted.

In the **System Configuration Overview** tab > **System Explorer**, select a tile layout.



General Settings	
Allow Save	False
AllowMoveTiles	True
Created	27/10/2011 09:58
Description	Provides a tile based layout fram
Enabled	True

In System Explorer, the default setting for existing and new layouts is set to **False**. When the layout is set to **False**, the **Save** icon does not appear in the tile layout as it is display-only and cannot be saved.

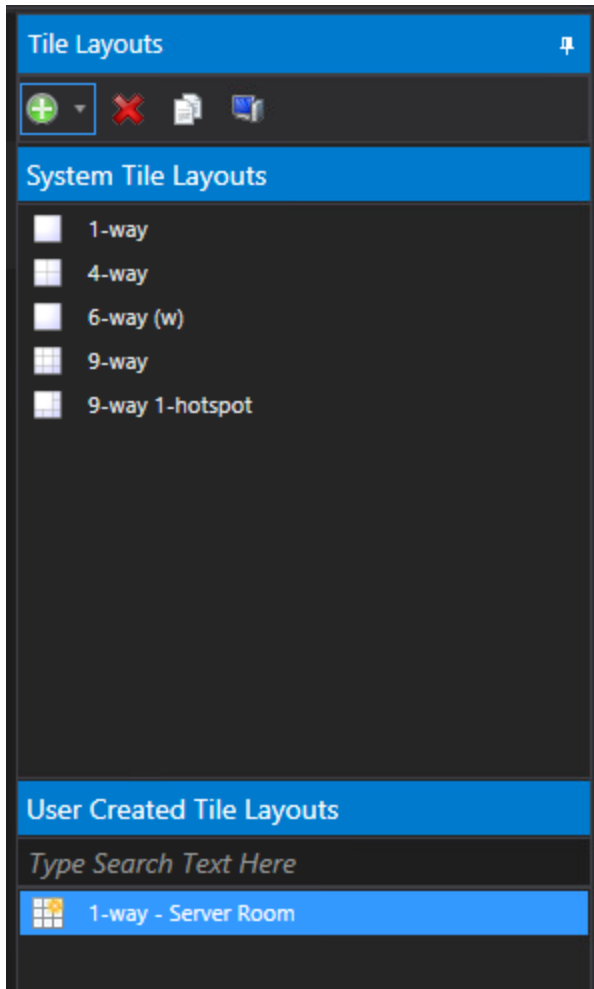
If this parameter is set to **True**, the **Save** icon is available to users when the tile layout is displayed.

By default, in layouts created by end users, this property is set to **True**.

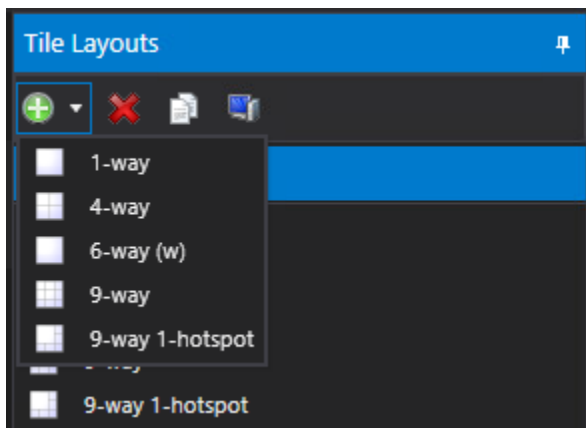
Creating a Tile Layout

To create a new Tile Layout:

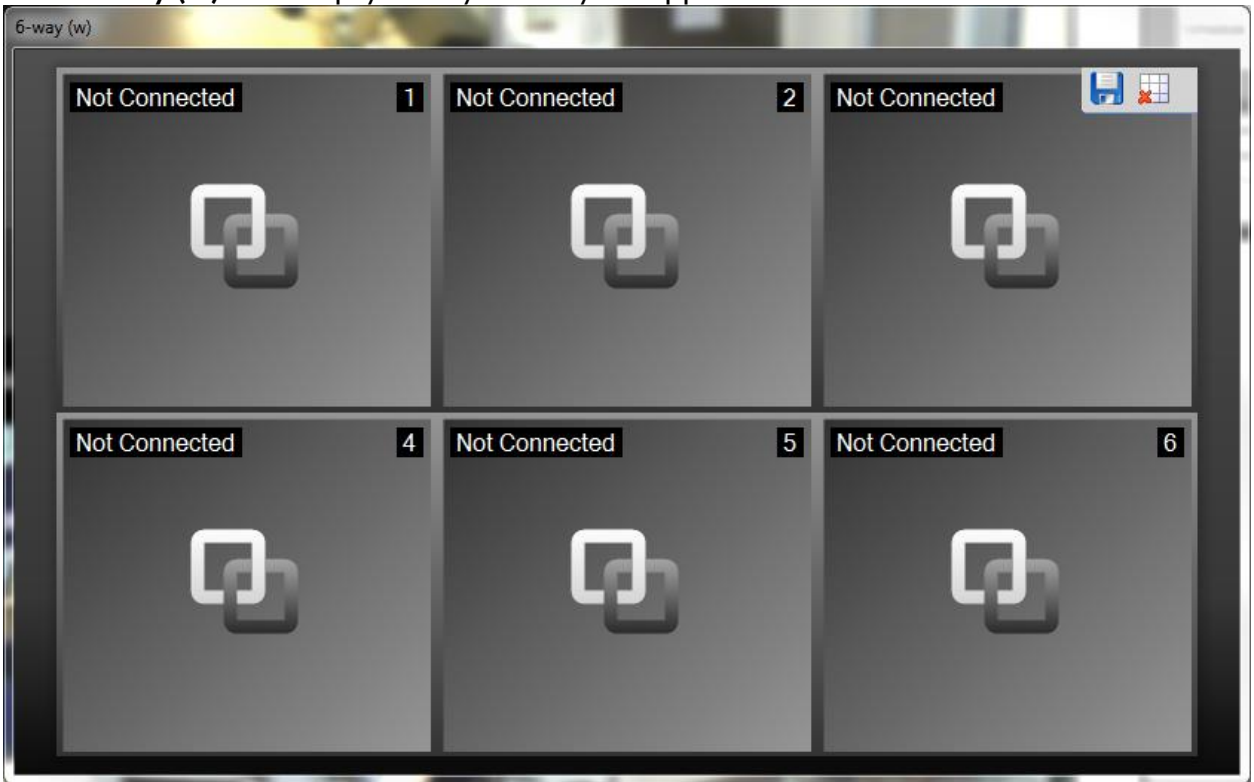
1. In **System Explorer** > **Tile Layouts** tab, click the green **Plus** button.



2. The available layouts drop-down appears. Clicking any one of these opens a new window displaying the tile layout.
3. The available layout definitions are determined by the selection made in System Explorer, see [Allow Users to Create Tile Layouts](#).

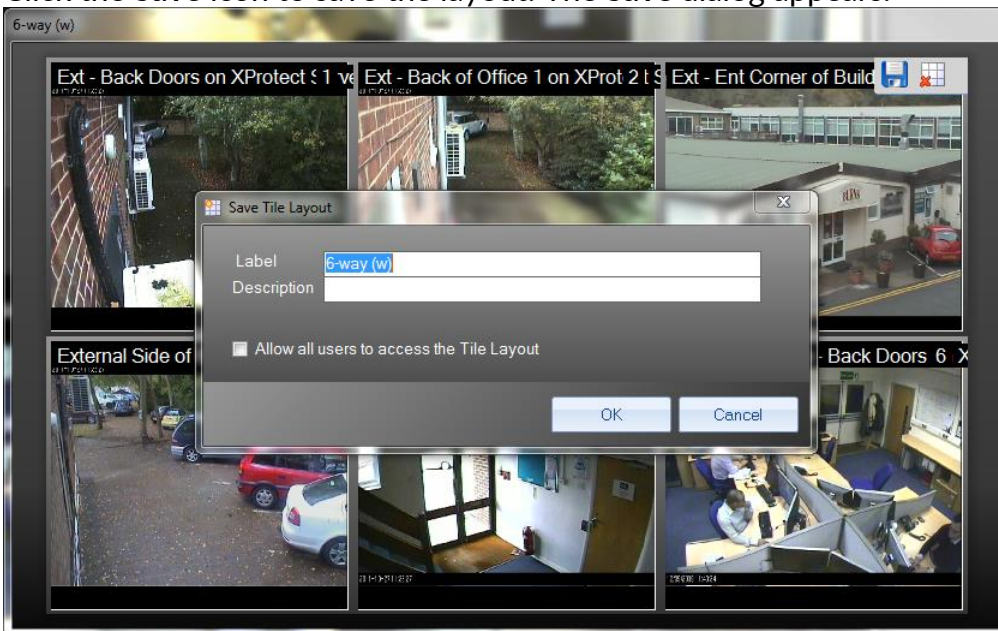


- Click **6-way (w)**. An empty 6-way Tile Layout appears.



- Now drag on the cameras, sequences and GUIs to display into the tiles. To remove content, select it and click **Close**.

- Click the **Save** icon to save the layout. The **Save** dialog appears.



7. Enter the **Label** and **Description** to identify the layout and click **OK**. A tile layout is only accessible to the user who saved it, by default. The **Allow all users to access the Tile Layout** checkbox allows the layout to be saved for global use.
8. To save a tile layout for global use, provide a Location to save the tile layout. This makes the layout available to everyone.

You can also create a layout by dragging out one of the available definitions onto an appropriate display area.

Display a Tile Layout

When the tile layout is saved, it appears in the list on the **Tile Layouts** tab in System Explorer. From System Explorer, drag the layout onto an appropriate display area to show it. If available, select the layout and click **Display** to display the video wall on the toolbar.



Change a Tile Layout

To do this:

1. To edit a layout, select it from the **Tile Layout** tab and display it in the display area.
2. Drag content into the layout and delete it.
3. Click **Save** and then click **OK**.

The **Save** icon only appears if the **Allow Save** option is set to **True**.

Delete a Tile Layout

Select a layout in the **Tile Layout** tab, and then press the **Delete** keyboard key or click the **Delete** button in the toolbar.

Copy and Rename a Tile Layout

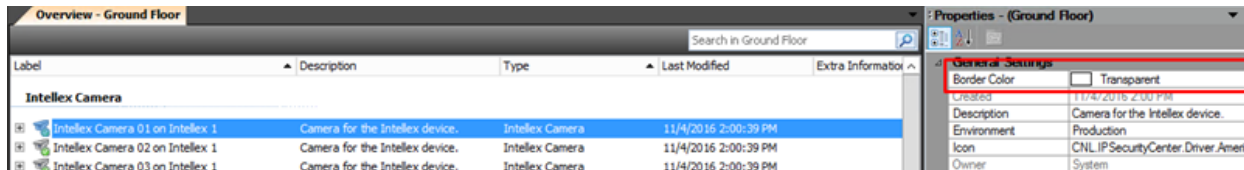
To do this:

1. Select a layout in the **Tile Layout** tab and click the Duplicate button. A copy of the tile layout is saved in the same location as the original layout and appears in **UserCreated Tile Layouts**. The copy uses the naming convention **TileLayoutName - copy**.
2. Open **TileLayoutName - copy** and set it up.
3. Click **Save**. The **Save** dialog appears.
4. Type the **TileLayoutName - copy** and rename the tile layout. Click **OK**. The tile layout appears in **User Created Tile Layouts** saved under its new name.

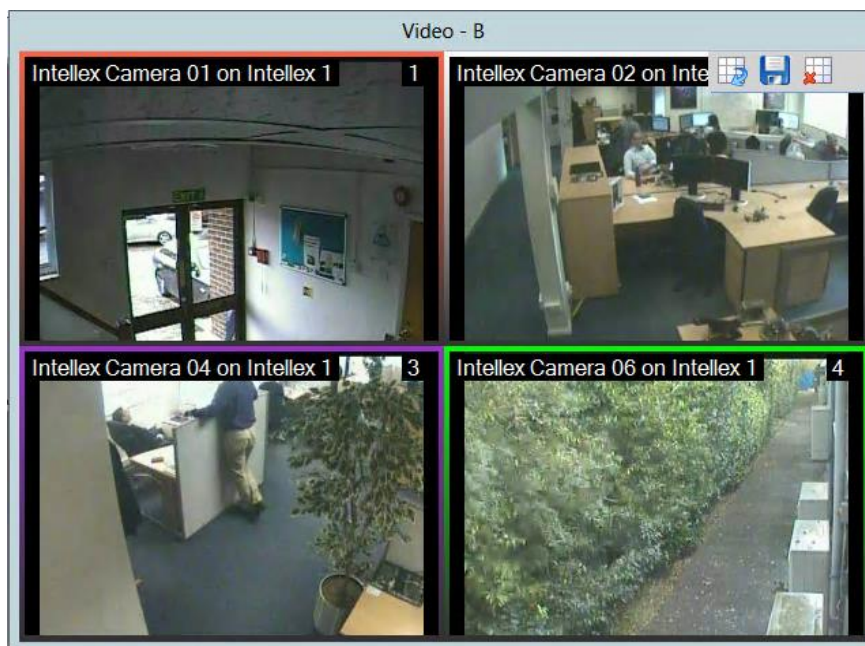
Configure Tile Layout Border Color

Camera Devices include a Border Color property that determines the border color when the camera is displayed on a tile layout.

By default, this property is set to Transparent for backwards compatibility, however you can change it during commissioning of the system.



To display the border color, configure the Allow Tile Menu to True for the chosen Display Area.



Camera Highlighting on the UI

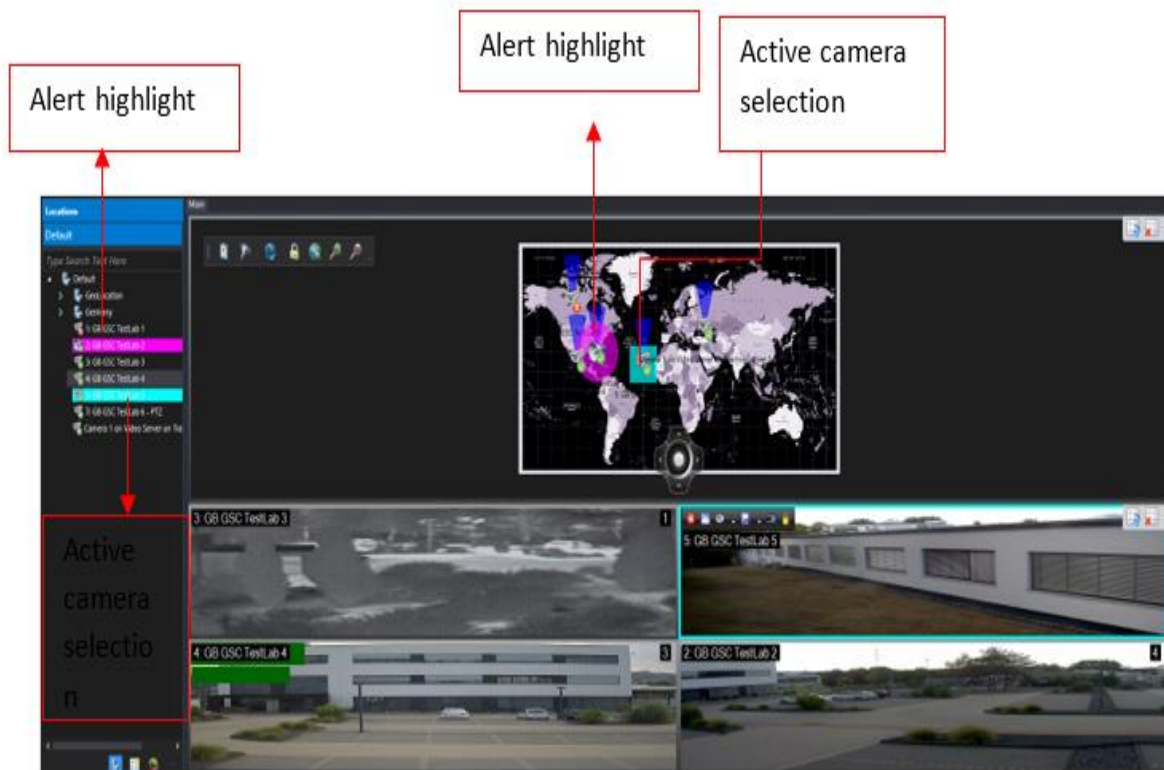
Operators can view what camera they have selected on a map or System Explorer when a camera is selected on a tile. This functionality is particularly useful when a location has several cameras configured with similar labels. The color in which the camera selection is highlighted can be customized in Global Settings. By default, the camera is highlighted in orange.

As this functionality requires multiple camera devices, you must configure a connector and add at least a few camera devices in Control Center.

To view the highlighting of camera selection:

1. Configure a tile layout, for example a 4-way tile layout.

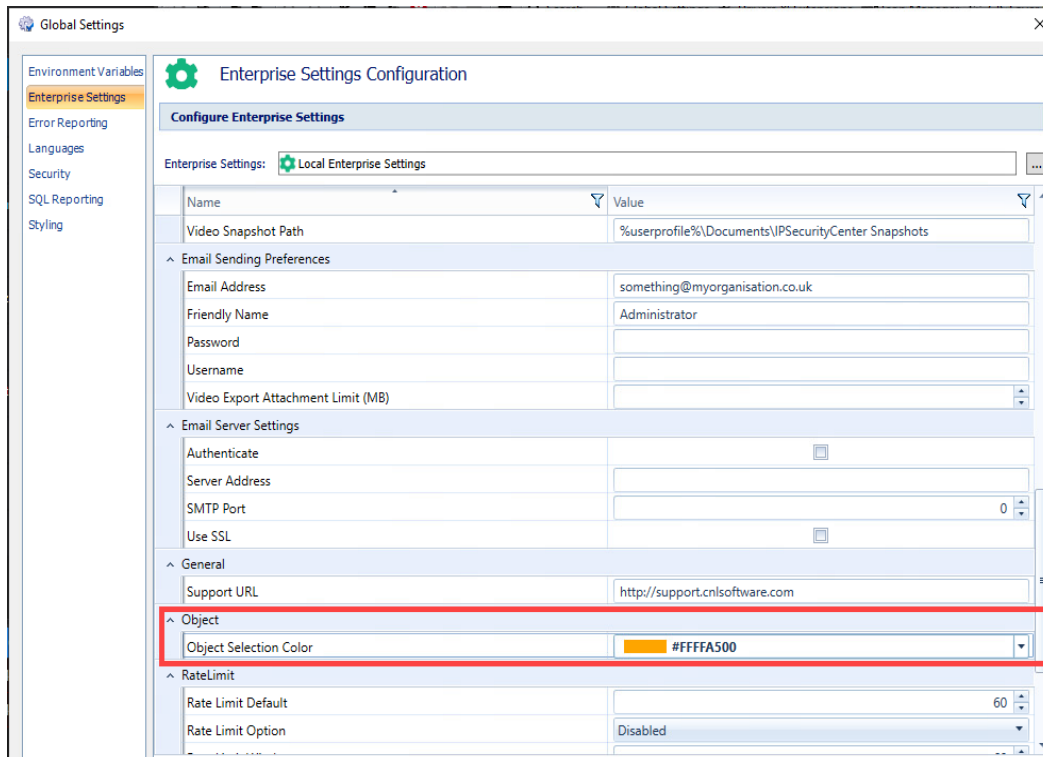
2. Drag and drop camera devices on all the four tiles.
3. Plot devices on the map (either Schematic or Geographic map).
4. Select between the tiles and notice how the devices are highlighted based on your selection in the following areas:
 - **Map (both 2D and 3D)**– On a 2D map, the camera selection appears as a square filled background behind the camera and a static halo around the camera on 3D maps.
 - **System Explorer** – Camera background is highlighted on selection.
 - **Tile Layout** – The border of the tile layout is highlighted around the video.



5. If there is an alert in the system and the camera alert highlight is active on a camera tile, then the tile will alternate between the active highlight and the alert highlight. The same condition applies on the map area as well.

Only a single camera is shown highlighted as the active selection at any one time.

6. To customize the active selection color in which the camera selection appears:
 - a. Click **Global Settings** in the toolbar. The **Global Settings** dialog appears.
 - b. Click **Enterprise Settings**. The **Enterprise Settings Configuration** dialog appears.



- c. Click **Object Selection Color** in the drop-down list and select the required color from the color picker. By default, the color is set to orange.
- d. Click **Apply** to save the changes.

You can publish the camera highlight color changes to all federated sites. In addition, if a tile is configured to display a PTZ-enabled camera, you can disable the PTZ commands with the selection highlighted.

Camera Highlighting in Sequences

You can view what camera is being displayed when the sequence is playing on a tile.

As a sequence is required for the camera to be highlighted when a sequence is being played, you must first create a sequence.

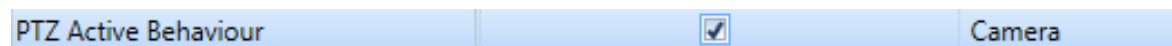
To view the camera when a sequence is being played out:

1. Configure a tile layout, for example a 1-way tile layout and drag and drop a sequence such that the sequence plays out the videos on the tile.
2. Click the tile that has the sequence displayed. As the sequence plays through, the tile is highlighted and the cameras in the sequence are highlighted one by one in the Explorer tree and on the map. For example, if a sequence tile contains camera 1, 2, 3, 4, then they are highlighted one after the other on the System Explorer and the map as the sequence plays through.

Auto-Enable PTZ Mode

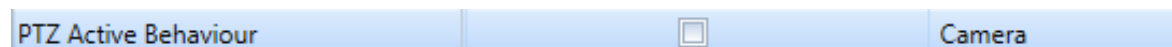
You can restrict users from enabling PTZ mode on a tile when a PTZ-enabled camera is being displayed on it. This is so that the user doesn't move the camera by mistake when clicking on the tile. The PTZ Active Behavior option in the Global Settings > Enterprise Settings tab provides the flexibility to switch the auto-enable mode setting on and off. In addition, you can publish the PTZ active behavior to all federated sites.

When the PTZ Active Behavior mode is active:



- Selecting on a camera tile within the video display area will send PTZ commands if the user has the required privileges.
- Selecting the tile will make the camera the active system object if it is not already active.

When the PTZ Active Behavior mode is not active:



- Selecting a PTZ-enabled camera will not send PTZ commands.
- To send PTZ commands, you must click the PTZEnable button on the menu of the tile where the PTZ camera is being displayed. This will switch on PTZ commands for that camera. Note: You must have the required privilege to send PTZ commands to be able to see the PTZEnable button.
- If Enable PTZ is switched on:
 - You have the option to click Enable PTZ again to disable PTZ commands on the camera using PTZ commands on the tile menu.
 - Selecting the tile will make the camera the active system object if it is not already active.
 - If you Enable PTZ and then select another camera before switching back to the original camera then the Enable PTZ button will revert to being switched off, which will result in PTZ defaulting to being disabled for that camera.

Video Export

Video from disparate sources and systems may be required for investigative purposes. In the past, pinpointing and gathering this footage was a difficult and time-consuming task. At best, footage could be requested by email and, at worst, involved on-site visits to find relevant footage. In Control Center, this process is automated by collecting video from multiple systems connected to Control Center – saving time, energy and associated cost.

Video export can be initiated at the end of an alarm resolution process, the main menu or any customized user interface.

The benefits of the Control Center video export feature allow users to:

- Pinpoint the exact cameras from which to export footage, irrespective of the system
- Specify the date and timeframe of the incident to avoid viewing irrelevant footage
- Schedule when to perform the data export to avoid excessive load on production servers
- Prioritize video export so that more important jobs are completed prior to less urgent cases
- If forensic review of video clips is required, you can email your video clips to the different authorities involved.

You can only specify one email address in the Video Export Wizard. If you need to send the email to more than one authority, you can forward the email to the other authorities once your email has been sent.

Exported video material that is to be used for criminal evidence must include proof that the video has not been edited since it was recorded. This is a feature of each integrated video management system and not part of the functionality currently offered by the video export service.

To install Control Center Video Export Service, see the Video Export Service Installation Guide. To export the video footage correctly, it is important to follow the instructions carefully to ensure that the relevant software and connectors are available on each server.

Video Export Configuration Settings

The Video Export Manager enables Server Administrators manage server resources, destination folder, file size, video export duration, and video export reports.

It may be important, for example, to set the location of exported video to a secure folder on an intranet to ensure it is not viewed inappropriately. Equally, limiting the size and duration of the video export could help Server Administrators manage production servers during busy periods.

1. Click **System > System/Video Export Scheduler**. The **Video Export Manager** appears. The Video Export Manager is set out in tabs for:
 - **My Jobs**
 - **Queued jobs**
 - **Completed jobs**
 - **Configuration Settings**
 - **Defer Locations**
2. Click the **Configuration Settings** tab. The **Configuration Settings** tab appears.

Video Export Folder Options

The left frame of the tab sets the Export Folder options available to users exporting the video footage.

The Default Path specifies the default folder for storing exported video, which is presented to users when defining a new export. This must be an available folder on the network or a local hard drive. To enter a new folder, search for it using the folder browse button or enter the folder location (such as \\10.10.10.10\Security\CCTV\VideoExport).

The Selection Mode user control specifies how the folder options are presented to users defining exports – as a pop-up dialog, a drop-down list, or both.

The Available Folder Paths contain the list of folders that are presented to users for video export. For example, a user may be permitted to save video on more than one network server.

To add a new video export location:

1. In the **Video Export Manager** dialog > **Configuration Settings** tab, click the **Default Path** and then select the required Selection Mode.
2. Click **Add**.

Video Export Folder Thresholds

The video export file size and export time is estimated when the export task is defined. To manage server resources, you must limit the video export file size and export time for each task. You can also set the maximum file size, export time, as well as a warning level, which are called thresholds.

- To set a warning level for file size or time, enter the amount in the **Warning** field.
- To set the error level for a file size or time, enter the amount in the **Error** field.

Video Export Report

When a video export job is complete, a report can be produced in the default folder. The video export report is produced based on a report template. The report template that is used for the report is specified in the Export Report field.

When all the Configuration Settings are set to the environment, click **Save**.

If navigating away from the **Configuration Settings** tab without clicking **Save**, a warning appears prompting to save changes.

My Jobs Tab

If you have any video export jobs defined in the system, they appear in My Jobs tab. The video export jobs appearing in the My Jobs tab can be filtered by Status, Schedule or Location.

1. In the **Video Export Manager** dialog, click **My Jobs**. The **My Jobs** tab appears.
2. To change the **Status** filter, click the first drop-down that shows **Any**. The job status options appear and includes:
 - Successful
 - Canceled
 - Failed
 - Queued
 - In Progress
 - Completed
3. To change the **Schedule** filter, click the second drop-down that shows **Today**. The job schedule option appears and includes:
 - Last 24 hours
 - Last 48 hours,
 - Last 7 days,
 - Last 2 weeks,
 - Last 4 weeks
 - Anytime.
4. To change the **Location** filter, click **Location**. The Control Center locations appear displaying the locations throughout the organization.

Creating a New Video Export

To create a new video export:

1. Double-click a camera in a tile to display the Playback Time bar.
2. Select a specific duration for which you want to export the video by hovering on the time bar and selecting it with the mouse, then right-click and select **Export Video**. The **Video Export Wizard** appears.
3. Click **Next** to continue.
4. Click **Name** and enter a name, for example Incident 33 – Public disturbance.

5. Enter a short description and click **Next**. The **Load Template** page appears. When using video export for the first time, there are no saved templates however a previously saved export job can be saved as a template for reuse. Using a template is useful when a camera location or period of time is frequently requested.
6. If setting up the first video export job, select **Do not use a template** and click **Next**. The **Video Source Selection** page appears. The **Video Source** page presents all the camera devices within Control Center to which the logged in user has access. The devices are grouped by Location. Individual or multiple devices can be selected, or even an entire Location and all the devices in that Location.
7. Select the camera devices to export video from and click the right arrow button to move it into the **Selected Tasks** field.

Use the Ctrl and Shift key to select multiple devices.

8. Click **Next**. The **Options** page appears. The **Options** page allows the footage date and time range, the video export path and job priority to be entered. .

Exporting video can be a time-consuming, processor-intensive, and memory-intensive process. To reduce interruption to other services, select the most precise incident time possible and set the job priority appropriately

9. Click **Start Time** and then select a date and enter the start time.
10. Click **End Time** and enter the date and end time for the video export. For training purposes, select a narrow time range to expedite the export. The **Location** field is used to specify the folder to which the video export is deposited. The options available here were configured in the **Video export folder** options.
11. Select the location for the video export. The Video Export Service prioritizes export jobs with Priority 1, regardless of when they were created, or the number of low priority jobs already present in the export queue.
12. Select **Normal** priority and click **Next**. The Export Scheduler Wizard calculates the estimated video export size and export time. The **Summary** page appears with the estimated Completion Time, Download Size and Total Tasks.
13. If forensic review of a video clip is required, you can email your video clips to the different authorities involved by selecting **Send via email**. The **Email** page displays.

Export Scheduler Wizard
✕

Options
Specify the export options

Start/End Date Time
Specify the start and end time of the required recorded video

Start Time

End Time

Location
Specify the location to which to export the video to

Path

Job Priority
Specify the priority of the job in the queue

Priority

Send via email

This checkbox is only available if you have configured your Email server settings in Control Center. See [Sending Emails From Control Center](#).

14. Configure the **Email** page as follows:

Name	Description
Email address	Add a valid email address.
Subject	Add the subject of the email message.
Message	Add the body of the email message. Note : Messages are stored in the Pacific database.

15. Select **Next**.

16. Select **Submit**.

If the export size and duration thresholds set in **Configuration Settings** are exceeded, warnings and errors are displayed in red on the **Summary** page.

The video export may have a status of **Successful** even though an email was not sent. Check the **Additional Information** column for your export job. If there are any issues with the job, a **See tasks for more details** message is displayed. Double-click this message for more information.

If you selected **Send via Email** and you have selected more than one camera to export video from, then Control Center adds each clip as a separate attachment, as long as the total number of attachments does not exceed the attachment file size limit. If one of the video clips causes the file attachment size limit to be reached, that clip is not attached and a **Could not attach to email (exceeded maximum attachment size)** error is displayed for that clip in **Additional Information**.

Video export jobs are saved to disk so if you do have a video clip that has not been sent then you can send that clip in a separate email.

Saving Video Export Templates

The Export Scheduler Wizard also allows you to save a template.

To save the exported template, from the **Summary** page of the **Export Scheduler Wizard**, click **Save Template**. For example, you can save a template for frequently exported camera locations.

Viewing Video Export Jobs

To view the video export jobs:

1. Click **My Jobs**. The video export job appears in the list.

If the job does not appear in the list, click the **Queued** tab while it is processing.

2. Locate the job in the **My Jobs** tab and then click the hyperlink label to view the job details. The job appears in a new tab and includes details of the original task, the information about the requestor, request time, actual start and finish time, and priority. It also includes a link to the destination folder to locate the exported video material.

Deferring Video Exports by Location

To manage system resources, you can defer video export tasks to run out of office hours, for example. Video export jobs are still run based on priority but outside the deferred time windows.

To defer video exports:

1. Click the **Defer Locations** tab. The **Defer Locations** tab appears.
2. Click the **Search** button beside the **Location** field. The Control Center search objects dialog appears.
3. Enter the location or use the **Find Now** button to locate the Control Center location that is to be deferred. Double-click to select it.

4. Enter the time frame during which video export is to be deferred in the **From** and **To** fields.
5. When complete, click **Submit**. Video export jobs submitted in the time frame selected are deferred until after the suspension window.

To cancel a deferred location, select it in the list and click **Cancel**.

Dynamically Launching the Video Export Wizard

It is now possible to launch the Video Export Wizard dynamically from a response plan or a custom User Interface. The option to launch the wizard is exposed as a function of the Windows Client object called Show Video Export. Additionally, using the Show Video Export With parameters function in the Window Client object, you can launch the Wizard with a set of parameters, for example, a list of cameras. These functions can be used to, for example, create a button on the Main menu that enables an end user to invoke the Video Export wizard.

Configuring Video Export Button on the Main Menu

Configuring a button in Control Center involves configuring two types of settings:

1. Display Settings
2. Button Clicked event settings

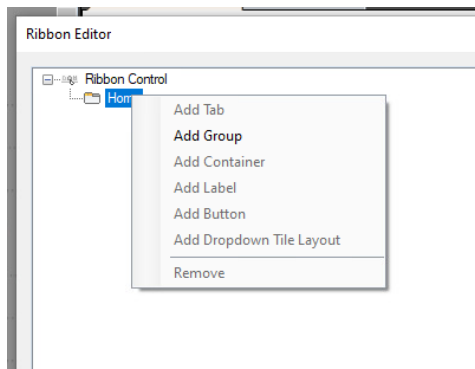
Configuring Display Settings

To configure display settings for the **Video Export** button:

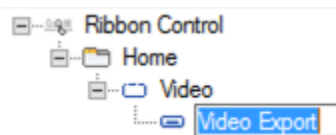
1. Open **System Configuration** > System Objects. The **System Objects** pane appears.
2. From the **Graphical User Interface** section, double-click the **Main Menu** object. The **Main Menu** object opens in the GUI Designer.
3. With the Main Menu GUI object selected, in the **Properties** pane, click **Custom Menu Items Collection**. >The **Ribbon Editor** appears.



4. In the **Ribbon Editor**, right-click **Home** and select **Add Group**. A new group is added.



5. Rename the group to provide a meaningful name, such as **Video**. This will appear in the main menu as the title of the group.
6. Right-click the newly created group, in this case **Video**, and select **Add Button**. A new button icon appears in the main menu GUI control.
7. Select the button to rename it with a more meaningful name, such as **Video Export**.



8. In the **Properties** pane on the right, click the **Name** property and rename the button to **Video Export**.
9. Click **OK**. The Main Menu GUI object displays the newly created **Video Export** button on the toolbar.



10. From the GUI Designer, right-click on the Main Menu title bar and click **Save**.

Configuring Button Clicked Event Settings

To configure button clicked event settings for the **Video Export** button:

1. From **System Configuration > System Objects**, double-click to open the Main Menu Graphical User Interface. The **Main Menu** object opens in the GUI Designer.
2. From the GUI Designer, select the **Video Export** button from the drop-down list.

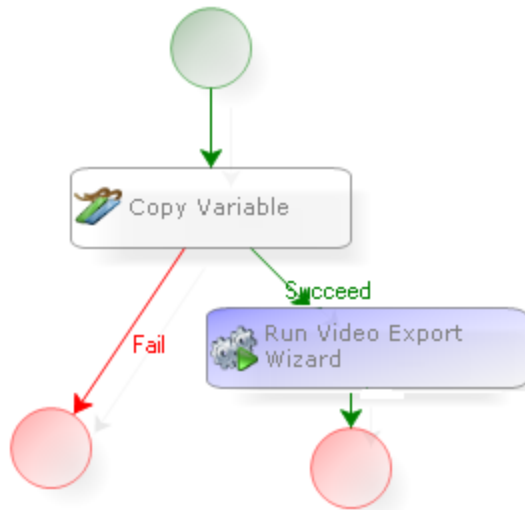
3. From the **Events** drop-down list on the right, select the **Clicked** event. The **Video Export Clicked** Event Page opens in the Response Plan Editor.



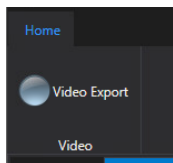
4. Configure the **Video Export_Clicked** Event from the Response Plan in the following order:
 - a. Create a new optional **Windows Client Page** variable and rename it to **Windows Client**.
 - b. From the **Shapes** palette, drag and drop the **Copy Variable** onto the editor.
 - c. With the **Copy Variable** selected, in the **Properties** Pane, specify the following details:
 - **Source Variable** – Current Generic
 - **Target Variable** – Windows Client
 - d. On the **Succeed** route, drag and drop the **Dynamic Action** shape.
 - e. Configure the **Dynamic Action** shape with the following information:
 - **Target Object** – Response Plan Variable
 - **Target Object** – Windows Client
 - **Actions** – Show Video Export
5. Right-click anywhere in the editor and select **Finish All Routes**.



VideoExport_Clicked
[Ribbon Button]



6. Save the response plan.
7. Return to the GUI editor and save it. Then switch to the main menu display. The **Video Export** button appears on the main toolbar.



8. From the main menu toolbar, click **Video Export**. The **Export Scheduler Wizard** appears.

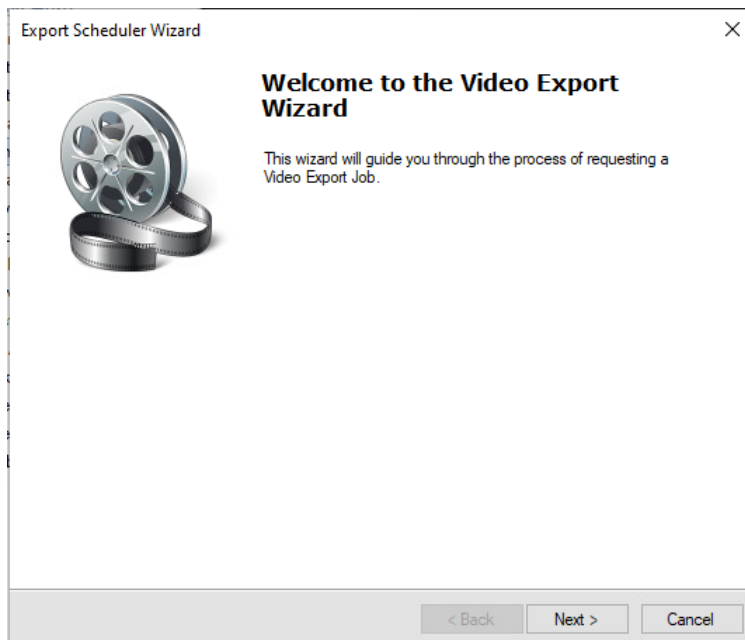
Populating Video Export Wizard From the Client

To populate the Video Export Wizard:

1. From the **System Configuration** window, click **Computers**.
2. Select the **Windows Client** object for the client you need to view the Video Export Wizard for.

Windows Client		
+	test17server.cnluk.com	Client Computer with the IP hostname of TEST17SER... Windows Client
+	test18server.cnluk.com	Client Computer with the IP hostname of TEST18SER... Windows Client

3. On the **Properties** pane, click the **Show Video Export** button. The **Export Scheduler Wizard** appears.



4. Click **Next** to continue with video export.

Showing Video Export Wizard with Parameters on the Client

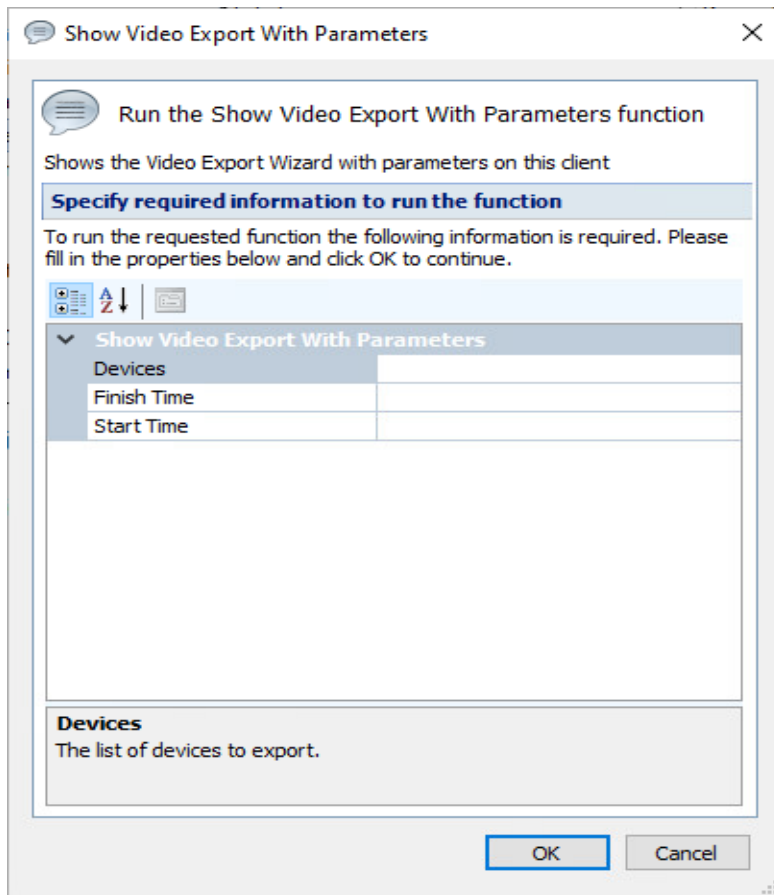
To show Video Export Wizard with parameters on the client:

1. From the **System Configuration** window, click **Computers**.
2. Select the **Windows Client** object for the client you need to view the Video Export Wizard for.

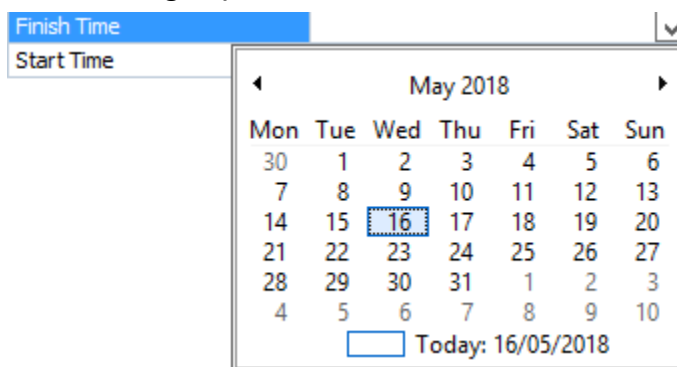
Windows Client

+	test17server.cnluk.com	Client Computer with the IP hostname of TEST17SER...	Windows Client
+	test18server.cnluk.com	Client Computer with the IP hostname of TEST18SER...	Windows Client

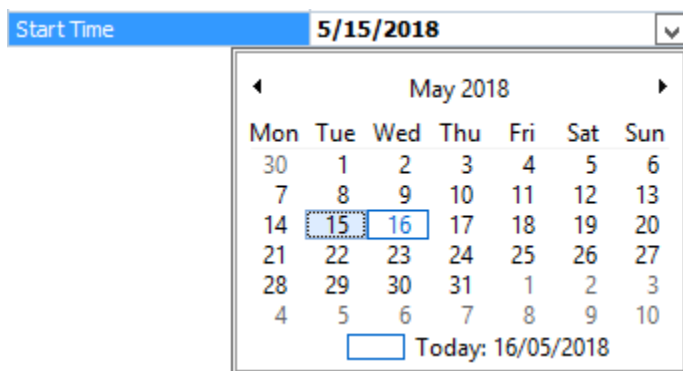
3. On the **Properties** pane, click **Show Video Export With**. The **Show Video Export With Parameters** dialog appears.



4. From the **Show Video Export With Parameters** dialog, click **Devices**. The **Search Objects** dialog appears.
5. Click **Find Now** and select a video device that you want to export the video for.
6. Click **Finish Time** and specify the finish date and time for the video footage that is being exported.



7. Click **Start Time** and specify the start date and time for the video footage that is being exported.



8. Click **OK**. The **Export Scheduler Wizard** appears.
9. On the **Export Scheduler Wizard**, click **Next**. Specify a **Label** and **Description** for the video export template and then click **Next**.
10. On the **Load Template** page, select **Do not use a template** option and then click **Next**.
11. On the **Video Source Selection** page, leave the default selection unless you need to change it. The **Selected Tasks** pane displays the camera that was selected in step 5. Click **Next**.
12. On the **Options** page, verify if the **Start/End Date Time** are populated correctly.
13. Click **Browse** to specify the destination path for the video that is being exported and then click **Next**.
14. On the **Summary** page, click **Submit**. The **Export** process is initiated.

Using Video Export Wizard Shortcut

The Video Time bar allows you to export a video while it is in Playback mode using the Video Shortcut option.

Troubleshooting Video Exports

Video Export Report Generated Without Template

If the report template specified in the **Configuration Settings** tab of the Video Export Manager is deleted, then video export reports are still generated after the video export is complete. To stop the generation of reports, open the **Configuration Settings** and remove the report template.

Video Export and Device Connector Packages

If the device connector package already existed on the Video Export Server prior to installing Control Center, the old package must be deleted and replaced with the latest connector pack. It is also advisable to delete the temporary files for the package (located in C:\windows\temp\CNLOrthe Local Settings\Temp\CNL folder of the user). After any update to the connectors on the Video Export Server, it **MUST** be restarted.

Restarting the Video Export server while video exports are in progress may result in loss of data.

Video Surveillance Control Board

The Command Center is bundled up with the Joystick feature which enables you to display cameras on a tile layout and control the angles or the directions of the device (if it is a PTZ camera). You can choose to perform all the PTZ actions such as Live/pause/playback and take snapshots of the video being played using the controls on the Joystick Control Board.

The control board has 3 units as listed below which can be connected separately or as a hub and can be placed in any order to suit your requirements.

- AXIS T8311 Video Surveillance Joystick
- AXIS T8312 Video Surveillance Keypad
- AXIS T8313 Video Surveillance Jogwheel

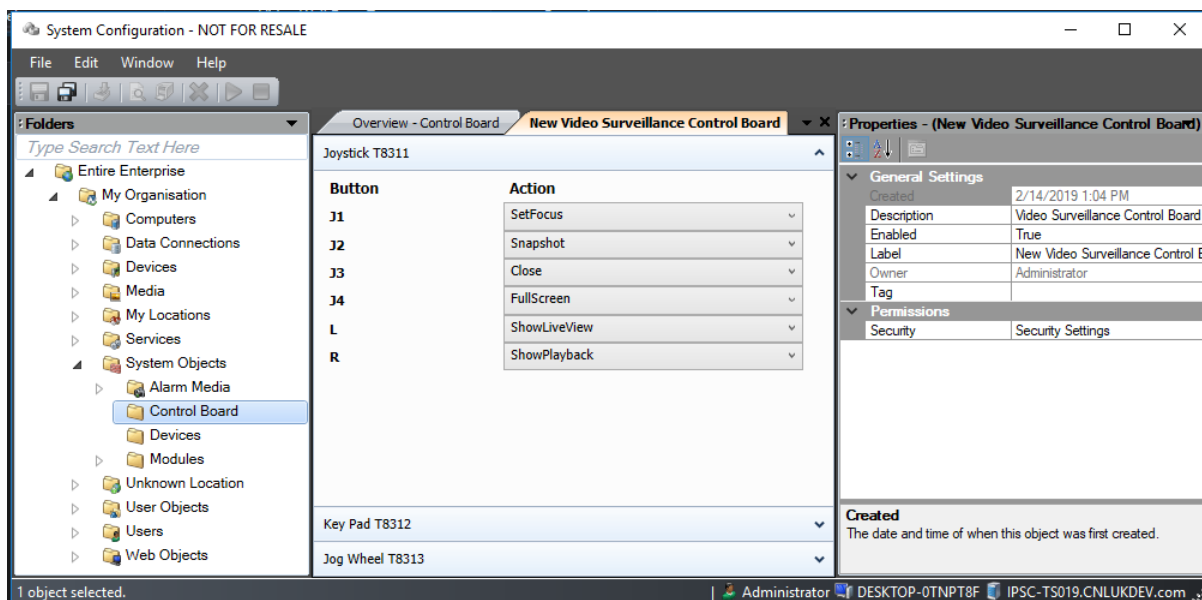
The Command Center comes with a preconfigured object for Joystick control board when the extension is installed. It is important to note that the extension can only be used with the latest version 5.8.7 of the Command Center. For the use of the Joystick feature, you need to upgrade the Command Center to version 5.8.7 using the Upgrade Manager and install the Joystick extension separately. The extension comes packed with the standard installation kit. For installation steps, please read the installation manual.

Note:

- The extension needs to be installed first before upgrading the Command Center to the latest version.
- The extension must be installed on both Server side and Client application.

Double click the Video Surveillance Control Board object to open the User interface where you can configure the actions for the keys/buttons on the Video Surveillance Control Board. The actions for each of the keys comes preset as the part of the solution, but these can be changed at any point by the administrator to suit the requirements.

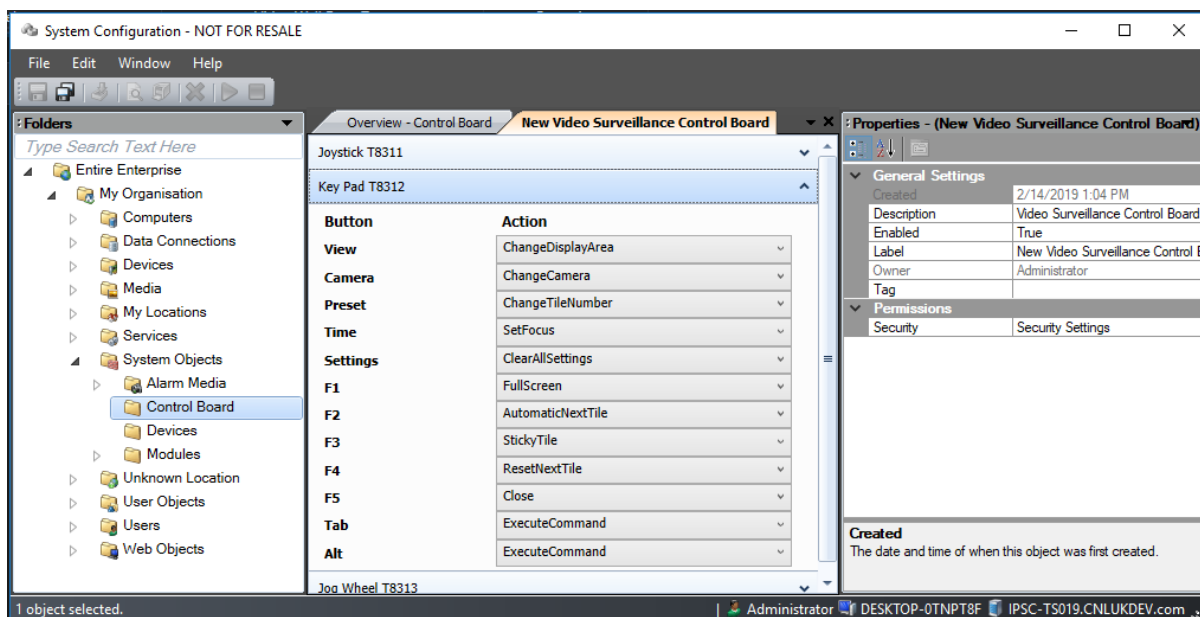
Joystick



There are six keys on the joystick control board which are configured as shown in the table below.

Keys	Actions
J1	SetFocus: Highlights the tile selected. Select the tile and SetFocus button to highlight.
J2	Snapshot: Takes a snapshot of the video being played in the selected tile.
J3	Close: Closes the camera on the tile.
J4	FullScreen: Plays the video of the tile selected in full screen.
L	ShowLiveView: Plays live video from the camera of the tile set to focus.
R	ShowPlayback: Playback the recorded video from the camera of the tile set to focus.

Keypad

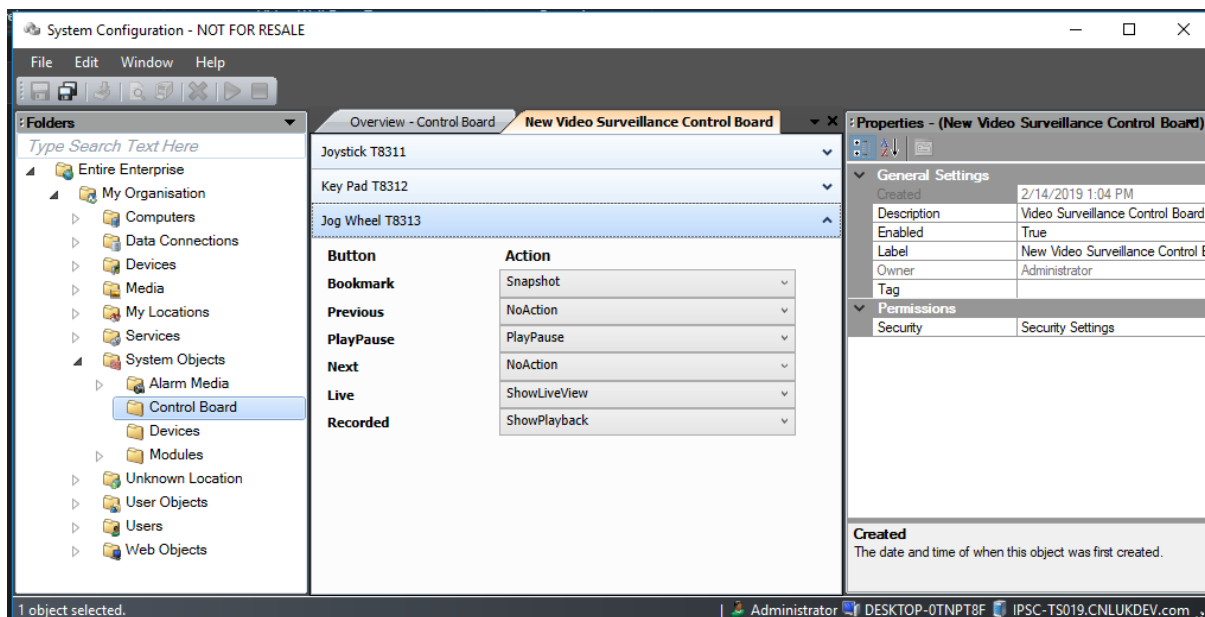


The keypad has thirteen actions configured into the board as shown in the table below.

Keys	Actions
View	ChangeDisplayArea: Press this button and the display area number for selection.
Camera	ChangeCamera: Press this button and the Camera number for selection.
Preset	ChangeTileNumber: Press this button and the tile number for selection.
Time	SetFocus: Highlights the tile selected. Select the tile and SetFocus button to highlight.
Settings	ClearAllSettings: Clears all actions previously done.
F1	Fullscreen: Plays the video from the camera of the tile selected in full screen.
F2	AutomaticNextTile: Puts the cameras being selected in consecutive tiles. If all the tiles are occupied, it goes back to the first tile in the display area and replaces the camera in it.

F3	StickyTile: Places the cameras being selected in the tile on focus.
F4	ResetNextTile: Takes the focus back to the first tile in the display area.
F5	Close: Closes the camera displayed on the tile selected.
Tab	ExecuteCommand: Executes the action command.
Alt	ExecuteCommand: Executes the action command.

Jog Wheel



Jog Wheel has six buttons with actions configured as shown in the table below.

Keys	Actions
Bookmark	Snapshot: takes a snapshot of the video for future use.
Previous	No action has been configured.
PlayPause	Play/Pause: Play/Pause a video from the camera of the tile set on focus.
Next	No action has been configured.
Live	ShowLiveView: Use this to switch to Live mode from Playback.

Recorded	ShowPlayback: Play back video from a camera from the selected tile.
----------	--

Working with Video Surveillance Control Board

The Video Surveillance Control Board solution comes with a configured object that can be found under system objects folder. The actions to all three boards are configured as mentioned in the table above but can be changed by the administrator to suit the working environment.

Double click on the object to open the Video surveillance configuration page. You will be able to see three tabs which displays the configuration for the three control boards of the Joystick unit.

The control tabs and the actions configured for each button on the corresponding control board is as shown in the previous section.

Click on any tab to view the configuration of the keys on the control board.

Assigning Unique Values to Display Areas and Devices

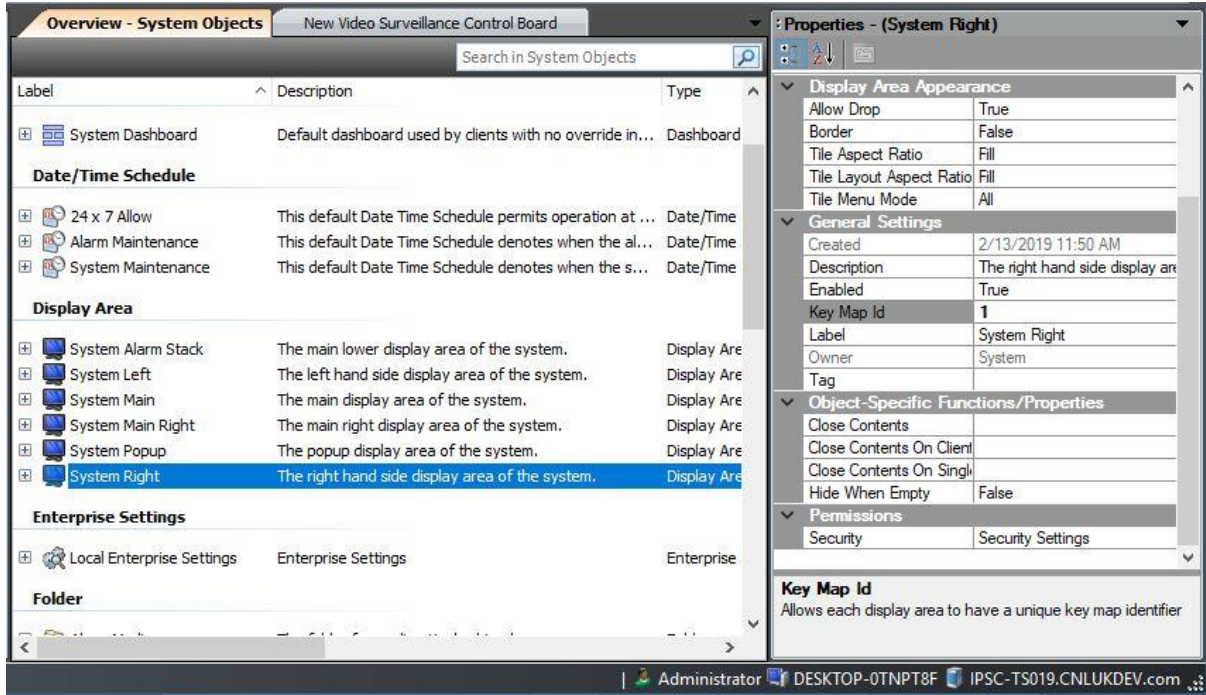
To be able to use the control board effectively, the cameras need to be identified by the control board through a unique identifier and displayed onto a display area or a video wall which can be recognized by the control board. To do this, a new key Map Id variable is introduced under General settings in the properties window of the display area and the devices, which takes a positive numerical value.

The value assigned to this variable has to be unique for each device and display area.

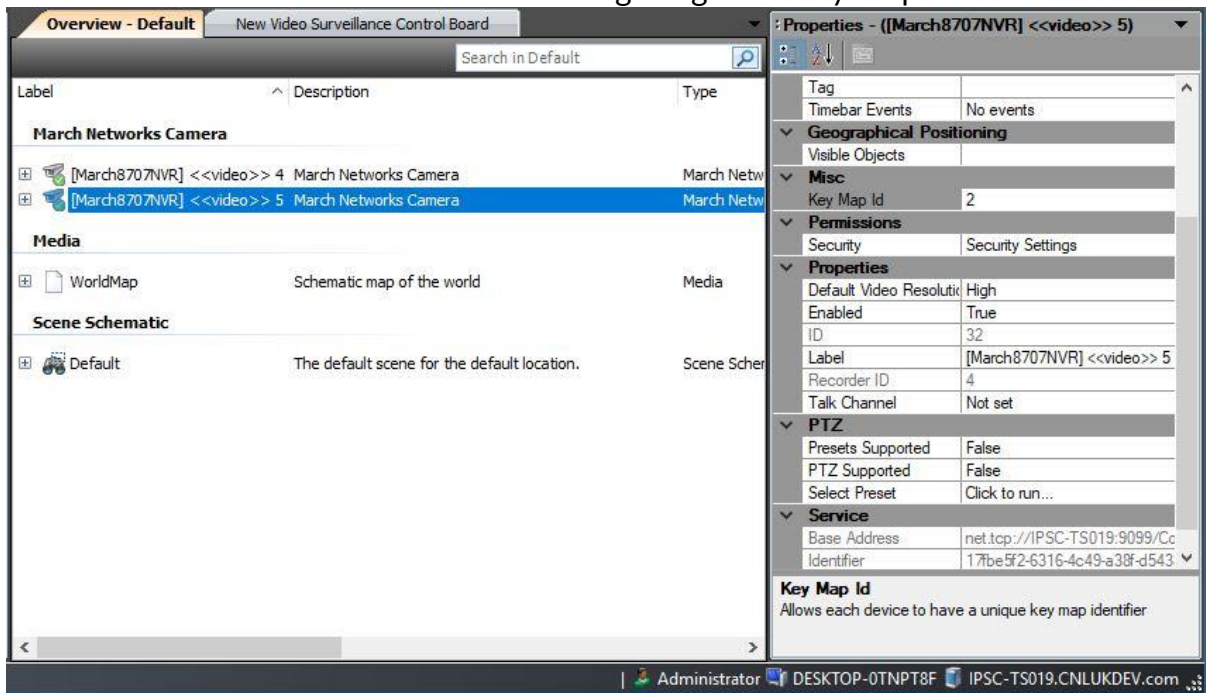
To do this:

1. Go to **System Configuration > System object > Modules > Display areas.**
2. Select the display area you want to assign the Key Map Id to.
3. In the Properties window on the right, select the **Key Map Id.**
4. Enter a unique positive number.
5. Select **Save.**

In the screenshot below, System Right Display area under System Objects is been assigned a Key Map ID value of 1.



The screenshot below shows a camera being assigned a Key Map ID of 2.



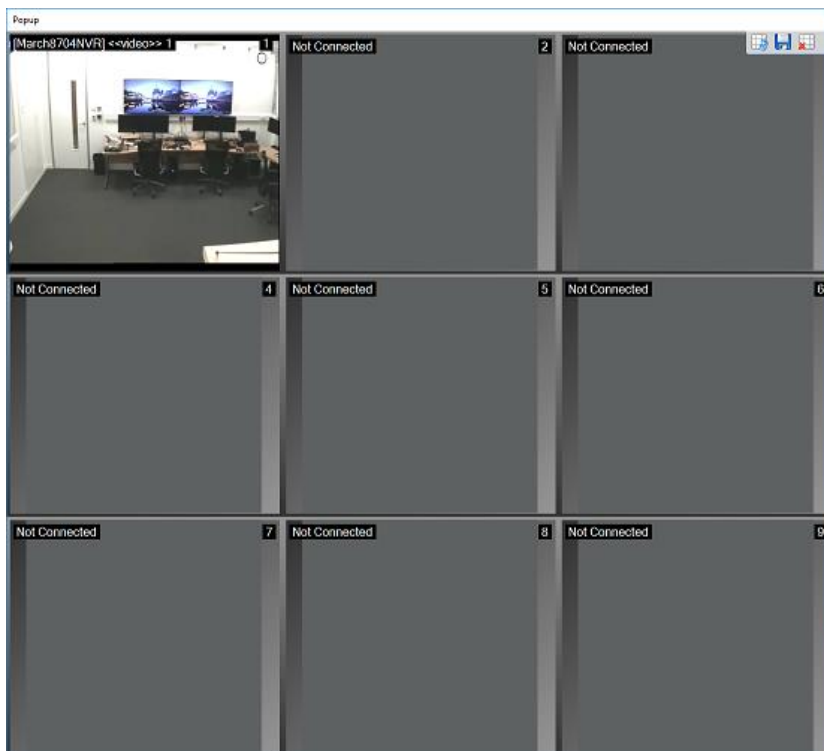
Using the Key Map ID's to Display a Camera

Assuming the Key Map ID for display areas and devices have been set priority, the following procedure will take you through the process of displaying the camera on a tile layout and performing various actions on it.

To display a camera on a tiled display area, do the following:

1. Go to **System > Setup Display** window.
2. Choose the Display area you want to display the cameras on. For example: **Popup**.
3. In the properties of the display area, set **Allow Drop** and **Allow Tile Menu** to **True**.
4. Return to the Main Screen of the Command Center and select a **9-way** tile layout and drop it onto the **Popup Display** area.
5. On the Keypad Control board, press the View Button and then 2 (considering that the Key Map ID for Popup display area is 2), to select the display area.
6. Press the Camera Button and 2 to select the camera.
7. Press Preset and 1 to select the tile.
8. Press Alt or Tab to execute the command.

This displays Camera 2 in tile 1 of the display area Popup, as shown in the screenshot below.



Displaying Cameras on Consecutive Tiles

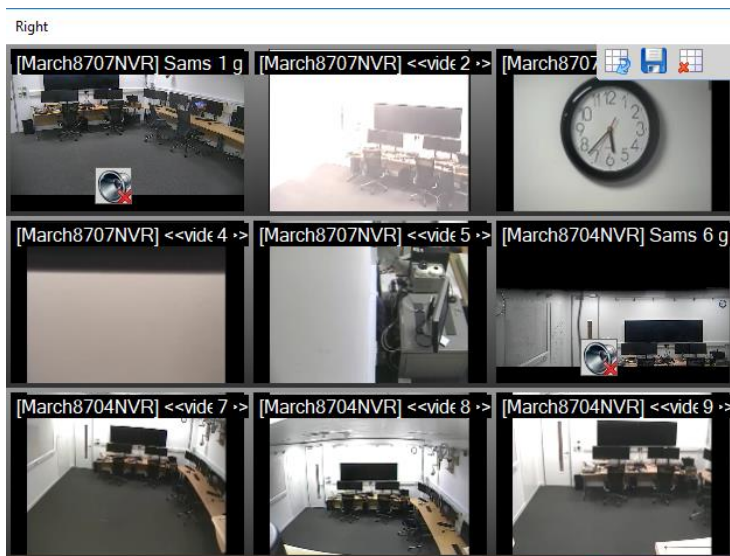
For a camera to be displayed on a tile there are selections to be done.

- Display area
- Camera
- Tile number

In cases where the display area remains the same and the tile number is the adjacent one to the tile on focus, you just need to key in the camera number using the **AutomaticNextTile** action on the keypad control board. This is done by following the simple steps explained below:

1. Display a camera on tile 1 of the display area as explained in the previous section.
2. Press F2, which initiates the **AutomaticNextTile** action.
3. Press the Camera button and the camera number on the keypad control board.
4. Press the Alt or Tab button to execute the command.
5. Continue step 3 and 4 until all the tiles are filled up.
6. Press F4 which initiates the **ResetNextTile** action. This, effectively, stops the **AutomaticNextTile** action and takes the focus to tile 1.

The tiles are filled with different cameras using the **AutomaticNextTile** action, as shown below.



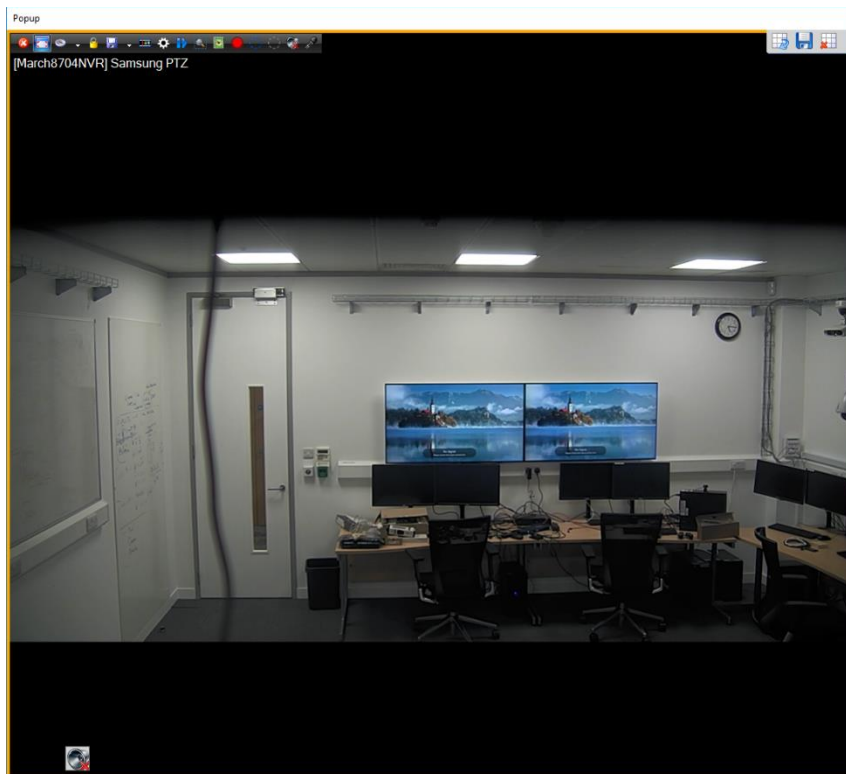
Note:

- This action can be started on any tile number, not necessarily on tile 1
- If the **AutomaticNextTile** action is continued after all the tiles have been occupied, it then starts to replace the camera from tile 1.

Displaying Cameras on the Same Tile

If you wish to have a closer look at the video from a camera, select a tile and enlarge it to be displayed in a Fullscreen size. Furthermore, you can also select different cameras to view on the same tile in the Fullscreen mode. To achieve this, do the following:

1. Display a camera on a tile as explained in [Displaying Cameras on Consecutive Tiles](#).
2. Set focus on the tile you want to enlarge by pressing the J1 button and selecting the tile number. The selected tile will have a highlighted orange border.
3. Press J4 on the Joystick control board to display the tile in Fullscreen.

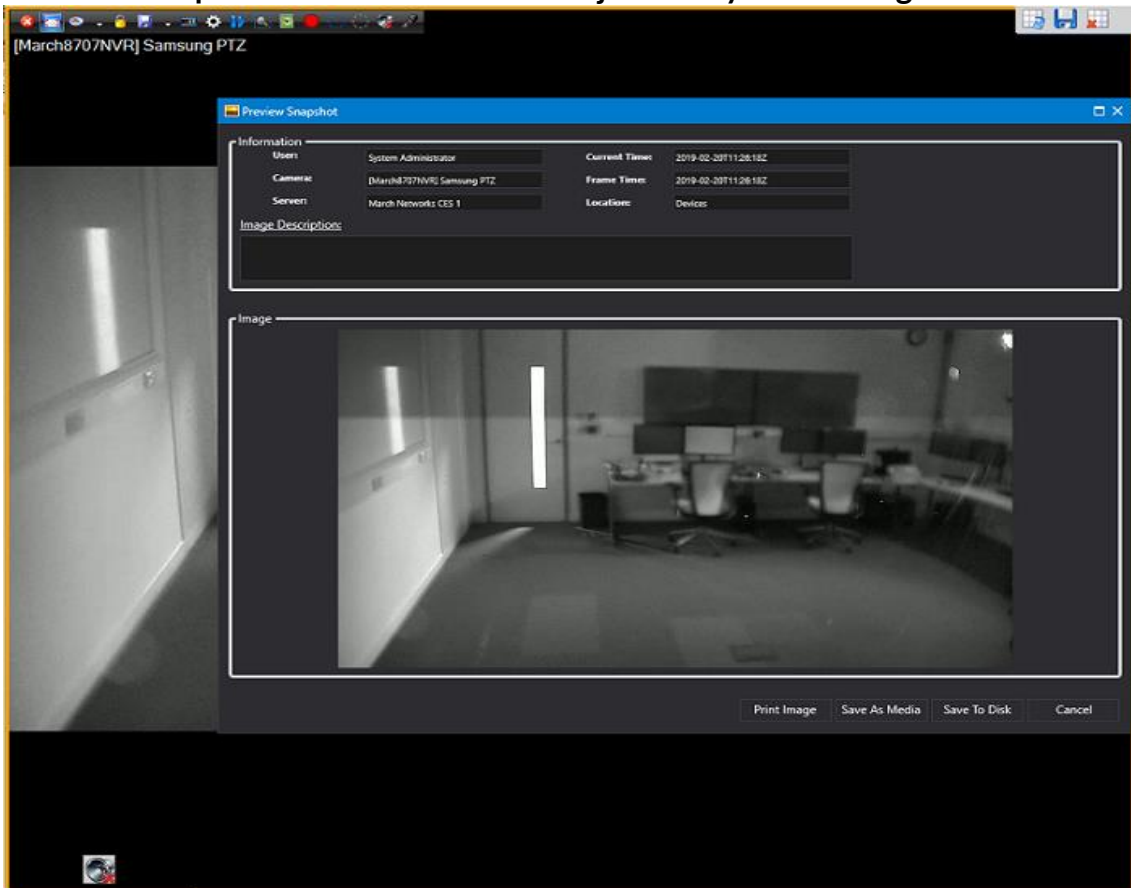


4. Press F3 on the keypad control board to kick off the sticky tile action.
5. Press the camera button and the camera number on the keypad control board.
6. Press Alt or Tab button to execute the command.
7. Repeat step 5 to display different cameras on the same tile.

Taking Snapshots From a Video

Snapshots can be taken from a live video and saved on to the disk or as a media file in the Command Center. Snapshots can be taken from a camera on a tile or when it is in Fullscreen mode. Follow the simple steps mentioned below to save the snapshots:

1. Display a camera on a tile or enlarge the tile to **Fullscreen** using the method mentioned above.
2. Press the bookmark button on the Jogwheel or J2 button on Joystick to initiate the **Snapshot** action. The **Snapshot** window appears for you to choose where the snapshot needs to be stored. You could select saving on to the disk or as a media file in the **Snapshots** folder under **User Objects** in **System Configuration**.



Play/Pause Recorded Video

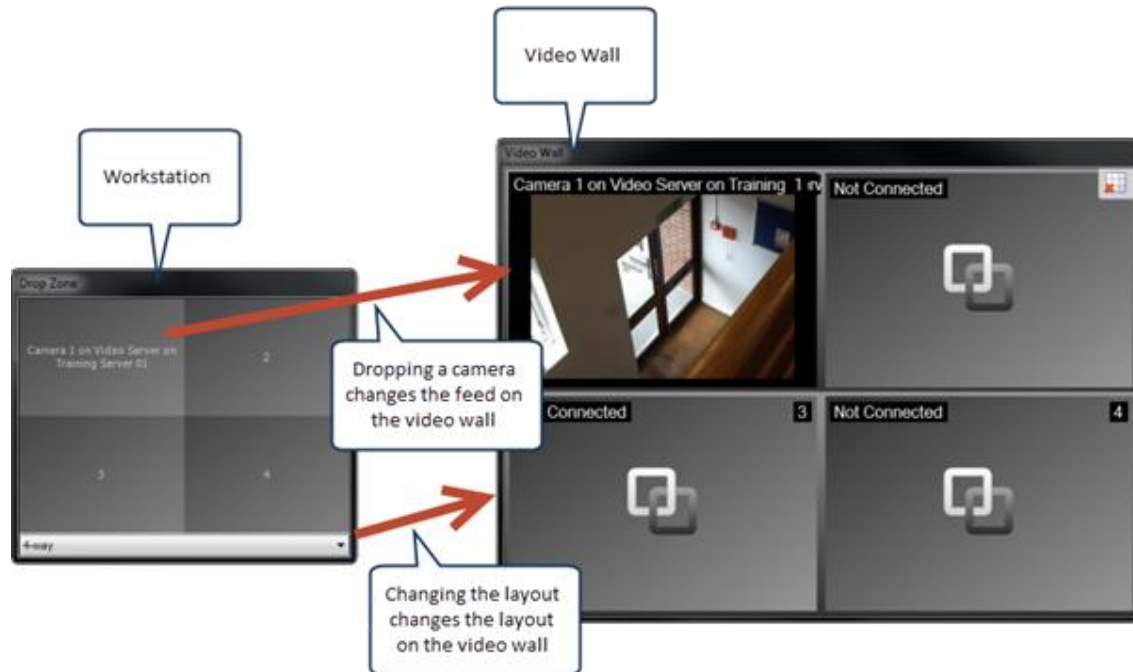
You can Play/Pause a video in the recorded mode to have a closer look or save a snapshot for future use. The Live(L) and Recorded button(R) button on Joystick or Jog wheel will allow you to toggle between the live feed and recorded mode. While playing the recorded video you could pause and then resume play with the Play/Pause button on the Jogwheel.

Right



Video Wall

Control Center comes in-built with a Video Wall functionality natively and enables you to interact with third-party Video Walls. This allows users to control video wall layouts and content, most commonly through a Drop Zone control.



Configuring Control Center as a Video Wall Client

To configure an Control Center workstation to be a Video Wall follow these steps.

- **Add Display Areas** - Create a Display Area for each Video Wall screen connected to the workstation. Position the display areas to fill the screens.
- **Add Tile Layouts**- Create a Tile Layout object per video wall screen.
- **Configure the Client**- Create a GUI and then configure the Client in Properties.

To configure the Client:

1. Select the Client Computer object that should be used as a video wall.
2. Select the **Video Wall Client** property and click the drop-down that appears when selecting **Disabled**.
3. Check the **Video Wall Enabled** checkbox.
4. Add the display areas and tile layouts to be controlled on the Client by clicking the **Add** button and finding and selecting the display areas and tile layouts.

Video Wall Enabled

Display Area	Tile Layout	
Video Wall Left	Video Wall Left	<input type="button" value="Add"/> <input type="button" value="Remove"/>
Video Wall Right	Video Wall Right	

The client has now been configured to act as Video Wall.

Configuring a Third-Party Video Wall

A third-party video wall does not require any specific configuration in Control Center other than being added.

Configuring a Video Wall Control

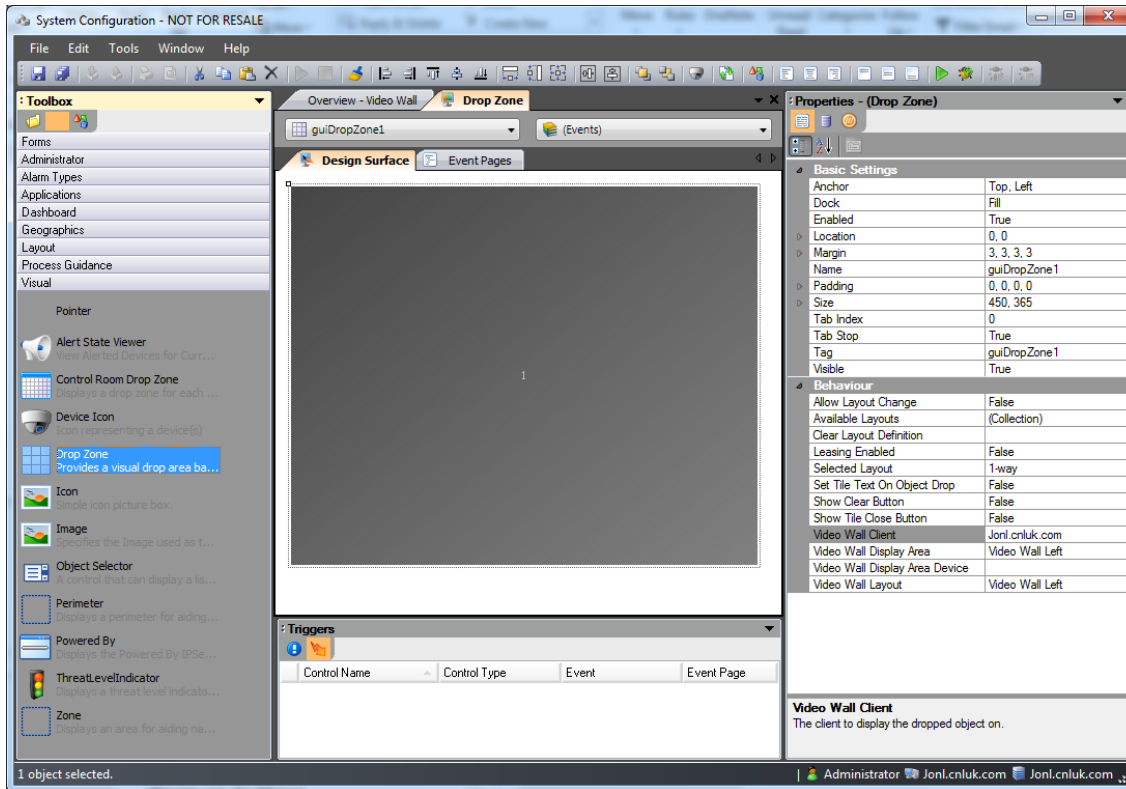
Video walls can be controlled through response plans or through the Control Center user interface by using Drop Zone controls. A Drop Zone illustrates the current layout and content of the video wall and allows you to change the layout, content and so on.

The following drop zone controls are available in the User Interface designer:

- **Drop Zone** - Used for configuring a drop zone for a specific video wall screen.
- **Control Room Drop Zone** - Used for automatically discover and control all video walls configured in a selected folder.

To configure a Drop Zone control:

1. Create a Graphical User Interface and provide a name, for example, Video Wall.
2. From the **Visual** palette, drag and drop a Drop Zone control onto the design surface.
3. In **Properties**, set the **Dock** property to **Fill**.



Using an Control Center Workstation as a Video Wall

To configure the drop zone to control an Control Center Client, update the **Video Wall Client** property so that the video wall client is selected. Then update the **Video Wall Display Area** and **Video Wall Layout** properties to point to the previously configured display areas and layouts.

Using a Third-Party Video Wall Controller as a Video Wall

To configure the Drop Zone to control a third-party video wall controller, update the Video Wall Display Area Device to be the Video Wall device.

Using a Control Room Drop Zone Control

To configure a Drop Zone control:

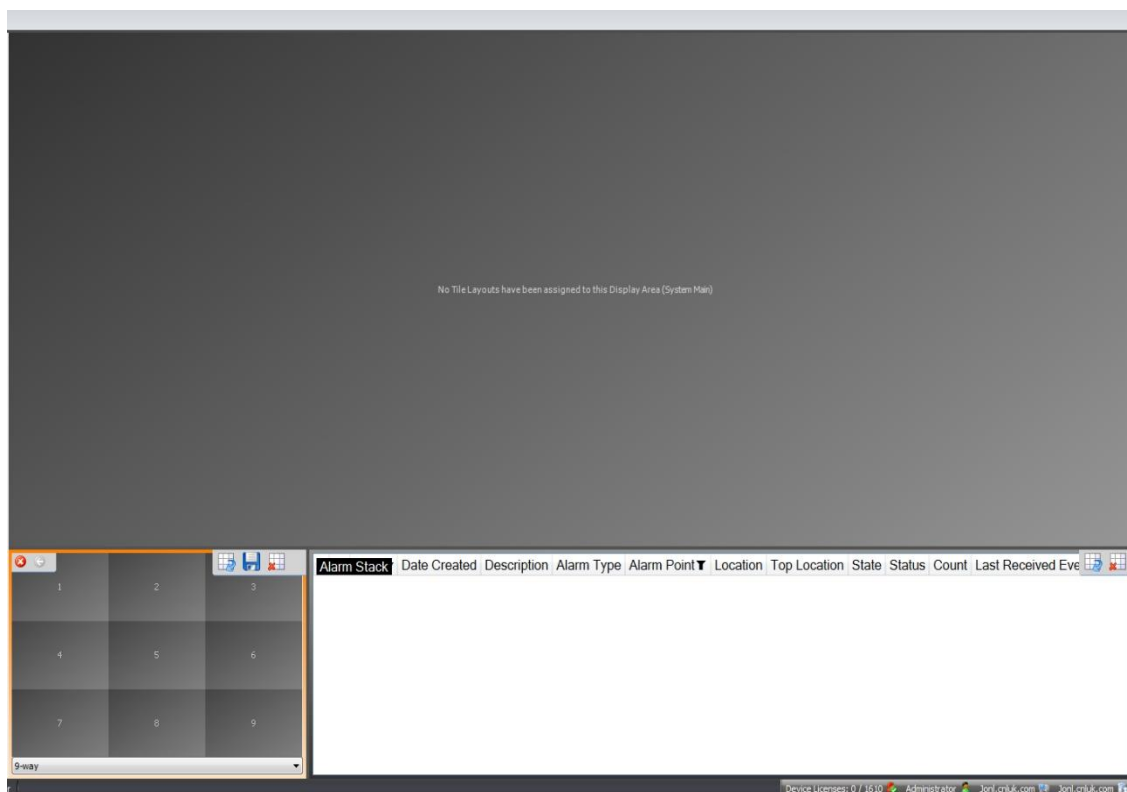
1. Create a Graphical User Interface and drag and drop a **Control Room Drop Zone** control onto the design surface.
2. Set the **Dock** property to **Fill**.
3. Set the **Folder** property to point to a folder where the Control Center Client objects exist that have been configured as a video wall. The drop zone automatically updates to reflect the configured display areas.

By default, the control will be laid out so that each display area to be controlled is presented next to the others in a horizontal row. This can be changed by using the Control Room Custom Layout property. Set this property to a tile layout to change how the drop zone is laid out.

Video Wall Common Properties

In addition to the properties described for the Drop Zone and Control Room Drop Zone controls, you can configure the following properties:

- **Allow Layout Change.** When this is enabled the user to change the layout on the Video Wall by choosing an available layout from a drop-down box below the drop zone.



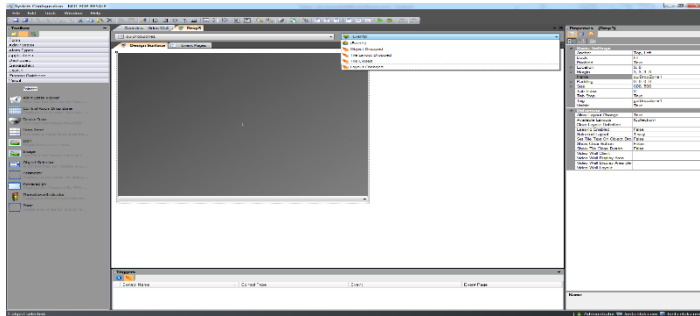
- **Available Layouts.** Use this to select which layouts should be available to the user.
- **Clear Layout Definition.** This defines what the default layout should be if the user clears the video wall.
- **Leasing Enabled.** Enable this to enable leasing (see below).
- **Set Tile Text on Object Drop.** When enabled the Drop Zone will be updated with the label of the object dropped on a tile.
- **Show Clear** button. Enable this to allow users to clear the video wall.

- **Show Tile Close** button. Allows users to close the content on individual tiles.

Drop Zone Events

It is normally not required to handle the Drop Zone events. The standard video wall functions apply as soon as the Drop Zone has been configured and displayed. Additional functions are supported however, this is only achievable by handling the four available drop zone events below.

- **Object Dropped** - Raised when an object is dropped on the drop zone by a user.
- **Tile Layout Dropped** - Raised when a user drops a Tile Layout object on the drop zone.
- **Tile Closed** - Raise when the user clicks the tile close button.
- **Layout Changed** - Raised when the user selects a different layout from the tile layout drop-down list.



Using the Drop Zone

You can perform the following actions by using the drop zone control:

- Change of video wall layout by selecting a layout form the drop-down list.
- Display of a camera on a video wall tile by dragging and dropping a camera object on the drop zone
- Display of a Graphical User Interface on a video wall tile by dragging and dropping a Graphical User Interface on the drop zone
- Display of a pre-configured Tile Layout on a video wall by dragging a Tile Layout onto the drop zone
- Closing of content on the video wall by clicking the close icon on a tile or the close button below the wall

Notes:

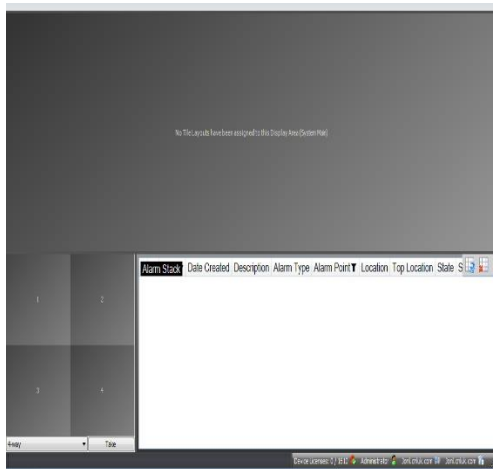
- When viewing a tile layout with several sources on the local monitor, you can also drag and drop the current layout onto the drop zone control to show that content on the video wall.

- If the drop zone control does not support the layout definition in the selected tile layout, then the control will block the drop request.
- You can also change the content on a video wall from a response plan so that content can be shown as a result of an event. Do this by using the Configure Tile and Display Tile shapes.

Video Wall Leasing

You can configure Control Center such that a user can take control of a wall to manage its content, which is also called leasing. You can also define a priority order for users and groups so that one user can take control from another user based on higher priority.

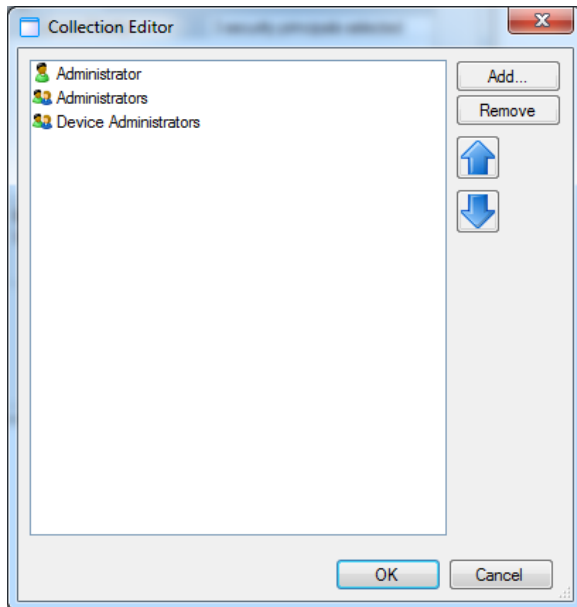
- To enable leasing, update the Leasing Enabled property on the Drop Zone or Control Room Drop Zone controls. The next time the control is shown, a Take button is displayed. A user must take control before the wall is controlled.



You can specify a user hierarchy of control over a video wall when leasing is used. So, if a lower priority user has control of the video wall a high priority user can still take control. Video Wall leasing is configured in the Security Policies editor.

To configure the Video Wall Leasing priority:

1. Right-click on the topmost folder where the policy should apply (for example, My Organization) and select **Security Policy....**
2. Select **User Policies** and double-click on **Video Wall Leasing Priority.**
3. Check the **Define Policy** checkbox and then click **Lease Priority** to define the priorities.



4. Add users and groups as required and organize them so that the user or group with the highest priority is at the top of the list and the user or group with the least priority is at the bottom of the list.

Notes:

- If a user is neither added to the policy nor a member of a group that has been added to the policy, then that user will automatically have the lowest priority.
- If a user has control of a Video Wall Drop Zone Control (either via leasing or because the control is not leased) then the change in user session will cause any cameras being displayed on the Video Wall to be re-evaluated and removed if appropriate.
- If no user has active control of the Video Wall Drop Zone Control via Leasing, then the video will not be able to be re-evaluated and there must be either a commissioned or manual process implemented to remove any content left that should not be displayed after the session change.
- If the Control Center Video Wall Client is used to display content on the Video Wall, then the user that the Video Wall Client is logged in as will be treated as any other user and therefore the video will be re-evaluated after the session change, based on the membership of the groups that the Video Wall client is logged in as.

Performance Monitoring and Diagnostics

A third-party tool has been built into Control Center to provide better easier diagnostics and performance monitoring. The tool is called Loupe and is provided by Gibraltar Software Inc.

' At its core, Loupe has a lightweight assembly that runs in the background of your programs logging the data you need to troubleshoot bugs and bottlenecks in your .NET applications. In addition to recording log messages as you'd expect from any logging framework, Loupe also records unhandled exceptions, performance metrics, and important details about the execution environment of your programs.'

Source: Gibraltar Software

The logging is turned on by default but can be turned off.

To access live and recorded logs, Everbridge recommends the free Loupe Desktop application that can be downloaded from Gibraltar's web site:

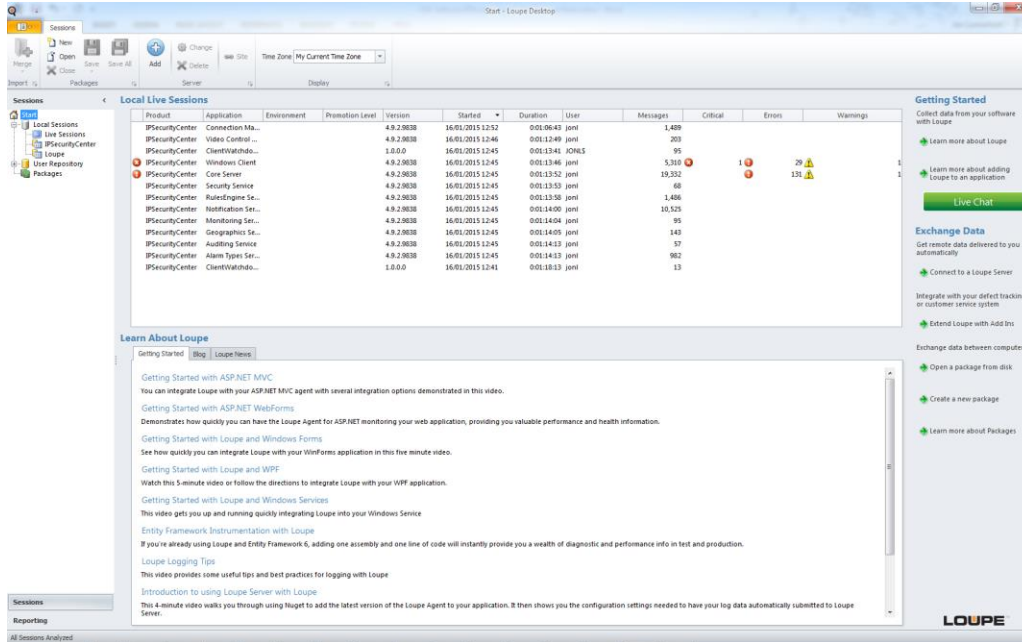
https://my.gibraltarsoftware.com/Support/Loupe/Latest_Version_Download

A lightweight log viewer is also included with the Control Center installation and can be found in the Control Center client and server application directories as well as in the **Tools** directory.

Providing Diagnostics Data to Everbridge When Reporting an Issue

As Loupe is constantly active it is now easier to collect data from a previous occurrence of an issue when reporting an issue to Everbridge. To collect the data, follow these steps:

1. Start **Loupe Desktop**.



2. Right-click on the **Packages** node in the **Sessions** tree on the left side and select to create a new package. Give the package a name relevant to the issue.
3. Select **Control Center** from the **Local Sessions** node in the session tree of the left-side.
4. Drag and drop sessions from the session list that are relevant to the issue. Typically, this is selected based on the time span of the session and the application.
5. Right-click on the package and select **Save As**. Save the package and send to Everbridge along with the issue description.

The screenshot displays the Everbridge Control Center interface for session analysis. The main window is titled "All Sessions - Lounge Desktop".

Find Sessions Within All Sessions

Sessions by Timeframe

Timeframe	Critical	Errors	Warnings	Total
Today	1	1	1	1
Yesterday	0	0	0	0
This Week	1	1	1	1
Last Week	0	0	0	0
Last 7 Days	1	1	1	1
Previous 7 Days	0	0	0	0
This Month	1	1	1	1
Last Month	0	0	0	0
Older	1	1	1	1
All	1	1	1	1

Sessions For the Last 7 Days

Product	Application	Version	Started	Ended	Duration	User	Computer	Dns Domain	Messages	Critical	Errors	Warnings	Added
SPSecurityCenter	ClientWatchdog...	1.0.0.0	16/01/2015 12:38	16/01/2015 12:45	00:00:06:20	JONLS	Joni	orkuk.com	812	1	1	1	3 16/01/2015 16:03

Session Details

Select a session from the list above to view details

Status: Critical, Error, Warning, Messages

No Session Data Available

Buttons: Remove, Open

Auditing in Control Center

Auditing enables you to keep track of the user activities concerning different modules in Control Center.

You can configure auditing across the following modules in Control Center:

- Alarms
- Device
- Device Manager
- Email Manager
- Federation
- Graphical User Interface
- Miscellaneous
- Secondary Authorization
- Security
- Snapshot
- Video Export

To be able to view auditing information, you must first configure the auditing server with the details of the Control Center server whose events you want to audit.

See [Configuring the Auditing Server](#).

You can select one or more activities for each module. By default, all options are selected. For auditing changes to take effect, you must restart all the clients that are connected to the server.

Once you have configured Control Center to capture audit information, you can use the Audit Viewer to view your events. See [Using Audit Viewer](#).

Configuring the Audit Server

To configure the Auditing Server, you must

- provide the Auditing Server with the Control Center server connection details whose audit events you want to track.
- select the events that you want to audit.


To do this:

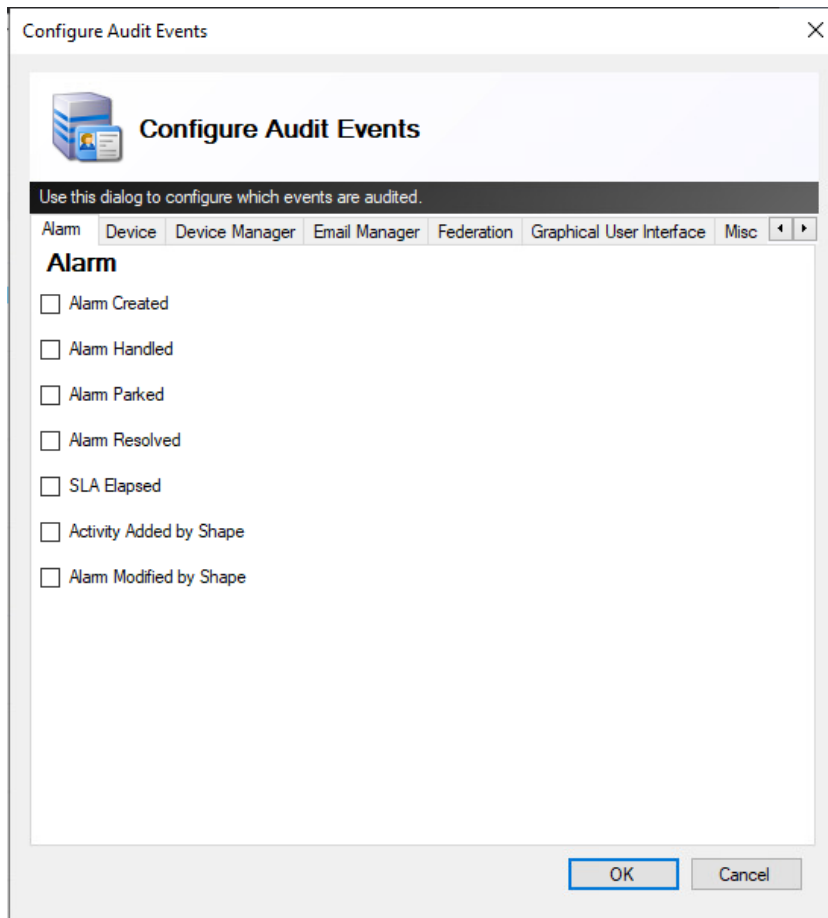
1. From the **Computers** folder, select the **Audit Server** and view the **Properties** pane.
2. In the MSMQ Server field, enter the audit server permissions and point this to the current server.

▼ Permissions	
MSMQ Server	test18server.cnluk.com
Security	Security Settings

- From the **Computers** folder, select the **Server** object and view the **Properties** pane.
- Select **Audit Server** and enter the current server name.

: Properties - (P-SR16-SQL16-01.dev.cnluk.com) ▼	
▼ General Settings	
Core Service	Core Service
Created	2/21/2019 11:28 AM
Description	Server Computer with the IP hostn
Enabled	True
Environment	Production
Fully Qualified Name	P-SR16-SQL16-01.dev.cnluk.com
Label	P-SR16-SQL16-01.dev.cnluk.com
Owner	System
Tag	
▼ Misc	
Execute Command	
IP	10.40.71.43
Maintenance	
Open URL Silently	Click to edit...
Send Email	Click to edit...
Send Email with Attachm	Click to edit...
Start Clients	
Stop Clients	
▼ Performance	
Run Performance Measu	Click to edit...
Show Notifications	False
Tuning Settings	Click to edit...
▼ Permissions	
Audit Server	P-SR16-SQL16-01.dev.cnluk.com
Security	Security Settings
▼ SNMP Settings	
SNMP Community	
SNMP Enabled	False
SNMP IP Address	
SNMP Port	

- From the **Computers** folder, select the **Audit Server** and view the **Properties** pane.
- Expand **Advanced** properties, and select  next to **Audit Events**. Configure **Audit Events** displays.



For information about the events you can select on each tab, see:

- [Alarms](#)
- [Devices](#)
- [Federation](#)
- [Graphical User Interface](#)
- [Miscellaneous Activities](#)
- [Security](#)
- [Snapshots](#)
- [Video Exports](#)

7. You must stop and restart the Control Center services for your changes to take effect.

Configuring a Database for Audit Service

The **Auditing Service** is installed to use the database specified in the **Installation** wizard. It is possible to change this to use an auditing database on a different server. To do this,

locate the connectionstrings.xml file in the **Auditing Service** application directory. By default, this is:

C:\Program Files (x86)\Everbridge\ControlCenter\ControlCenterAuditor\Debug
 Edit this file and update the connection settings for the cnlAuditing tag.

Auditing Alarms

Select alarm activities in this tab to store alarm information in the **Audit** database.

Action	Audit Entry Operation
Alarm Created	AlarmCreated
Alarm Handled	AlarmHandled
Alarm Parked	AlarmParked
Alarm Resolved	AlarmResolved
SLA Elapsed	SlaElapsed - The elapsed time since the alarm was created.
Activity Added by a shape	ActivityAdded - Create an Alarm activity using response plans
Alarm Modified by shape	AlarmModified - Modify alarms using response plans

It is still possible to track alarm auditing via alarm activities.

Auditing Devices

Select device activities in this tab to store device information in the **Audit** database.

Action	Audit Entry Operation
Live Video	
Start	Start
Stop	Stop
View Requested	ViewRequested

Close Requested	CloseRequested
Operator Action	
Operation Action Invoked	OperatorActionInvoked
Recorded Video	
Start	Recorded video started
Stop	Recorded video stopped
Telemetry	
Start	Telemetry video started
Stop	Telemetry video stopped
Preset Recall	Preset Recall
Preset Stored	Preset Stored

Auditing Device Manager

Select device manager activities in this tab to store device manager information in the **Audit** database.

Action	Audit Entry Operation
Device Management task started	Started
Device Management task completed	Completed

Auditing Email Manager

Select email activities in this tab to store email information in the **Audit** database.

Action	Audit Entry Operation
Email Sending	Sending
Email Sent	Sent

Auditing Federation

Select the federation activities in this tab to store federated environment information in the **Audit** database.

Action	Audit Entry Operation
Object Published	Log of users and published changes across the federated environment.

Auditing Graphical User Interface

Select the GUI activities in this tab to store GUI information in the **Audit** database.

Action	Audit Entry Operation
Drop Zone	
Object Dropped	Drop
GUI	
Load	Load
Close	Close

Auditing Miscellaneous Activities

Select the miscellaneous activities in this tab to store this information in the **Audit** database.

Action	Audit Entry Operation
Global Settings	
Settings Changed	Changed
Export	
Object Exported	Exported
Import	
Import New	ImportedNew
Import Overwrite	ImportedOverwritten

Object	
Object Created	Created Object
Object Enabled	Enabled Object
Object Disabled	Disabled Object
Object Deleted	Deleted Object
Object Updated	Updated Object
Object Action Invoked	ObjectActionInvoked
Audit Remote Object Updates	RemoteObjectUpdated
Service	
Service Started	Started Services
Service Stopped	Stopped Services

Auditing Secondary Authorization

Select activities in this tab to store secondary authorization information in the **Audit** database.

Action	Audit Entry Operation
Secondary Authorization Request	Authorization Requested
Request Approved By User	Approved
Request Rejected By User	Rejected
Request Timed Out	Timed Out

Auditing Security

Select the security activities in this tab to store security information in the **Audit** database.

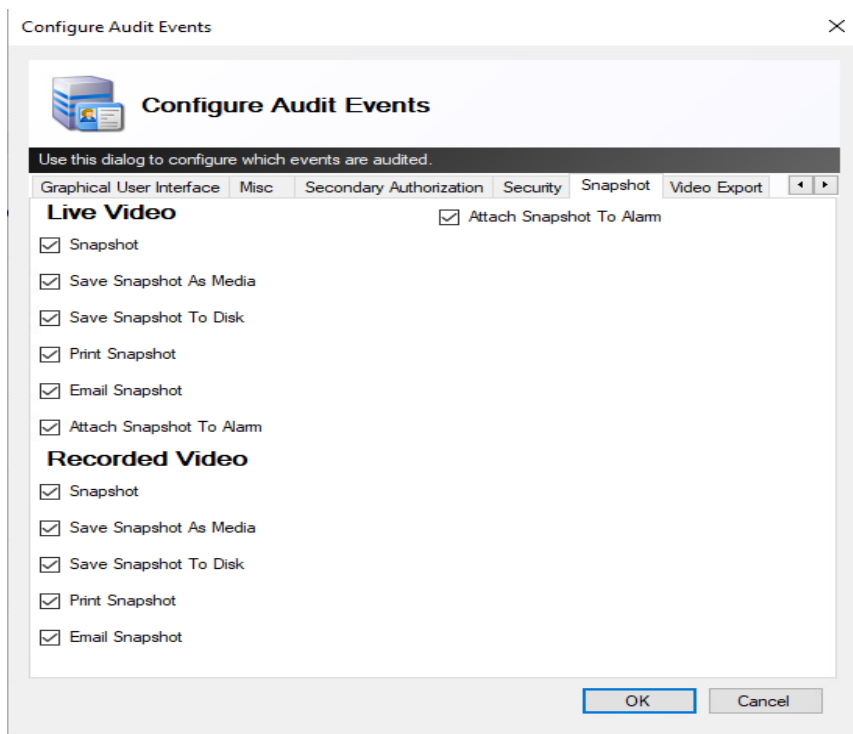
Action	Audit Entry Operation
Membership Changed	

Membership Added	Added membership
Membership Removed	Removed membership
Permission Changed	
Allow Added	Added Allow permissions
Allow Removed	Removed Allow permissions
Deny Added	Added Deny permissions
Deny Removed	Removed Deny permissions
Allow Inheritable Permissions	InheritablePermissionsAllowed
Reset Permissions	PermissionsReset
Security Policy	
Security Policy Changed	PolicyChanged
Reset Policy	PolicyReset
Session	
Log in	Logged in back to Control Center
Log out	Logged out of Control Center
Session Ended	Ended Control Center session
Forced Log out	Force logout
System Locked	System lockout
System Unlocked	System unlocked
Authentication Challenge Successful	Successful Authentication Challenge
Authentication Challenge Failed	Failed Authentication Challenge (VRP Shape)

Failed Login Attempt	Failed login attempt (UserInvalid, UserLockedOut)
Failed Unlock Attempt	Failed unlock attempt (VRP Shape)
User	
Administrator Reset	Reset Administrator
Password Changed	Changed password
Lockout Reset	Reset Lockout

Auditing Snapshots

Select live or recorded video activities in this tab to store this information in the **Audit** database.



The user can control the audit log entries created for the following actions:

Action	Audit Entry Operation
Snapshot	Snapshot

Save Snapshot As Media	SaveSnapshotAsMedia
Save Snapshot to Disk	SaveSnapshotToDisk
Print Snapshot	PrintSnapshot
Email Snapshot	EmailSnapshot
Attach Snapshot to Alarm	AttachtoAlarm

RecordedVideoAuditEvent eventtype represents snapshots from Playback Video

LiveVideoAuditEvent eventtype represents snapshots from Live Video

clienttype	object1guid	object1label	object2guid	object2label	eventtype	operation
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		LiveVideoAuditEvent	Snapshot
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		LiveVideoAuditEvent	EmailSnapshot
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		LiveVideoAuditEvent	Snapshot
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		LiveVideoAuditEvent	SaveSnapshotAsMedia
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		LiveVideoAuditEvent	Snapshot
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		LiveVideoAuditEvent	SaveSnapshotToDisk
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		LiveVideoAuditEvent	Snapshot
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		RecordedVideoAu...	Snapshot
uk.com	49763193-F407-4B2F-AC7C-E2CEBAE19941	Intellex Camera 02 on Intellex 1	NULL		RecordedVideoAu...	SaveSnapshotAsMedia

You can also view auditing for Device Operator actions as executed by users.

Auditing Video Exports

Select activities in this tab to store video export information in the **Audit** database.

Action	Audit Entry Operation
Tile Video Export	
Start	Start exporting a video from a selected tile.
Finish	Finish exporting a video from a selected tile
Failed	Record any failed export attempts
Task	
Started	Create the video export task
Completed	Notify when the video export task was complete

Cancelled	Notify when the video export task was cancelled
Deferred	Notify when the video export task has been deferred
Requeued	Send the video export task back in the queue
Failed	Failed video export task
Job	
Requested	Video Export Server requests for a export task
Started	Server starts the export
Completed	Server completes the export. If the video export has been emailed, the extrainfo column in the VideoExportServiceJobAuditEvent logs the email address, subject, message, success and failure reason, if an email fails to send.
Failed	Server reports a failed export attempt
Cancelled	Server cancels the export on request
Deferred	Server defers the export on request
Requeued	Server puts the export task back in the queue
Deleted	Server deletes the video export task on request

Using the above audit events and configuring them to generate various reports, the administrator can analyze the events more appropriately. The information available for the administrator are as follows:

1. User's data who have published changes to the Federated sites and also users who attempted to publish in a given time frame and what sites were affected. The outcome of the published attempt is also recorded and reasons if failed.
2. User's workstation details who are not connected or operational. Also the administrator can keep a log of clients logged-in and logged-out, time/date and reason if disconnected. It is possible for the administrator to see a clear distinction between logged out status and disconnected so that you can take the necessary action.
3. Generate reports to analyze the above mentioned events at any given point of time.
4. Ability to see the actions taken by the user in the event of an alarm. i.e., if the user has handled the alarm, parked it, resolved it, or completed a specific process guidance step.
5. Ability to see the user actions with respect to a device. As an administrator you will be able to view the user actions on a particular device. i.e. if the user has controlled Pan, Tilt or Zoom, or had requested a preset position.
6. Generate reports of all users who created, modified or deleted a specific object.

Using Audit Viewer

You can use the Audit Viewer to see your audit events. The Audit Viewer enables you to see audit events for a time period that you specify. This is useful because it helps you to answer questions such as:

- Was there a recent change to my Control Center configuration that is related to an issue I am currently facing?
- Who was logged in yesterday?
- When was an update published to a specific site?

To access the Audit Viewer, you can either:

- Go to **System Configuration > Entire Organization > My organization > Computers** and double-click the **Audit Service**. The **Audit Viewer** is displayed.
- Add the Audit Viewer control to a GUI and configure a display area for the GUI. See [Graphical User Interfaces](#).

When you first open the Audit Viewer, the **From Date** and **To Date** are set automatically to display events that have occurred one hour before and one hour after the current date and time.

The table below describes the information you can see in Audit Viewer.



Name	Description
------	-------------

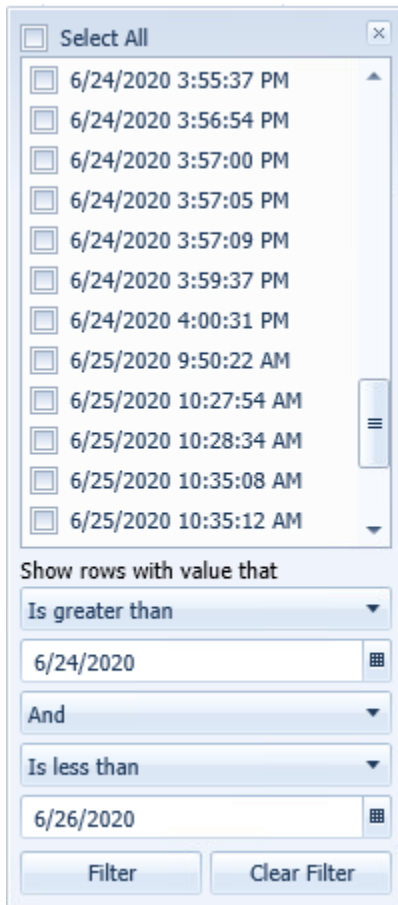
Time	The time the audit event occurred in the format <i>hh:mm:ss</i> AM or <i>hh:mm:ss</i> PM.
Event Type	The type of audit event. For example, ObjectAuditEvents are events raised on objects, like New Response Plan. SessionAuditEvents are events raised on a session, like LogIn and LogOut, AlarmAuditEvents are events raised on alarms and so on.
Operation	The operation performed on the event. For example, Created, Updated, Removed, Start, Stop, and so on.
User	The username of the user who initiated the event.
Client	The name of the Control Center client where the event was raised.
First Object	The name of the object where the event occurred. This could be a username, for a SessionAuditEvent, the name of a device, like Door 1, for an AlarmAuditEvent or a Control Center server name for a ServiceAuditEvent.
Second Object	The name of an object referenced by a first object. For example, when a call is raised on an Intercom device, the first object is the name of the Control Center client that initiated the call and the second object is the Intercom device that received the call.

Filtering in Audit Viewer

You can filter the events in your Audit Viewer. For example, you may want to find out the name of an operator that handled a door forced alarm on Door 2 during a specific period of time.

1. To define the time period when the events you want to view occurred, you can either:

- select  next to **From Date:** and **To Date:** and select the date and time from the date and time picker.
- Alternatively, you can select  to display the **Filter** dialog. You can either select a specific date and time or a period of time. In this example, we know approximately when our operator resolved the alarm so we can define the time period as follows:



The screenshot shows a 'Select All' dialog box with a list of timestamps and a filter configuration section.

Timestamp	Selected
6/24/2020 3:55:37 PM	<input type="checkbox"/>
6/24/2020 3:56:54 PM	<input type="checkbox"/>
6/24/2020 3:57:00 PM	<input type="checkbox"/>
6/24/2020 3:57:05 PM	<input type="checkbox"/>
6/24/2020 3:57:09 PM	<input type="checkbox"/>
6/24/2020 3:59:37 PM	<input type="checkbox"/>
6/24/2020 4:00:31 PM	<input type="checkbox"/>
6/25/2020 9:50:22 AM	<input type="checkbox"/>
6/25/2020 10:27:54 AM	<input type="checkbox"/>
6/25/2020 10:28:34 AM	<input type="checkbox"/>
6/25/2020 10:35:08 AM	<input type="checkbox"/>
6/25/2020 10:35:12 AM	<input type="checkbox"/>

Filter configuration:


Show rows with value that

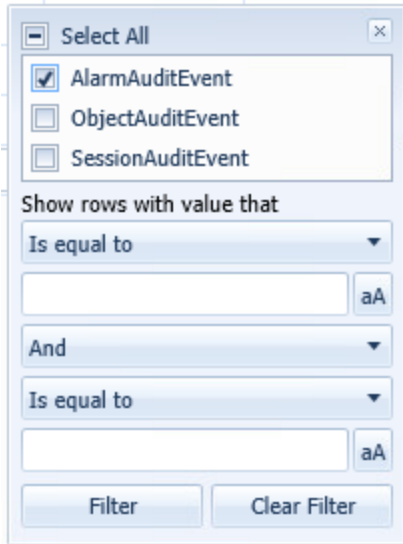
Is greater than


And

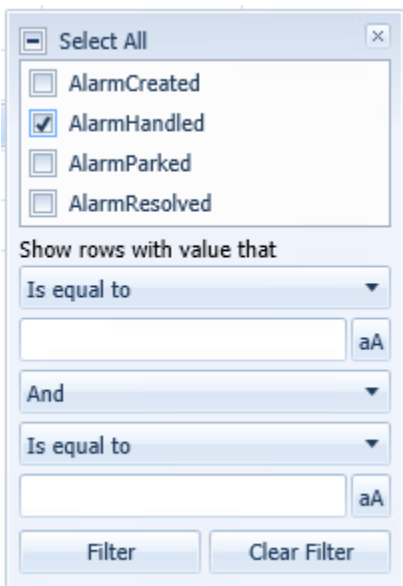
Is less than


Buttons: Filter, Clear Filter

2. In this example, the type of event you want to view is an AlarmAuditEvent, so you select  next to **Event Type** and AlarmAuditEvent from the **Filter** dialog.



- To filter on an operation, you select  next to **Operation** and select AlarmHandled from the **Filter** dialog.



- Ignore **Username** for now, since the username is unknown at this time.
- Select  next to **Client**, and specify the client that raised the AlarmHandled event.

6. Select next to **First Object**, to specify Door Forced on Door 2 on which the alarm handled event was raised.

The Audit Viewer displays the events according to the filter criteria, identifying TestUser1 as the user who handled two Door Forced alarms on Door 2, in the time period specified.

Time	Event Type	Operation	User	Client	First Object
6/25/2020 12:20:48 PM	AlarmAuditEvent	AlarmHandled	TestUser1	P-Win10-3.dev.cnlu	Door Forced Alarm on Door 2
6/25/2020 12:20:46 PM	AlarmAuditEvent	AlarmHandled	TestUser1	P-Win10-3.dev.cnlu	Door Forced Alarm on Door 2

7. Select an entry in the Audit Viewer table to display the details of the event.

Details
Extra Info ✖

AlarmAuditEvent

6/15/2021 4:28:06 PM

Operation

ActivityAdded

User

Administrator

Client

P-SR19-SQL19-2.dev.cnluk.com

Address

P-SR19-SQL19-2.dev.cnluk.com

First Object

Motion Detected

First Object Type

Alarm

Additional Details

Activity

SOP step 'Is there a security incident?' completed, outcome 'No' selected

- Select **Details** to get more information about an event. For example, in an EmailManagerAuditEvent, the object's unique ID, the user who sent the email, the subject and message contents, and whether the email was successfully sent. This helps you answer questions such as, how was a value changed for a specific object, which user handled this object on a remote host, or what service level agreement was breached?
- If available, select **Extra Info** to see the XML (or text) from the **Extra Info** column in the audit database. This is useful if you want to troubleshoot any issues that have arisen due to changes to an event.

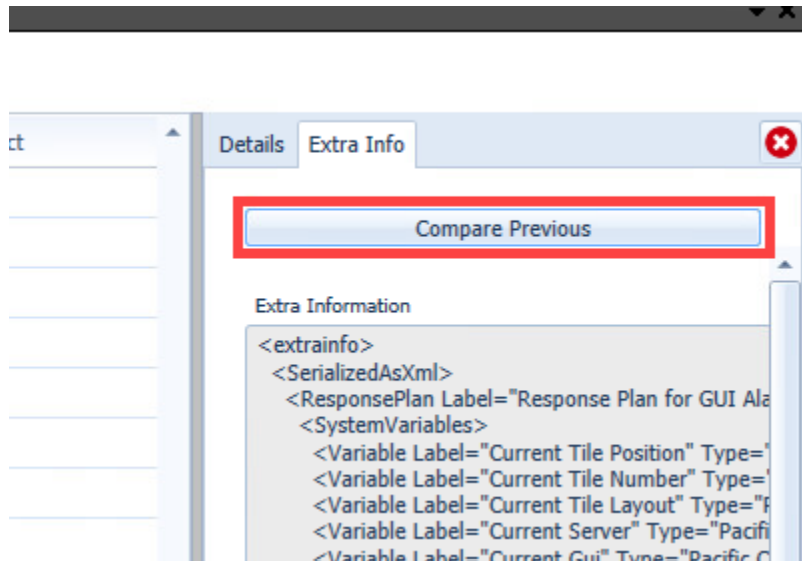
```

Details  Extra Info
<extrainfo>
  <SerializedAsXml>
    <Addon Type="CNL.IPSecurityCenter.SystemAddons.EnterpriseSettings">
      <EnterpriseSettingsCollection xmlns:i="http://www.w3.org/2001/XMLSchema"
        <Settings>
          <EnterpriseSetting>
            <AllowNullValueForReference>>false</AllowNullValueForReference>
            <Category>Object</Category>
            <Description>Highlight color of object when selected in a tile.</Desc
            <IsSystem>true</IsSystem>
            <Name>Object Selection Color</Name>
            <Reference xmlns:d4p1="http://schemas.datacontract.org/2004/07/
            <SettingType>Color</SettingType>
            <UnderlyingTypeName>System.String, mscorlib, Version=4.0.0.0, Cu
            <Value>#FFFA500</Value>
          </EnterpriseSetting>
          <EnterpriseSetting>
            <AllowNullValueForReference>>false</AllowNullValueForReference>
            <Category>Camera</Category>
            <Description>States whether PTZ on a camera is active by default in
            <IsSystem>true</IsSystem>
            <Name>Auto-enable PTZ Behavior</Name>
            <Reference xmlns:d4p1="http://schemas.datacontract.org/2004/07/
            <SettingType>Boolean</SettingType>
            <UnderlyingTypeName>System.Boolean, mscorlib, Version=4.0.0.0,
            <Value>True</Value>
          </EnterpriseSetting>
          <EnterpriseSetting>
            <AllowNullValueForReference>>false</AllowNullValueForReference>
            <Category>General</Category>
            <Description>Support URL, empty string hides Support URL option.<
            <IsSystem>true</IsSystem>
            <Name>Support URL</Name>
            <Reference xmlns:d4p1="http://schemas.datacontract.org/2004/07/
            <SettingType>String</SettingType>
            <UnderlyingTypeName>System.String, mscorlib, Version=4.0.0.0, Cu
            <Value>http://support.cnlsoftware.com</Value>
          </EnterpriseSetting>
          <EnterpriseSetting>
            <AllowNullValueForReference>>false</AllowNullValueForReference>
            <Category>Camera</Category>
            <Description>The path where video snapshots are saved</Descriptio
            <IsSystem>true</IsSystem>
            <Name>Video Snapshot Path</Name>
            <Reference xmlns:d4p1="http://schemas.datacontract.org/2004/07/
            <SettingType>String</SettingType>
            <UnderlyingTypeName>System.String, mscorlib, Version=4.0.0.0, Cu
            <Value>%userprofile%\Documents\IPSecurityCenter Snapshots</Va
          </EnterpriseSetting>
          <EnterpriseSetting>
    
```

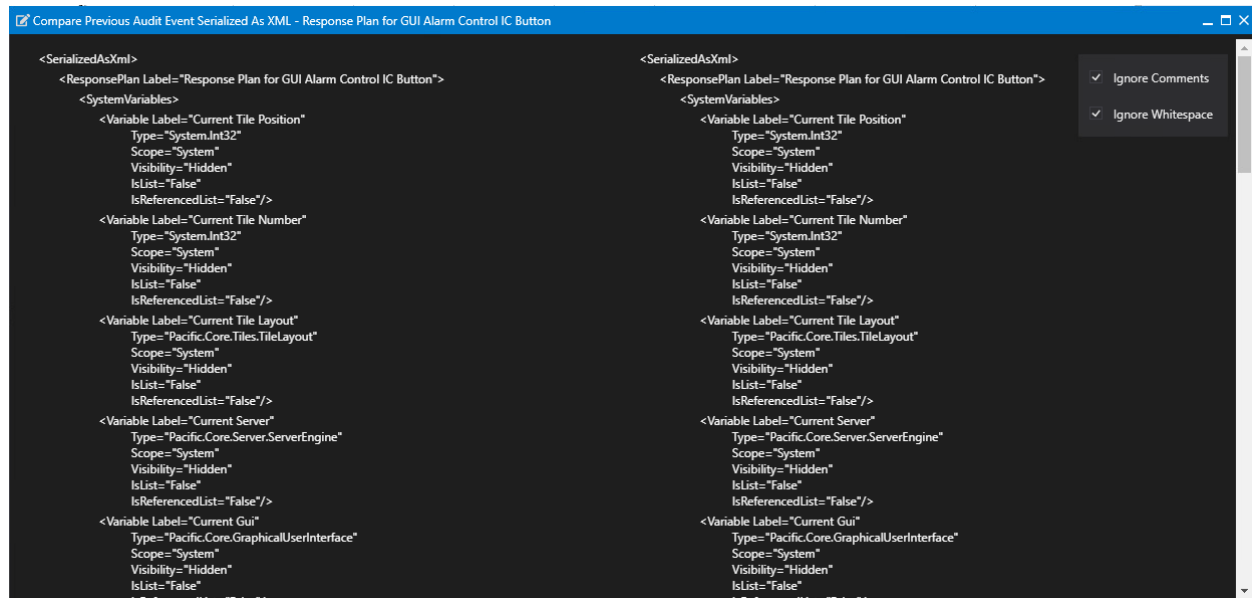
- If available, select **Compare Previous** to compare the XML for two different events, enabling you to see differences between the two events, saving you time. For example, for two events:


9/6/2021 4:56:19 PM	ObjectAuditEvent	Updated	Administrator	P-Win10-2.dev.cnl	Response Plan for GUI Alarm C	Response Plan	
9/6/2021 4:56:19 PM	ObjectAuditEvent	Updated	Administrator	P-Win10-2.dev.cnl	Response Plan for GUI Alarm C	Response Plan	

Double-click the second event, and select **Extra Info**.
 Select **Compare Previous**.



The **Compare Previous Audit Event Serialized as XML** dialog is displayed. Optionally, select **Ignore Comments** and **Ignore Whitespace**.



8. To clear the filters, select  and select **Clear Filter** in all the **Filter** dialogs where you have configured a filter.
9. Select **Refresh** to refresh the Audit Viewer.

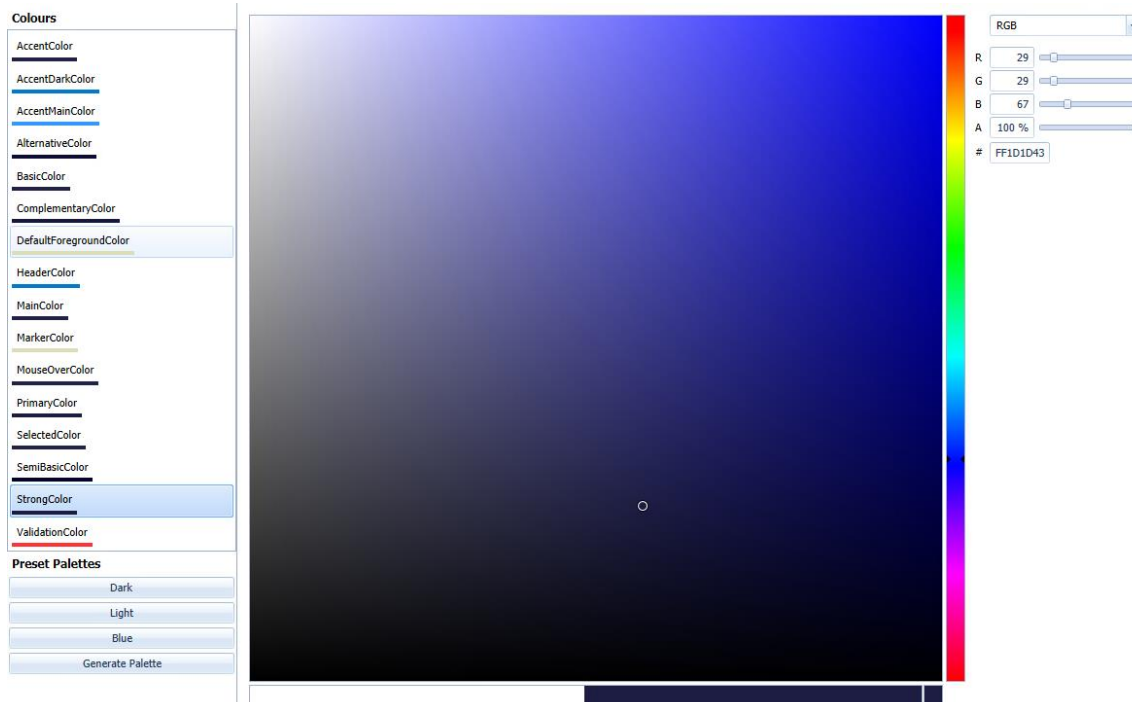
Client Default Theme

Every install of Control Center comes packaged with a Client Default theme in the System Objects module. You can select from one of the predefined themes or customize your own theme color of the Client interface to have your own preferred color, which is black by default. Every Theme has a list of color properties in the Colors palette that can be customized to represent an aspect of the User Interface in Control Center.

Additionally, the Client Themes can be published to all the federating sites.

Configuring a Customized Client Theme in Client

1. From System Objects, select the default Modern Client theme object or to customize your own theme, click **New > Modern Client Theme**. The **Client Theme** palette page appears.



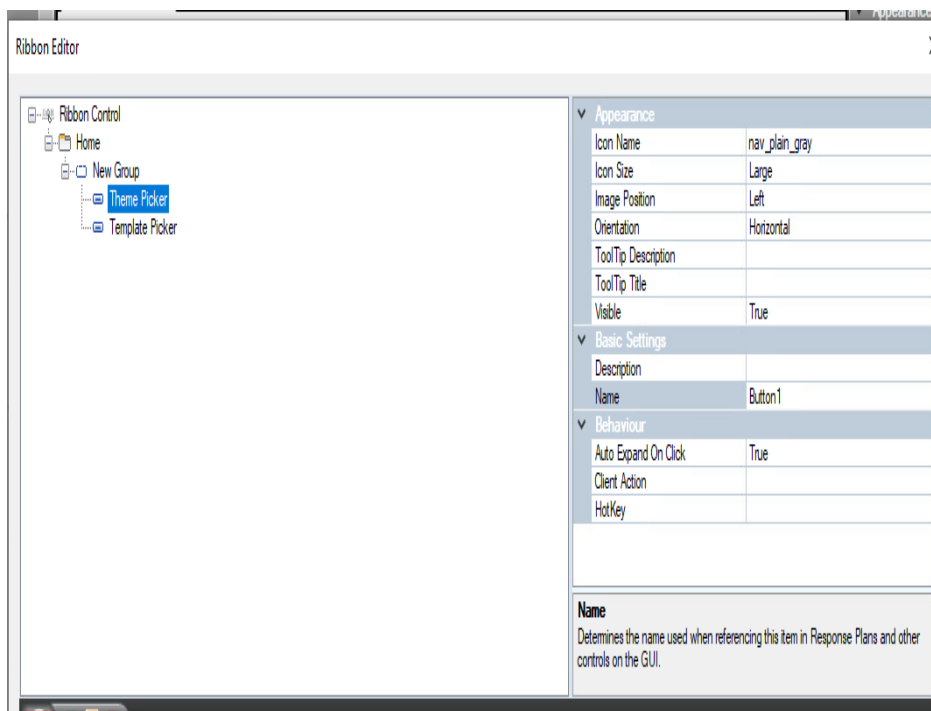
2. To set your own color for one or any of the elements on the User Interface, select the option on the left and click on the required color or drag the **Color Picker** on the right until your preferred color is appears.
3. To apply changes to a specific element of the User Interface, select from one of the below properties:
 - AccentColor – Main color for the theme in Control Center.
 - AccentDarkColor – Darker accent color for the theme.

- AccentMainColor – Affects the color of the hyperlink displayed within System Explorer, for example, the View contacts for this Location.
 - AlternativeColor – Changes color of the primary background. Also used as background of Popups and Dropdowns.
 - BasicColor – Border color of controls in their normal state.
 - ComplementaryColor – Color for elements in disabled state.
 - DefaultforegroundColor – Foreground color
 - HeaderComponent – Color used for background of headers.
 - MainColor – Used as the background for all the main controls.
 - MarkerColor – The color for the text elements that appear on the theme.
 - MouseOverColor – Background of elements that are in MouseOver/Hover state.
 - PrimaryColor – Primary color for most controls that have no direct input in their normal state.
 - SelectedColor – The main color for text or paths which are over elements with accent background.
 - SemiBasicColor – The color of the selected or Hover-over states.
 - StrongColor – Text that is in bold when active, for example, Alarm Stack header.
 - ValidationColor – Used for validation where it is applicable to controls.
4. Alternatively, you can specify the RGB (Red Green Blue) value, if you already know the values for a color property.
 5. To set the main theme for the Client to your preferred color, specify a color property or choose it via the **Color Picker**. The color changes reflect almost instantly, however to have the changes applied permanently, you must modify the **User** object and specify a **Theme** that has the changes.
 6. To specify the theme with the changes, select the **User Object** and then from **Properties> Theme**, select the theme.
 7. Alternatively, the following color variations are available as part of the **Preset Palettes**:
 - Dark – Sets the theme to black.
 - Light – Sets the theme to white.
 - Blue – Retains the theme to white but changes the selection of AccentMainColor to blue theme.
 8. Click **Save** and then restart the Client. The changes applied to the theme are applied to the Client theme.

Using the Theme Picker and Template Picker

Custom theme created and saved using the Modern Client Theme object can be used in the Main Menu by picking the theme from the Theme Picker. The user can launch the theme picker from the Main Menu GUI bound by a client action to a button displayed on the Main Screen. To configure a button to do this, you need to:

1. Go to **System configuration > System Objects**.
2. From the **Graphical User Interface**, double click on the **Main Menu GUI**.
3. From the property window on the right, click on **Custom Menu** items to open the **Ribbon Editor** window.



4. Right click on the **New Group** option and select **Add Button**.
5. In the **Appearance** section on the right window, choose an icon from the icon picker.
6. In the Behavior section
 - o Set the **Auto Expand On Click** to **true**.
 - o Select **Theme Picker** for **Client Action** property.

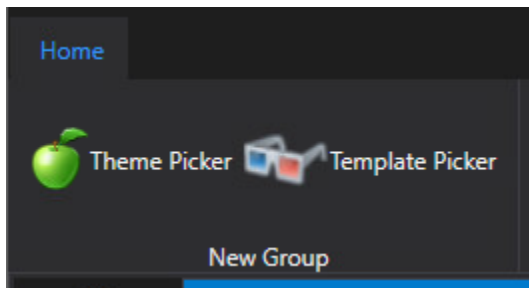
You can also set hotkeys in the hotkeys properties.

7. Click **OK** to save the settings.
8. Restart the client.

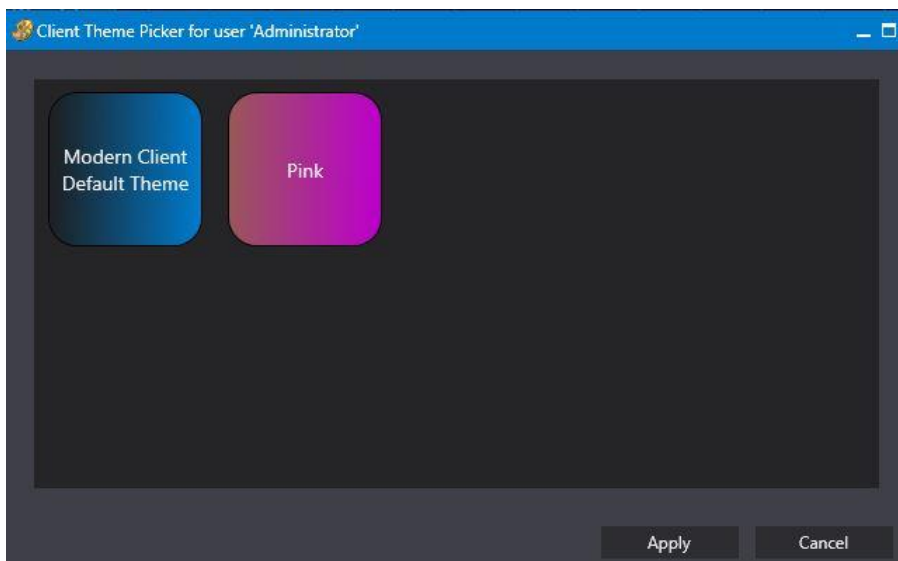
You could follow the same steps to create a button for the template picker as well. In the Client Action property choose the Template Picker instead.

For the Template Picker window to popup on selection, you must have at least two templates saved. When a new client is connected to the system, the template picker will be displayed to the user with the options to choose from. If there is only one template the default will be applied automatically.

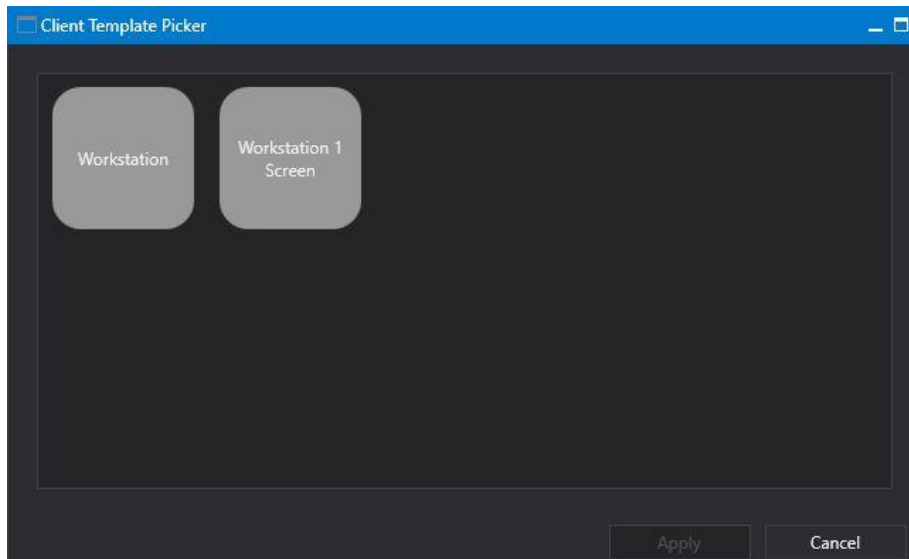
The Main Screen will now look like this:



On clicking on the Theme Picker button, the Theme Picker Window will be displayed with the choices of the themes available.



On clicking on the Template Picker Button. The Template Picker window will be displayed with the choices of template available.



The user can choose the option and click on apply to save changes. Restart the client to see the applied changes.

Configurable Branding

Configurable Branding objects can be used to replace brand imagery and text within Control Center. When combined with Client Themes, customers can better integrate Control Center within their own organization and present a more consistent user experience to their users. This add-on is controlled via license key.

Creating a new Configurable Branding Object

1. Open **System Configuration**. Right click in the center pane and select **New > Configurable Branding** to create a new **Configurable Branding** object and name it appropriately.
2. Double click on the branding object to open the **Branding** window.

The screenshot shows a 'Branding' configuration window with a tree view on the left and a 'Display Value' field on the right. The tree view is expanded to show the following categories and their properties:

- Company**
 - Company Logo
 - Company Url
- Product**
 - Product Name
 - Product Logo
 - Show Product Logo in System Explorer
- Application**
 - Login Page Background
 - Splash Screen
 - Application Button
 - Application Icon
- Tile Layout**
 - Tile Layout Background
 - Tile Layout Image Mode (set to Center)

3. For each property, enter text or select from an available Media object. Any property that doesn't have a value will use the default resources.

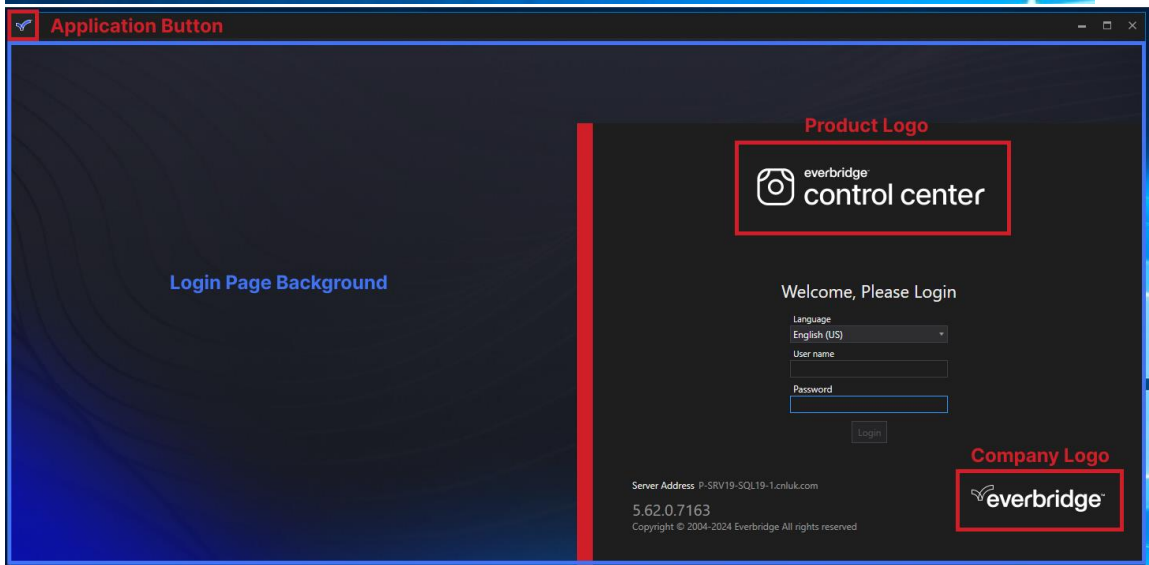
Available properties are:

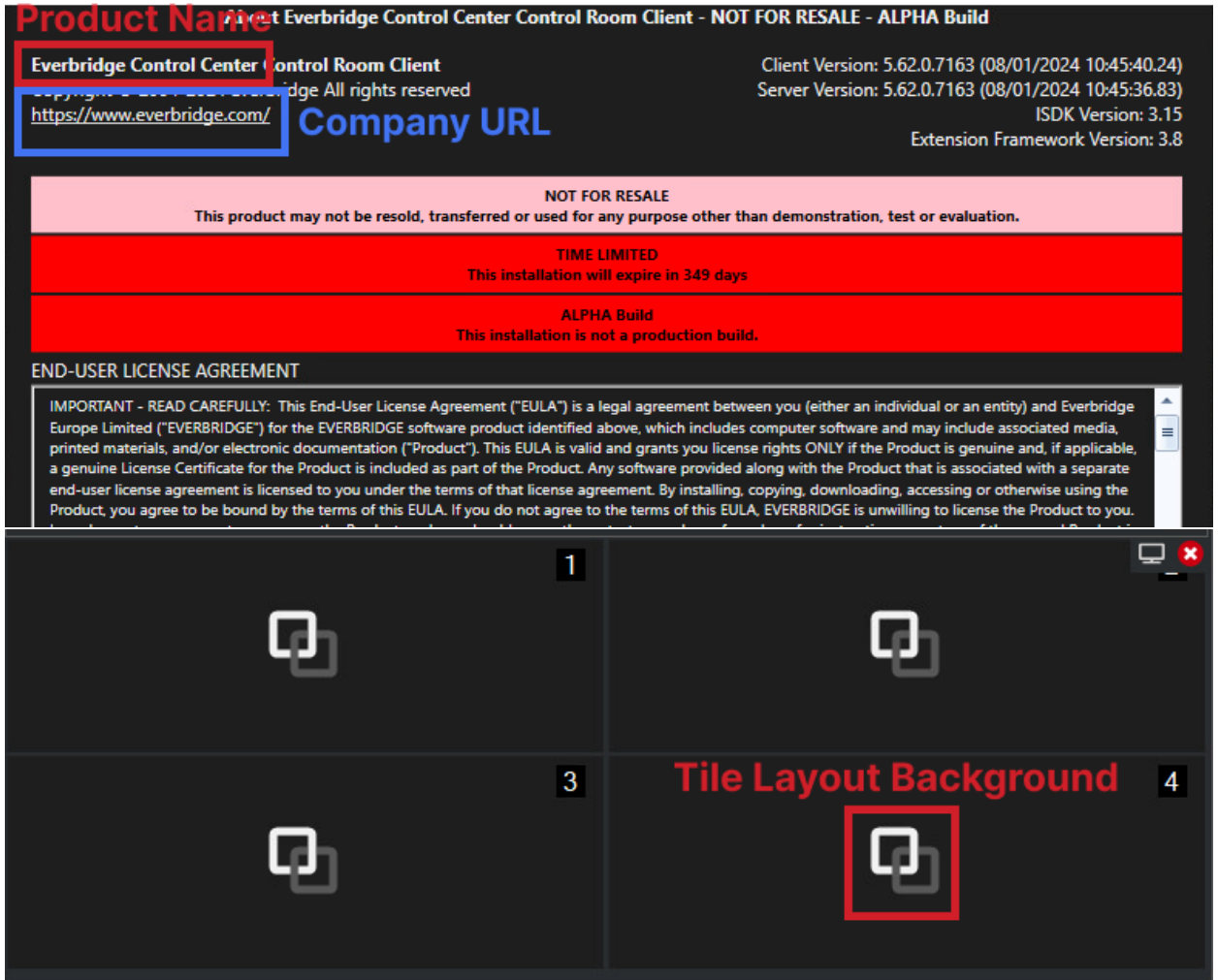
Name	Type	Usage
Company Logo	Transparent PNG	Displayed in the lower right of the login and unlock workstation screens. Default size: 400 x 140 pixels Image will be resized to fit within the default area.
Company Url	Text	Displayed in the 'About' screen.
Product Name	Text	Displayed throughout the product in message box headers and 'About' menu

		<p>items. Maximum 50 characters.</p>
Product Logo	Transparent PNG	<p>Displayed in the top center of the login and unlock workstation screens, as well as the rights elevation screen. Default size: 640 x 220 pixels Image will be resized to fit within the default area.</p>
Show Product Logo in System Explorer	Checkbox	<p>When enabled, the product logo is displayed above at the top of the System Explorer.</p>
Login Page Background	Transparent PNG, MP4, GIF	<p>Displayed on the login and unlock workstation screens. Supports animation including MP4 videos with audio track. Default size: 1920 x 1080 pixels Image will be stretched to fit the default area.</p>
Splash Screen	Transparent PNG	<p>Displayed on first launch before the login screen becomes visible. Default size: 1080 x 720 pixels Image will be stretched to fit the default area.</p>
Application Button	Transparent PNG	<p>Displayed in the top left corner of the main product window. Default size: 32 x 32 pixels</p>
Application Icon	Icon	<p>Displayed in the top left corner of message boxes within the product. Default size: 32 x 32 pixels</p>
Tile Layout Background	Transparent PNG	<p>Displayed whenever empty tiles are visible. Default size: 100 x 100 pixels</p>

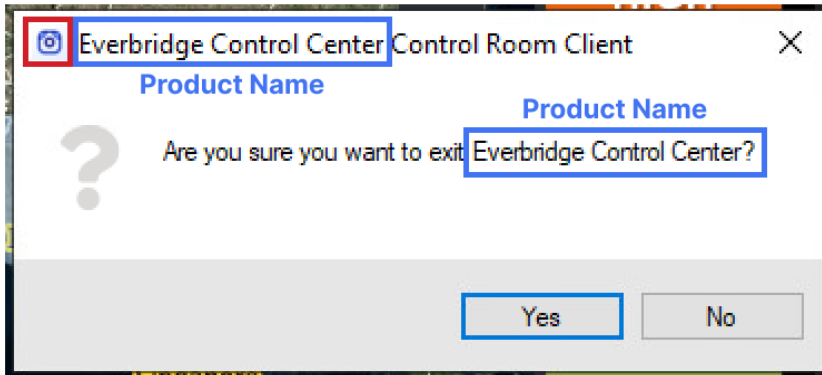
		Image will be resized to fit a 1:1 aspect ratio.
Tile Layout Image Mode	Dropdown	Controls whether the background image is displayed centrally or resized to fill the empty tile. Default = Center

The following screenshots show examples of each resource in the product.



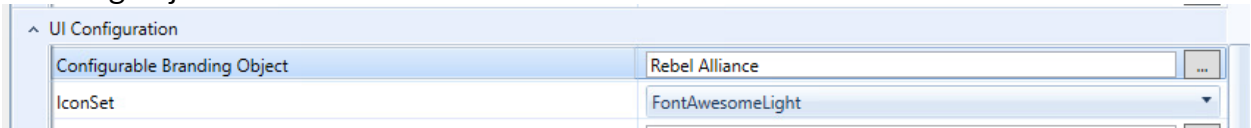


Application Icon



4. Save the **Configurable Branding** object.
5. Open **Global Settings** from **System Configuration**.

- On the **Enterprise Settings** page, in the **UI Configuration** section, there is an option called 'Configurable Branding Object' where you can select from available branding objects to use.



- After selecting an object, press **OK** to save the changes.

The next time a user logs in to Control Center, the selected branding object will be retrieved and stored on that client and the user will see branding changes reflected in the system.

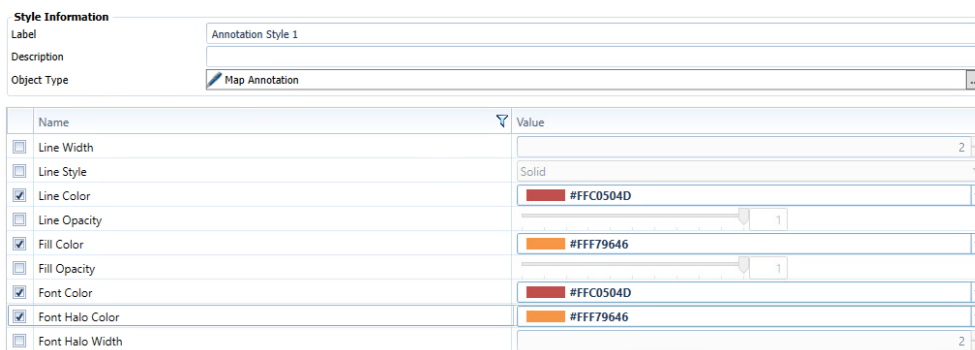
After Control Center is restarted a second time, the stored branding object will be applied to the splash screen and login screen.

Object Style Templates


Object Style Templates can be used to alter the visual appearance of some objects displayed on a scene. Currently the **Geofence** and **Map Annotation** objects are supported.

Creating a new Object Style Template

- Go to **System Configuration**. Right click in the center pane and select **New > Object Style Template** to create a new **Styling** object and name it appropriately
- Double click on the styling object to open the **Styling** window. If you do not already have a style defined, this window appears blank.
- Click on the **Add** button on the bottom of the left pane. A new styling sheet appears on the right.



- Enter an appropriate name for the style sheet
- Enter a description about the style you are working on

13. Select the **Object Type** by clicking on the  button against the **Object Type** parameter and click **OK**.
14. Adjust the styling parameters for the object. Default values will be used for any parameters not specified in the style. The available parameters are shown in the table below:

Name	Value
Line Width	Width of the line surrounding the perimeter of the Object
Line Style	Style of the line surrounding the Object. There are six options available from the drop-down menu to choose from
Line color	Color of the line surrounding the Object. You can choose the color from the palette which is shown by clicking on the field
Line Opacity	Opacity of the line. 0 if hidden and 1 if visible. Sliding between 0 and 1 will set the transparency to the chosen level
Fill color	Color that fills the Object area. You can choose the color from the palette which is shown by clicking on the field
Fill Opacity	Opacity of the fill color of the Object area. 0 if hidden and 1 if visible. Sliding between 0 and 1 will set the transparency to the level chosen
Font Color	Color of the font used by a Label-type Map Annotation. You can choose the color from the palette which is shown by clicking on the field
Font Halo Color	Color of the halo surrounding a Label-type Map Annotation. You can choose the color from the palette which is shown by clicking on the field
Font Halo Width	Width of the halo surrounding a Label-type Map Annotation. You can choose the color from the palette which is shown by clicking on the field

15. Save the **Object Style Template**.

Multiple styles can be added to the template. Once an Object Style Template has been created, additional styles can be added to it by double-clicking on it from **System Configuration**.

Keyboard Shortcuts for Windows Client

The HotKeys Mappings functionality enables you to configure Keyboard Shortcuts to use in Control Center. For example, you can add new mappings, delete existing mapping, and modify existing mappings. Additionally, you can assign a set of Hot Key mappings to one or more Control Center Clients, allowing Clients to share mappings or use mappings specific to each Client. If no specific mapping of hot keys is configured for a Client, then the system hot key mappings will be applied.

Before modifying Hotkey Mappings, Everbridge recommends that you identify the Windows Shortcut Keys configured on your computer to avoid assigning the same key combination in Control Center.

By default, the following System Hot Key Mappings are available.

Keyboard Shortcut	Context	Action
Windows+PageUp	From anywhere within the Windows Client	Opens the System Configuration window
Windows+PageDown	From anywhere within the Windows Client	Opens the Setup Display window
Windows+End	From anywhere within the Windows Client	Shows the confirmation dialog to exit.
Windows+Home	From anywhere within the Windows Client	Locks the system you are working on
Windows+A	From anywhere within the Windows Client	Opens the Admin Interface

Configuring Mapping of System Hot Key Mappings

To modify mapping of the system shortcut keys:

1. Open **System Configuration > System Objects**. The **System Objects** pane appears.

2. Double-click **System HotKeys** to open the system default mappings for shortcut keys.
3. In the **Hot Key** list, choose the hot key that you want to assign, for example, 0 (zero) and then select a key modifier such as Shift from the Key Modifier list.
4. In the **Operation** list, select the operation that you want to use the key combination with, for example, **LockSystem**.
5. Restart the Control Center Client.
6. Use the shortcut key mappings that you just configured: 0 + Shift. The shortcut key's configured function should take into effect, in this case, the System should get locked now.

To add a new mapping:

1. In the **System HotKey Mappings** dialog, click **Add Mapping**.
2. A new set of drop-down boxes to select key combinations from are added to the page.
3. Select the required combination of hot keys using the available drop-downs to assign the shortcut mapping. For more information, see how to modify the existing mapping of system shortcut keys in the previous section.
4. Save the changes.

Notes:

- To delete an existing mapping, select the row of mapping that you want to delete, and click Delete Mapping.
- You **MUST** restart any Control Center Client which is using the selected set of Hot Key Mappings for the changes to take into effect.

Use from the following list of available keys along with the key modifier to assign shortcut key mapping:

Hot Key selection/ Windows keyboard keys		Key Modifier
<ul style="list-style-type: none"> • Alt+None • Back • Cancel • Clear • Ctrl+Alt+Shift+None • Ctrl+None • Del • Down 	<ul style="list-style-type: none"> • F9 • F10 • F11 • F12 • Help • Home • Ins • Left 	Alt Control None Shift Windows

<ul style="list-style-type: none"> • End • Enter • Escape • Execute • F1 • F2 • F3 • F4 • F5 • F6 • F7 • F8 	<ul style="list-style-type: none"> • None • PgDn • PgUp • Print • Right • Scroll Lock • Select • ShiftKey • Shift+None • Space • Tab • Up 	
---	---	--

Note: None indicates that no shortcut key is associated with the selected menu item.

Control Center modules that use shortcut keys

Currently, the following modules use shortcut keys.

Operation	Use to...
AdminInterface	Open the Admin Interface
ElevatedUserLogOff	Logs off an elevated user session
LockSystem	Lock the application
Logout	Logs off the User
QuickSearchEntry	Displays a Search box for entering a search value when the System Explorer is open
SetupDisplay	Open the Display Configuration dialog
SystemConfiguration	Open the System Configuration dialog
ToggleSystemExplorer	Switch the System Explorer tree on and off

Tile Layout / Video specific commands

These hot keys will only apply if you have a tile selected for displaying video.

Hot Key selection	Use to...

ToggleFullScreen	Switch between fullscreen mode and normal mode for a selected tile
TogglePlaybackAndLive	Switch between playback and live for a selected tile
TogglePlayPause	Switch between Play and Pause for a selected tile (only applicable if the video is in playback mode)

Client Actions

You can link hotkeys to menu buttons on the main menu while commissioning. You can assign shortcut keys to the following Client Actions:

- Client Template Picker
- User Theme Picker

Alarm Handling

The Administrator has the ability to configure hotkeys for various tasks to handle alarms. The various operations available for alarm handling are as listed below.

Hot Key selection	Use to...
Handle Alarm	This will execute the same logic as when the user clicks the Unhandled link in the alarm stack. Any Response Plan associated with the Alarm Handled action will be executed and tasks defined within the Response Plan, such as navigate to location and displaying CCTV, will be processed in the same way.
ProcessGuidanceConfirm	This will execute the Confirm action in the current process guidance step
ProcessGuidanceNo	This will execute the No action in the current process guidance step
ProcessGuidanceYes	This will execute the Yes action in the current process guidance step
ProcessGuidancePark	This will execute the Park action in the current process guidance step

Adding a New Hot Key Object

In addition to the System Hot Keys Mapping object, you can also add your own customized set of hot keys.

To add a new hot keys object:

1. In **System Configuration**, right-click anywhere in the middle pane, for example the **Devices** folder and select **New > Hot Key Mappings**. A new **Hot Key Mappings** object appears in the list of objects.
2. Specify a name for the new **Hot Key Mapping** and press **Enter**.
3. Double-click the new **Hot Key Mappings** object to open it. The new **Hot Key Mappings** appear in the **Design Surface**.
4. Create new mappings using the **Add Mapping** button.

Assigning Hot Key Mappings to the Client

By default, the **Hot Key Mapping** for the Control Center client is left blank, in which case the **System Hot Key Mapping** will apply. You can choose to assign the newly created **Hot Keys Mapping** object or the default System Hot Keys mapping depending on your requirement.

To assign the hot key mapping to a client:

1. Open **System Configuration > Computers**.
2. Select the Windows Client that you would like to assign the hot key mappings to.
3. In the **Properties** pane, click the **Hot Keys Mapping** button. In the **Search Objects** dialog, the hot keys object appears.
4. Locate the hot keys mapping object, for example, **System Hot Keys**, and click **OK**.
5. The selected hot keys mapping is assigned to the chosen client. You can assign a different set of hot key mappings for each client in the same way as long as they are connected to the same server.

When assigning a different set of hot key mappings to a client, make sure to restart the client for the changes to take effect.

Event Flood Prevention/Rate Limiting

Control Center is designed to gather events from various devices, process it and raise alarms appropriately to notify the user. If the devices are raising events at a very high frequency, the system may get clogged up and slow down the raising of alarms in response to the event.

For example: if there are 100 door closed events and a fire alarm event queuing up after that, the system would have to process 100 door closed events before processing the fire event, resulting in a delay to report the critical fire alarm to the user.

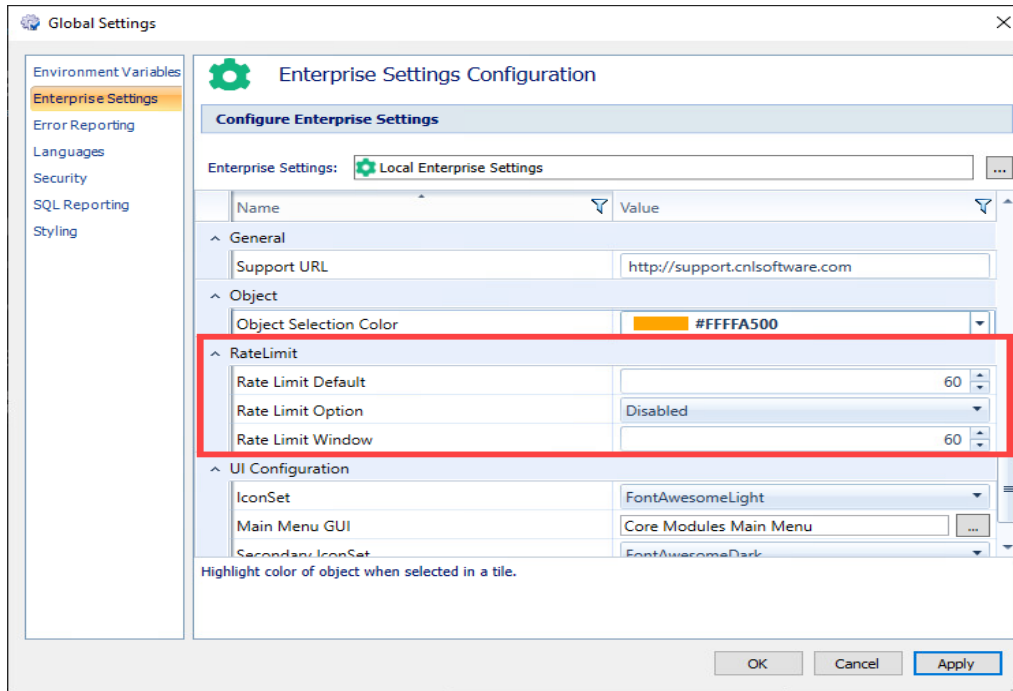
To provide an active and intelligent response to this situation, Control Center is now equipped with the rate limiting mechanism. If the device is configured for rate limiting, the events being pushed into the system by the device will now be grouped. A pre-defined time window is set by the administrator over which rate generation is measured. When the number of events received from the device during the window exceeds a threshold, then the device enters rate limiting mode. Instead of processing every event, the system will now maintain a count, per event type, of events received and process a single event with the event count recorded against that event.

For example: If the rate limit time window is set to 10 seconds and 100 door forced events occur in that time frame, only one event with count equal to 100 is recorded. This will result in only one event being processed and one alarm being triggered. This will make the system more efficient by making it possible to trigger only one alarm in response to 100 similar events and discarding the rest, increasing the chance of responding quickly to critical events. This not only reduces the latency but also increases the chance of quickly responding to the alarms.

Configuring Rate Limiting in Control Center

For a device to be rate limited it needs to be configured in the Global Settings by the administrator as follows:

1. Go to **System Configuration** and click on the **Global Settings** tab on the Top Ribbon toolbar to open the **Global Settings** window.
2. Click on **Enterprise Settings** in the left pane options.
3. In the **Enterprise Settings Configuration** window, you will see three options as shown in the picture below.



Parameter	Description	Value
Rate Limit Default	Default Rate Limit set to events coming from a device	Any positive integer. Default value is set to 60
Rate Limit Option	Option that can be chosen to configure the rate limit	There are three options: <ul style="list-style-type: none"> ○ Disabled – Rate limiting option will be disabled ○ Enabled – Rate Limit option will be enabled with the rate set in the properties window of the Device ○ EnabledUsingDefault – Rate limit will be applied with the rate set in the Rate Limit Default variable mentioned above

Rate Limit Window	The time frame measured in seconds over which the rate measurement is made	Any positive integer. Default is set to 60
-------------------	--	--

4. Click **Apply** to save the settings.
5. Restart the application for the settings to be activated.

This will be the default settings applied to all devices monitored by the Control Center. If you choose to have a different rate limit for a device, it can be done as described in the steps below:

- a. Go to **System Configuration** and navigate to the location of the device you wish to change the rate limit for.
- b. On the **Properties** window, change the **Rate Limit** field value to the desired value.

Properties	
Door Count	3
Enabled	True
Event Interval	00:00:10
Image Set	Standard
Initial Camera Count	9
Label	Training Server 1
Lock Dwell Time	00:00:03
Rate Limit	10
Room Busy Threshold	3
Simulate Events	False

- c. Go to **Global Settings** window and choose **Enterprise settings** from the left pane options.
- d. Set the rate **Limit Option** to **Enabled**.
- e. Restart Control Center.

The rate limit specified here will only be applied for this device. You can always roll back to default settings by selecting the **EnabledUsingDefault** option.

Understanding the Working of Rate Limit Mechanism

Though the rate limit settings are made globally to be applied to all devices in Control Center, the events coming from various devices are individually categorized under the device name. The classification and grouping of events are done separately for every device.

To view the list of events from a device:

1. Go to **System Configuration** and select **Services** from the left pane options.
2. Open the **Connection Manager Service** by double clicking on it.
3. **Device Events** window opens to display the list of events.

Event Raised Time	Device Type	Device	Event	Event Count
12/6/2018 12:00:10 PM	Training Server	Training Server 1	CredentialSwiped	89
12/6/2018 12:00:10 PM	Training Server	Training Server 1	PerimeterBreached	1
12/6/2018 12:00:10 PM	Training Server	Training Server 1	PerimeterBreached	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	RoomBusy	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	RoomBusy	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	RoomBusy	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	RoomBusy	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	RoomBusy	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	DoorStateChanged	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	DoorStateChanged	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	DoorStateChanged	1
12/6/2018 12:00:09 PM	Training Server	Training Server 1	DoorStateChanged	1

You can observe that the events are individually listed before the rate limit is initiated. Then the events of similar type are grouped together with the event counter being incremented.

To have a closer look at the events that were handled by the rate limit mechanism

- Go to **System Configuration** and select **Computers** on the left pane options.
- Double click on the **Rules Engine Server**.
- The **Rules Engine Events Viewer** window opens to display the list of events.

Event Processed Time	Event Raised Time	Object Type	Object	Event	Event Co
12/6/2018 12:27:32 PM	12/6/2018 12:27:32 PM	ConnectionManager	Default	RateLimitedDeviceEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	PerimeterBreachedEventArgs	89
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorForcedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorForcedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ConnectionManager	Default	RateLimitedDeviceEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorForcedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorStateChangedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorStateChangedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorStateChangedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorStateChangedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorStateChangedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	CredentialSwipedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	CredentialSwipedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	CredentialSwipedEventArgs	1
12/6/2018 12:27:22 PM	12/6/2018 12:27:22 PM	ITrainingServer	Training Server 1	DoorForcedEventArgs	1

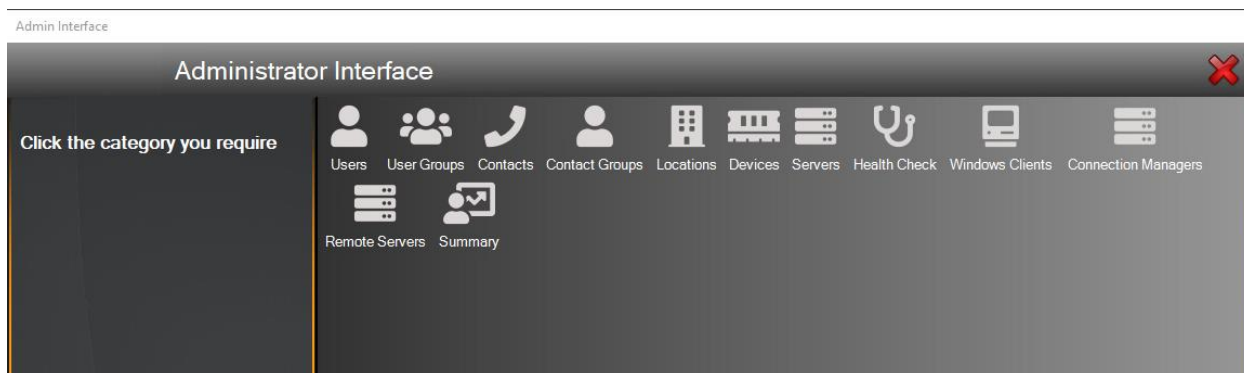
The two entries from the connection manager is when the rate limit mechanism was initiated and ended. This status can be seen in the property window when the entry is selected.

: Properties	
Event Properties	
ConnectionManager	908428df-5822-44a1-b576-9438ecel
DateTimeRaised	12/6/2018 12:27 PM
Device	72b0aef4f358-4b11-b1cd-817a46db
DeviceTypeName	CNI_IPSecurityCenter_Driver_Training
IsRateLimited	True
Misc	
EventId	36252d47-52f9-e811-892c-000c293
SenderEventId	ae4c85e6-a9df-4a2e-964d-3a58952
SenderId	908428df-5822-44a1-b576-9438ecel

This property will be set to false when it is out of the rate limit window.

Administrator Interface

The Administrator Interface allows for simple administration of system components, that are available in System Configuration but not accessible to an end user. For example, you can access user management, device status, location management and so on from the Administrator Interface.

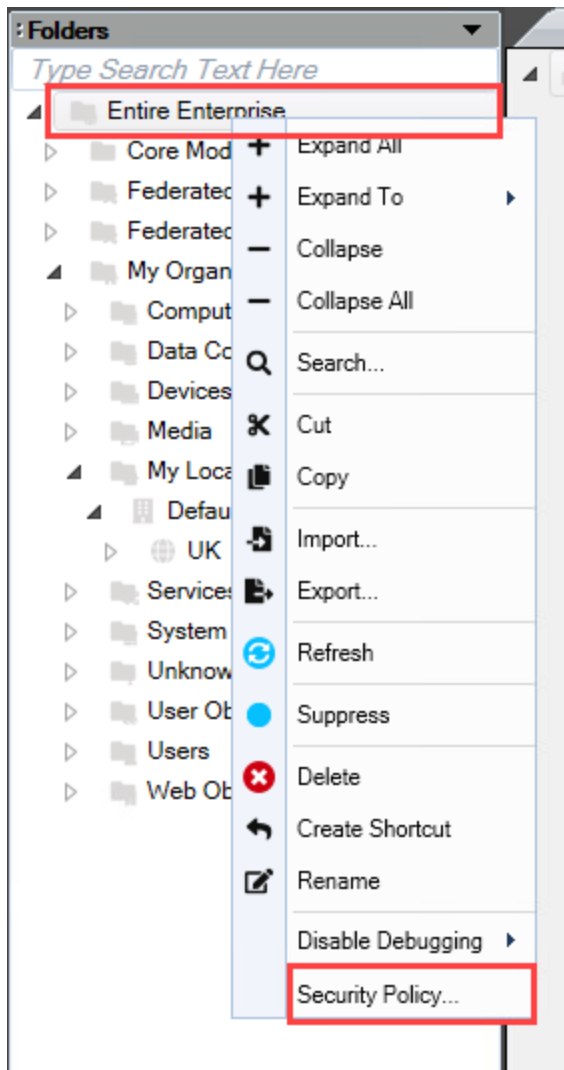


Accessing Administrator Interface

You must add the user accounts to the appropriate security policy for the new users to access the Administrator Interface. By default, the Administrator user account (root) and all members of the Administrators Group have access to the Administrator Interface.

To grant a new user access to the Administrator Interface:

1. From **System Configuration**, right-click on the **Entire Enterprise** folder and select **Security Policy**. The Security Policy Editor opens.

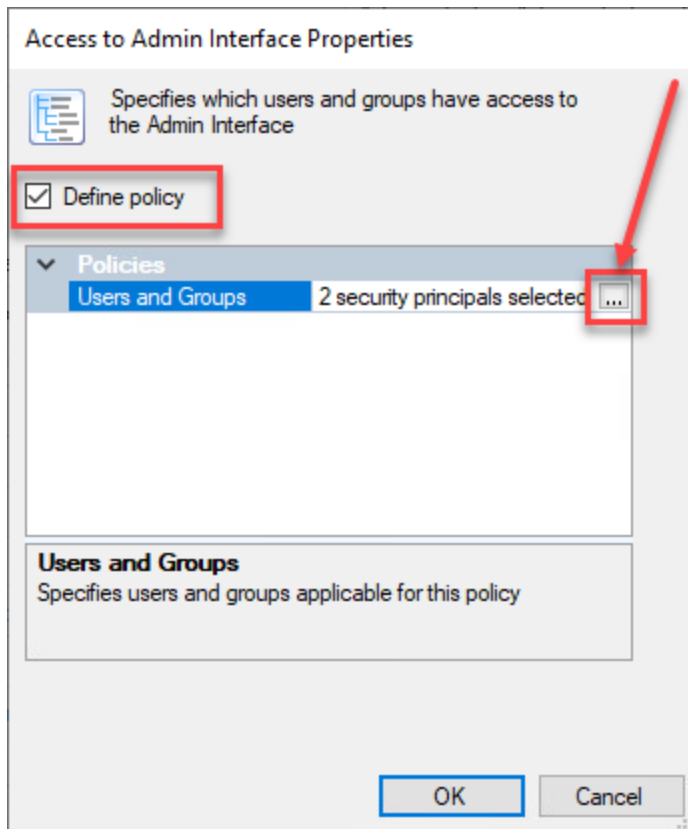


2. Expand **Security Policies > User Policies**. All security policies are displayed on the right.

A screenshot of the 'Security Policies (Entire Enterprise)' window. The left sidebar shows 'Security Policy Types' with 'User Policy Types' selected. The main table lists various policies. The first row, 'Access to Admin Interface', is highlighted with a red box.

Policy	Security Setting	Defined for this Folder
Access to Admin Interface	Administrator, Administrators	False
Access to Response Plan Designer	Administrator, Administrators, Response Plan Designers	False
Access to Setup Display window	Administrator, Administrators	False
Access to System Configuration	Administrator, Administrators	False
Access to the Map Note Editor	Administrator, Administrators, Users	False
Account Expiration Notification	Disabled	False
Add Clients	Administrator, Administrators, Account Administrators	False
Allow Alarm Handling Takeover	No Security Principals Defined	False
Allow Bulk Resolution of Alarms	Administrator, Administrators, Users	False

3. Double-click the **Access to Admin Interface** policy to provide access to the user. The **Access to Admin Interface Properties** dialog appears.



4. Select the **Define policy** check box and then click the ... button to select the users. A Collection Editor appears.
5. Click **Add**. The **Search Objects** dialog appears.
6. In the **Search Objects** dialog, search for the users that should be granted access to the Administrator Interface.
 - a. In the **Label** field, type the username and click **Find Now**
 - b. Select the user from the list of search results that is displayed.
 - c. Click **OK**.
7. Click **OK** to confirm that the new user has been added to the list of accounts allowed to access Admin Interface. Then click **OK** to close the **Access to Admin Interface Properties** window. The new user now has access to the Admin Interface.

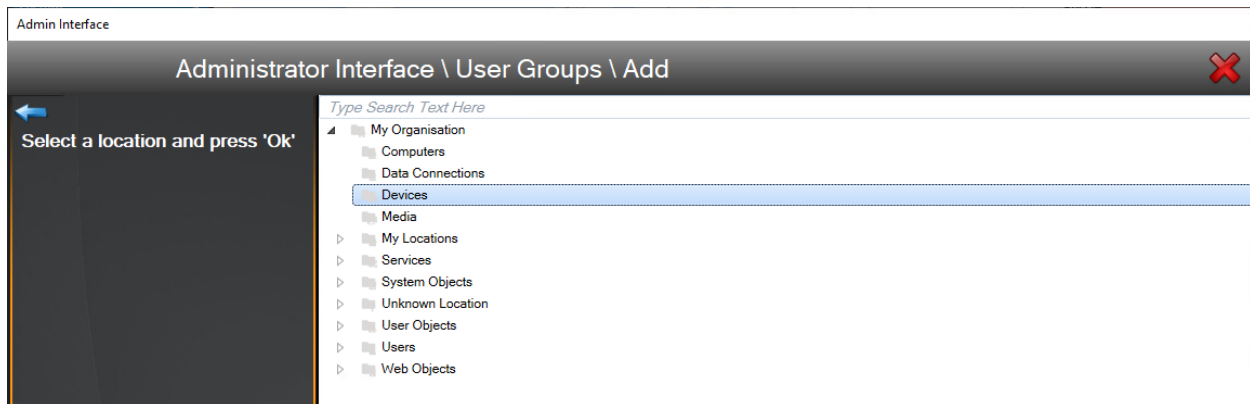
If the user is logged in while the change is made, then they must log out and log back in for the change to take effect.

Users and Users Groups

The **User Groups** screen provides the ability to create user groups and users. You can add users or remove them from a user group, which provides a way to control what access each user has. You cannot edit security permissions from the Admin Interface.

To create a new user group:

1. From Admin Interface, select **User Groups**. The **Administrator Interface \ User Groups** dialog appears.
2. Click **Add**.
3. Enter the name of the user group and optionally a description.



4. Select the location where the user group should be stored, typically the folder called **Users** and then click **OK**.

Additional Operations in User Group

You can perform the following additional operations with users and user groups:

- **Add** – Create users and user groups.
- **Edit** – Edit existing users and user groups.
- **Delete** – Delete user groups or users.
- **Enable** – Enable disabled users.
- **Disable** – Disable enabled users.
- **Membership** – Configure membership for user groups.
- **Wizard** – Creates user groups using the wizard (not applicable to Users).
- **Status** – Displays the online status of the existing user groups.
- **Reset Password** – Used for resetting passwords. This option is available to Users only.
- **Reset Lockout** – Used for resetting a locked-out user. This option is available to Users only.

Creating Users

You can create users in both Admin Interface and System Configuration. To create a user:

1. From the Admin Interface, select **Users** and then click **Add**.
2. Enter the details for the user account and click **OK**.

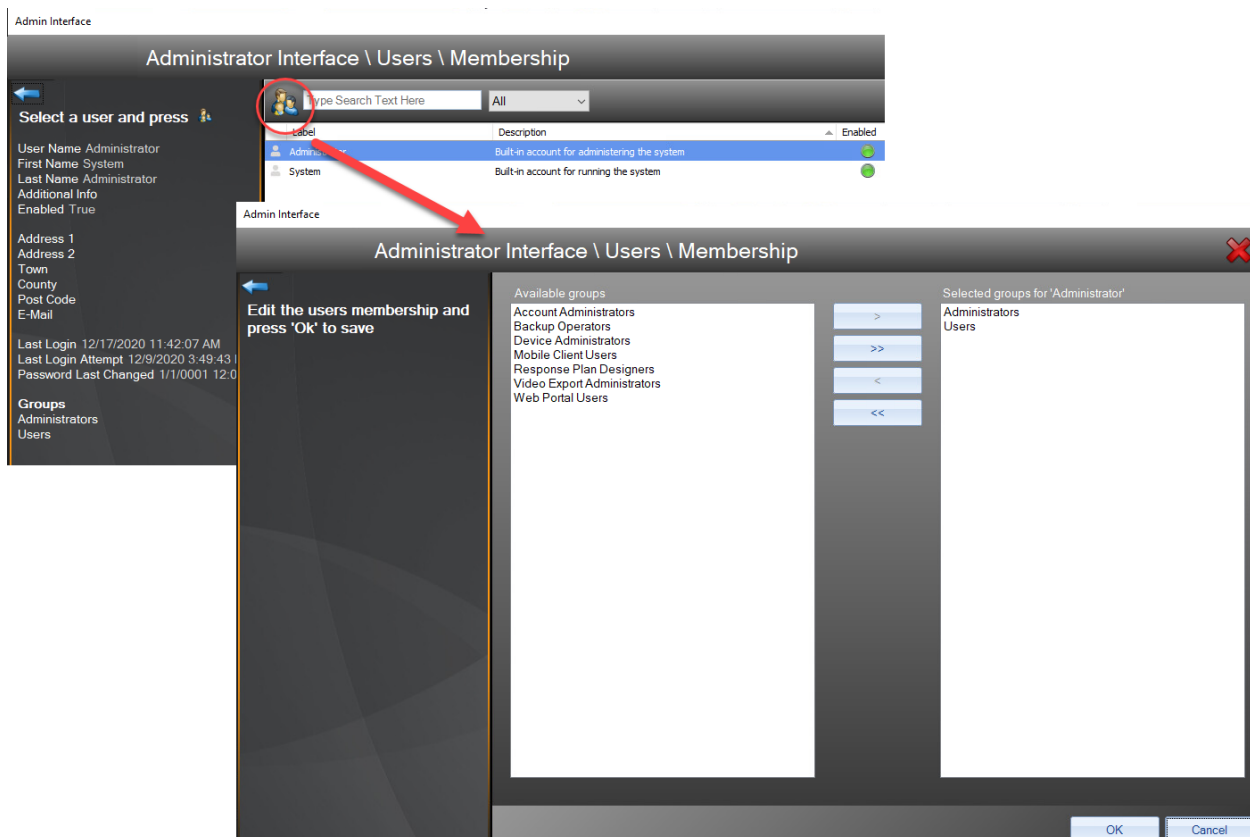
The password must adhere to the site password policy.

User Group Memberships

By default, all newly created user accounts are members of the default user group called **Users**. You can set up security permissions at the Group level in System Configuration and manage user permissions in the Admin Interface by moving users into the appropriate groups.

To modify user group memberships:

1. Select the **Membership** option on the **Users** page.
2. Highlight the user in the list of users and double-click to open the membership page.



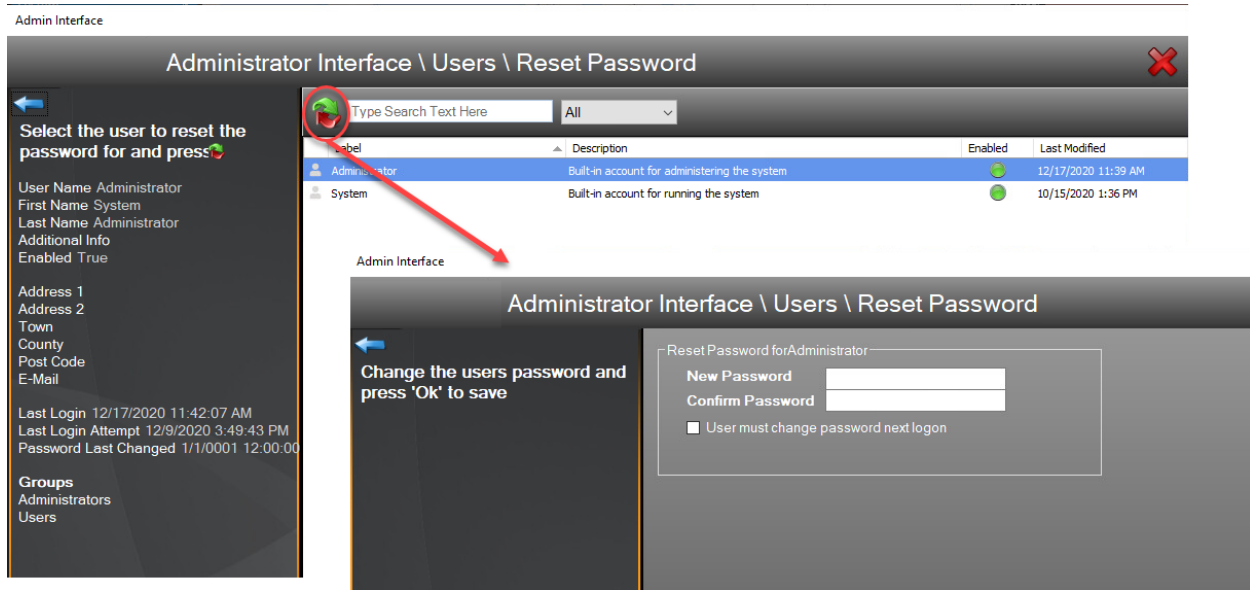
3. Select the groups that the user should be a member of and click **OK**.

Managing an Account

Once an account has been setup in for you in Control Center, you can maintain it from the Admin Interface to perform common tasks such as resetting the user’s password and resetting a locked-out user. Typically, you get locked out if you entered an invalid password several times.

Resetting a Password

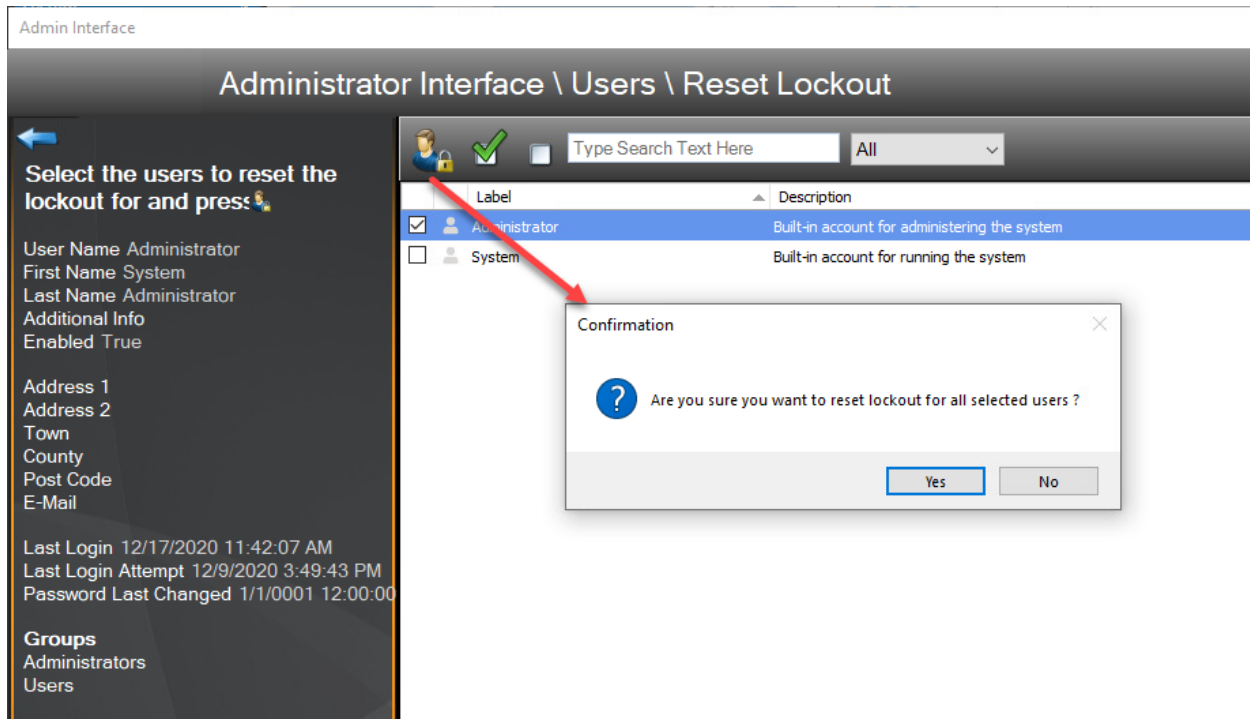
The **Users** section of the Admin Interface provides an option to **Reset Password**. Select the specific user in the list of users and then click the **Reset** button in the top-left corner. Enter a new password for the user.



The new password must comply with the site password policy.

Resetting a locked-out user

To reset a locked-out user, select the specific user in the list of users and then click the **Reset** button on the toolbar menu.



Contacts and Contact Groups

Contacts and contact groups enable you to add a contact that has similar fields to a User but without the ability to log in to Control Center. You can store contacts in a Control Center solution to provide details of who to contact in various situations. You store contacts under a location to enable you to quickly access them when required. In addition, you can store various details against each contact.

To create a new contact group:

1. From the Admin Interface, select **Contact Groups**. The **Administrator Interface \ Contact Groups** dialog appears.
2. Click **Add**. The **Add** dialog appears.
3. Enter the name of the contact group.
4. Select the location where the contact should be stored, typically the folder called **Contacts** and click **OK**.

Additional operations in Contact Groups

You can perform the following additional operations with Contacts and Contact Groups:

- **Add** – Create contacts and contact groups
- **Edit** – Edit existing contact and contact groups
- **Delete** – Delete contact groups

- **Enable** – Enable disabled contact groups
- **Disable** – Disable enabled contacts
- **Membership** – Configure membership for contact groups.
- **Status** – Displays the status of the existing contact groups.

Adding Contacts

To create a contact:

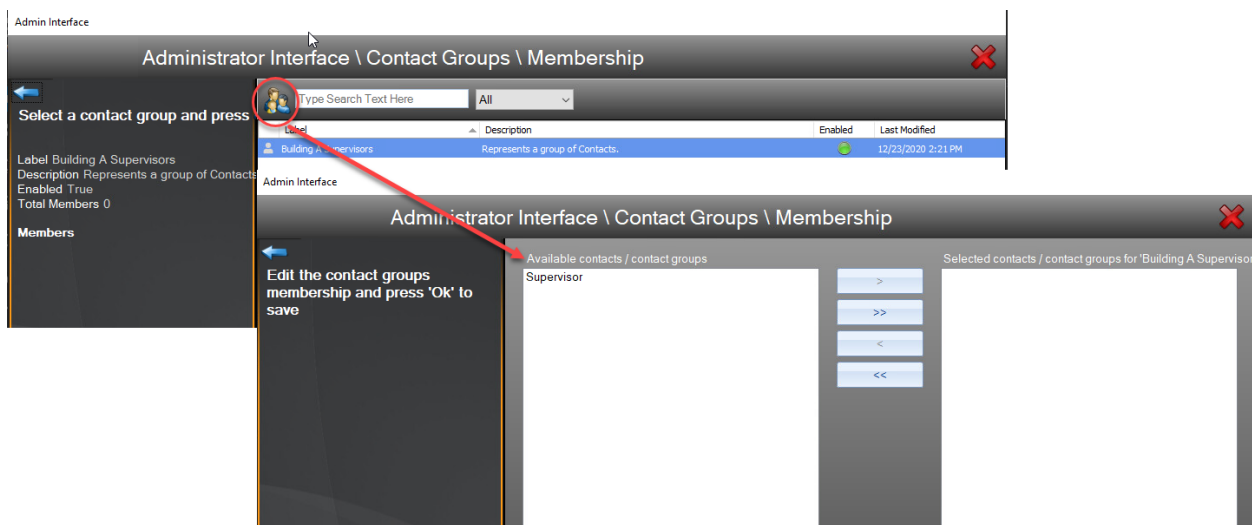
1. From the Admin Interface, select **Contacts** and then click **Add**.
2. Enter the details of the new Contact. **Label, First Name, Last Name** and **Location** are required fields.
3. Click **OK** and then click **Save** when prompted. The newly added contact should be visible when clicking **View Contacts for Location** in System Explorer.

Contact Group Memberships

Contacts cannot log into Control Center on their own. They are mainly there to be notified in the event of an issue. For example, a contact might be a member of the management group, belong to a certain building group, such as the fire wardens group. By default, a new contact is a member of the default contact group.

To modify contact group memberships:

1. Select the **Membership** option on the **Contact Groups** page.
2. Highlight the contact in the list of contacts and double-click to open the membership page.



3. Select the contact groups that the contact should be a member of and click **OK**. The remaining options are the same as Users and User Groups.

Managing Locations

Use locations to create or edit locations, sub locations and plot devices in Control Center. A tree control is displayed when you log in to the Control Center Client for the first time allowing you to select an individual location from the location hierarchy. Typically, you have a single top-level location and then several locations below that.

Editing Locations

You can assign schematic or geographic scenes when creating or editing a location.

To add or edit a location:

1. From the Admin Interface, select **Locations**. The **Locations** page appears.
2. Click **Edit Locations**. The **Edit Locations** page appears.
3. Expand the **My Locations** tree and perform any one of the following options:
 - To add a location, select the parent location in the tree and click **Add**.
 - To edit a location, select the location in the tree and edit the details.
 - To move a location, select the location in the tree and use the drag and drop operation to move it to the target location.

Use the built-in Search functionality to quickly find a required location. The search results automatically update with each new character entered.

4. When you click **Add**, a new location is created in the Locations tree below the selected folder\location and the Location fields become active.

Fields	Description
Address1, 2 & 3	The first, second, and third line of the address.
Town	The town of the location.
County	The county of the location.
Postcode	The postcode of the selected location.
County	The county of the selected location.
Considerations	Additional considerations, if any.
Phone number	The Phone number of the location, if applicable.

Location Type	The Location Type of the selected location. For example, Country, Region, Site, Building, Floor, Room, Zone and Customer.
Default Scene	Select the button to associate scene with this location.

Deleting a location is not possible from the Admin Interface. Therefore, to delete a location, you must delete it from System Configuration.

You can also optionally create a geographic or a schematic scene for that location by selecting the appropriate option from the Location Default Scene dialog.

5. Click **Save** to save the changes.

Plotting devices

Once you have defined a location and assigned a scene, you can plot devices into each of the scenes as required.

To plot devices:

1. From the **Admin Interface**, select **Locations**. The Locations page appears.
2. Click **Plot Devices**. The Plot Devices page appears.
3. Select a location and then wait for the scene to appear.
4. Drag and drop the device that you want to plot on the selected scene.
5. Select the device and view the Properties grid to edit the appearance and viewshed properties in case the device is a camera.

By default, the following properties are displayed when you select a scene, however some of the options are different depending on the type of scene selected, for example Background Type:

Appearance	
Alarm Stack View option	Select from the following options to determine how the alarms are plotted on the map from the Alarm Stack view: <ul style="list-style-type: none"> ○ None – No alarms appear plotted on the map. ○ All – Alarms that are visible on at least one of the user's visible alarm stacks. ○ CurrentView – Only alarms that are visible in the currently selected Alarm Stack View are displayed.
Background Type (only for Schematic Scenes)	Click the background type for a schematic scene. The options available are:

	<ul style="list-style-type: none"> ○ Media – Select a media object that is already available within the system. ○ NetworkShare – Select a media from your network folder by clicking the button that appears next to the field.
GIS Layers	<p>Select the layer from the System Layers list.</p> <p>You must first assign a GIS layer in the GIS Layer Manager from System Configuration to be able to select a GIS layer in this drop-down.</p>
Layers	Click the Layers option to edit the layers for a scene.
Lock Extents	Select True to lock the extents of the map thereby preventing users from panning or zooming, for example.
Pan to Location on Selection	Select True or False to determine if the map pans to a location if selected in the System Explorer and that location is plotted on the currently displayed scene. This option is particularly useful where many locations are plotted on the same scene.
Scene Search Mode	<p>Where a scene has many devices plotted, it is useful to allow the user to search for a plotted object. To enable the Scene Search Mode:</p> <p>Set search mode to AssetOnly. A small search box will appear at the top of the scene which allows a user to find a plotted object. Geocoded searches are not supported in Control Center.</p>
Zoom to location on Selection	Select true or false to determine if the map zooms to a location zoom level if it selected in the System Explorer and that location is plotted on the currently displayed scene.
Zoom to Max Extent	Zooms the map to the full extent of the data on load.

The following properties are available when you select a device:

Appearance

Base Object Label	Default label of the object.
Custom Icon	When the Use Custom Icon is set to true, you can set the custom icon in the Icon Picker dialog. For more information about setting custom icons.
Device Type	<p>Select the type of device. The options are:</p> <ul style="list-style-type: none"> ○ Camera ○ Door ○ Reader ○ Firehead ○ Temperature ○ Pressure ○ Location ○ Other
Has Viewshed	Select true to enable viewshed for the selected device.
Hide Icon	Select true to hide the icon from the map. This setting overrides all other visibility settings.
Icon Size	Select the size of the icon. The options are: Small, Medium, Large.
Icon Visibility	<p>Determines the icon visibility on the map. Specify when the icon should be visible based on the following options:</p> <ul style="list-style-type: none"> ○ Always – Always visible. ○ Hover – Visible only when you hover the icon. ○ Alert – Visible during an alert. ○ Never – Invisible.
Rotation	Specify whether to rotate the icon on the map by dragging the slider.
Use Custom Icon	Select True or False to use a custom icon instead of the default icon.
Visible Objects Search Radius	Specify the radius of the search used for visible object mapping. The Visible Object Mapping is mainly set for a PTZ device.

Text Appearance	
Font Color	The font color on the label.
Font Opacity	The opacity of the label, where 0 is transparent and 1 is opaque.
Font Size	The font size on the label.
Horizontal Alignment	The horizontal alignment of the label, for example: <ul style="list-style-type: none"> ○ Center ○ Left ○ Right
Label Halo Color	The color of the halo on the label. A halo is an expanded region around the text that can make the text stand out more.
Label Halo Width	The width of the label halo that controls how much of a halo surrounds the text.
Label Offset X	Applies a horizontal shift to the label position. Positive values shift the label to the right and negative values shift the label to the left.
Label Offset Y	Applies a vertical shift to the label position. Positive values shift the label down, negative values shift the label up.
Label Visibility	The behavior of the label visibility on the map.
Leader Line Color	The color of the leader line and its box. Only visible if the Show Leader Box field is set to true.
Show Leader Box	Displays a box around the label when set to true. This makes the label stand out more.
Show Leader Line	Displays a line that joins the label to the asset when set to true. To view the leader line properly, ensure that the label is positioned away from the asset using the offset properties.
Vertical Alignment	The vertical alignment of the label: <ul style="list-style-type: none"> ○ Top ○ Center ○ Bottom

Width Label before text wraps	Define the Width of the label, which allows the label text to be wrapped.
Viewshed Appearance	
Bearing	Set the direction at which the viewshed is pointing in degrees from north using the slider.
Distance	Set the distance of the camera viewshed in meters for geographic scenes, and pixels for schematic scenes.
Opacity	Set the opacity of the viewshed, where 0 is transparent and 1 is opaque.
Search Mode	The search mode that is used for Visible Object mapping. The available modes are Viewshed and Radius.
View Angle	The width of view either side of center in degrees.
Viewshed Color	Set the color of the viewshed.
Visibility	Visibility style of the viewshed. For example, Always, Hover, Alert, Never.
Visible Zoom	The zoom setting at which the viewshed becomes visible.

6. Click **Apply** to save the changes.
7. Click **Close** to close the Admin interface.

Managing Devices

Use the Devices option to manage devices, for example to enable and disable devices, view the status of the device, and set an existing device against a new location.

To enable/ disable a device:

1. From the Admin Interface, select **Devices**. The **Devices** page appears.
2. Click **Enable**. The **Devices Enable** page appears listing the devices in the system based on the filter options.

Admin Interface

Administrator Interface \ Devices \ Enable ✖

Mark the devices you wish to be enabled and press ●

Total Devices 22
Total Devices Online 11
Percentage Online 50%

Label CNL-Door-05
Description CNL Demo Simulator Door
IP Address
Port Number 0
Enabled False
Online State Offline
Location Devices
Path My Organisation\Devices\

Online State History

Custom: 12/17/2020 11:37:09 AM

Custom: 12/11/2020 10:16:47 AM

Custom: 12/9/2020 3:37:27 PM

Custom: 11/6/2020 12:54:14 PM

Custom: 10/21/2020 3:41:23 PM

Custom: 10/16/2020 12:43:04 PM

Custom: 10/16/2020 10:34:05 AM

Type Search Text Here
 Disabled
All

Label	Description	Enabled	Last Modified	Online Status
<input checked="" type="checkbox"/> CNL-Door-05	CNL Demo Simulator Door	●	10/15/2020 4:45 PM	Offline
<input type="checkbox"/> CNL-Door-06	CNL Demo Simulator Door	●	10/15/2020 4:45 PM	Offline
<input type="checkbox"/> CNL-Door-07	CNL Demo Simulator Door	●	10/15/2020 4:45 PM	Offline
<input type="checkbox"/> CNL-Door-08	CNL Demo Simulator Door	●	10/15/2020 4:45 PM	Offline
<input type="checkbox"/> CNL-Door-09	CNL Demo Simulator Door	●	10/15/2020 4:45 PM	Offline
<input type="checkbox"/> CNL-Door-10	CNL Demo Simulator Door	●	10/15/2020 4:45 PM	Offline
<input type="checkbox"/> Fence 11	CNL Demo Simulator Fence	●	10/15/2020 4:45 PM	Offline

3. Specify one or all the filter options:

- **Green/Gray circle (enable icon)** – Select devices that you want to be enabled and click the circle. Note that enable icon turns green only after you select a device.
- **Green checkmark box** – Select to mark all devices on the page.
- **Blank check box** – Clears the selection, that is unmarks all the selected items.
- **Text field** – Type a text to filter quickly. For example, typing CCTV will only display devices that have CCTV in their name.
- **First drop-down** – Select the state of the device:
 - **All** – Displays all the devices in the system.
 - **Enabled** – Displays only enabled devices in the system.
 - **Disabled** – Displays only disabled devices in the system.
- **Second drop-down** – Select the status of the devices:
 - **All** – Displays all the devices regardless of their status.
 - **Online** – Displays only devices that are online in the system.
 - **Offline** – Displays only devices that are offline in the system.
 - **Pending** – Displays devices with pending status in the system.

- **Failed** – Displays all failed devices in the system.
 - **PDF icon** – Click on the icon to generate a report of the device status for all current monitored devices.
4. Repeat the above steps to disable devices, except that instead of a green circle the disabling icon will be indicated in red.

To view the status of devices:

1. From the Admin Interface, select **Devices**. The **Devices** page appears displaying the status of the clients configured with your Control Center Server.
2. Select from the options available to customize the status view:
 - **Text field** – Type a text to filter quickly. For example, typing CCTV will only display devices that have CCTV in their name.
 - **State drop-down** – Select the state of the device:
 - **All** – Displays all the devices in the system.
 - **Enabled** – Displays only enabled devices in the system.
 - **Disabled** – Displays only disabled devices in the system.
3. The following information appears depending on the options selected above:
 - **Label** – The client computer label that relates to the server.
 - **Description** – Description of the client computer with the IP address.
 - **Enabled** – The state of the client computer whether enabled or disabled. Enabled state is indicated by a green circle and disabled state is indicated by a red circle.
 - **Last Modified** – Last modified date and time.
 - **Online Status** – The online status of the client.
4. To set a location, see Editing locations.

Managing Servers

Use the Servers option to view the status of servers. The following options are available:

- Label
- Description
- Enabled
- Last Modified

You can also filter by All, Enabled, and Disabled options.

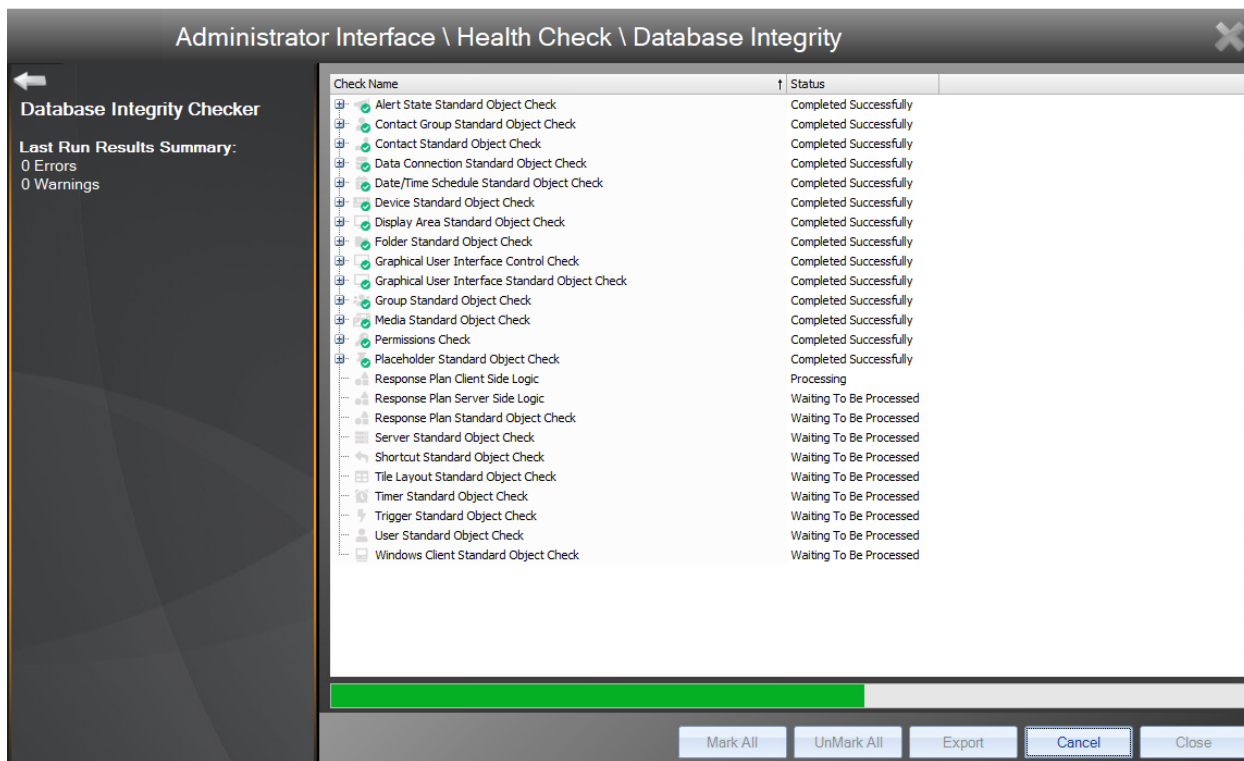
Health Check

Use the **Health Check** option to verify any health performance issues with the client or the database.

To perform a health check on the client:

1. From the Admin Interface, click **Health Check**. The **Health Check** page appears. You can select either:
 - Client Issues - go to [step 2](#).
 - Database Integrity go to [step 3](#)
2. Select **Client Issues**. The **Client Issues** page appears displaying the client loading status along with the GUI plugin and connectors that have been loaded into your Control Center solution.
3. To run a health check on the database:
 - a. From the Admin Interface > **Health Check** option, click **Database Integrity**. The **Database Integrity Checker** appears.
 - b. Select the items that you want to run a check against by manually selecting every check box or use the options available. The following options are available:
 - **Mark All** - Selects all the displayed items.
 - **UnMark All** - Unchecks all the selected items.
 - **Export** - Generates a health check report in csv format.
 - **Start** - Starts the health check process.
 - **Close** - Closes the **Health Check** dialog.
4. Click **Start** to run the health check. A progress bar appears displaying the status of the health check on the database items.

Admin Interface



5. Click **Close** when the process is complete.

Windows Clients

Use the Windows Clients option to view the clients that are connected to the IPSECURITYCENTER Server. To view the status of Windows Clients:


1. From the Admin Interface, click **Windows Clients**.

Admin Interface

Administrator Interface \ Windows Clients \ Status

Windows Clients Status View

Type Search Text Here All

Label	Description	Enabled	Last Modified	Online Status
P-Win10-2.dev.cnluk.com	Client Computer with the IP hostname of P-WIN10-2.DEV.CNL...		12/17/2020 11:47 AM	Online

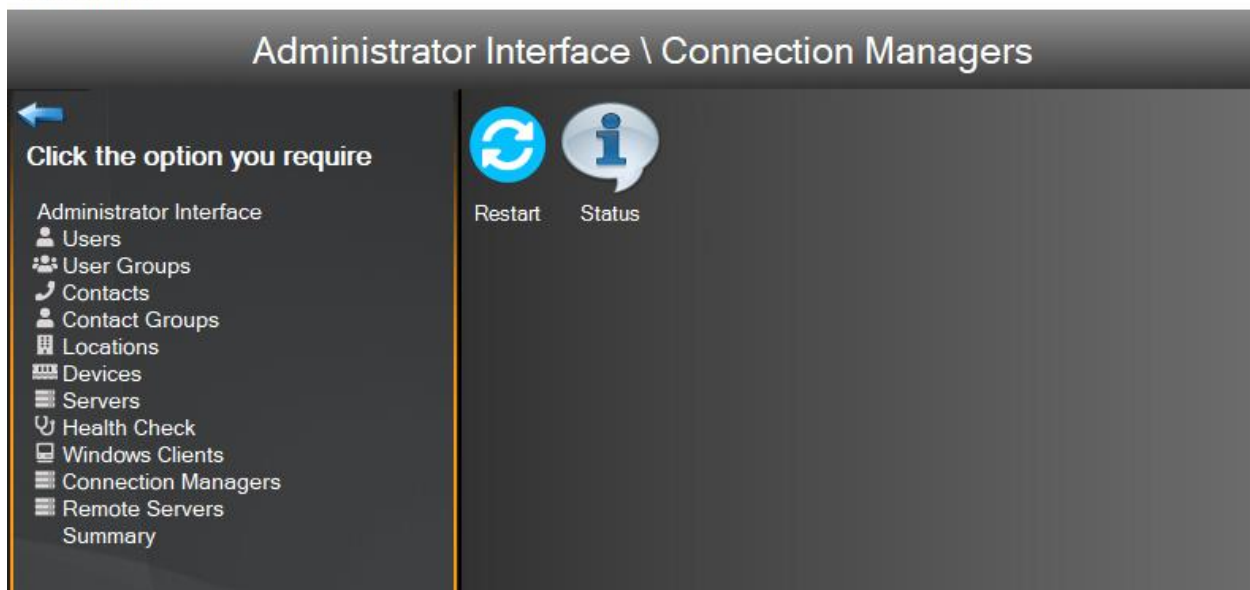
Label
Description Client Computer with the IP host
IP Address
Serial Number
Enabled True

2. Filter the items based on **Select All, Enabled, Disabled** options.
3. Use the **Search** text field to quickly find the required client from the list of clients displayed. The search results automatically update with each new character entered. This functionality is particularly useful if you are connected to several clients.

Connection Managers

Use the Connection Managers option to monitor the status of Connection Managers and restart them.

Admin Interface



To restart the Connection Manager through the Administrator Interface:

1. From the Admin Interface, select **Connection Managers**.
2. Double-click on the Connection Manager that needs to be restarted.

To monitor status of Connection Managers through the Administrator Interface, select **Connection Managers > Status**.

The status of the Connection Managers is shown.

Summary

Use the **Summary** option for a brief overview of each of the options available on the **Summary** dialog. For example, you can click **Connection Managers** to view the status of the Connection Manager instance that is running or click **Devices** for a quick overview of the device status. You can even enable/disable devices that are available within Control Center.

Known Issues



Product Area	Feature	Known Issue
VRPs	Script Shape	<p>When using the script shape method of Count on a List of Variable, in conjunction with certain response plan shapes, the list of variable may be blanked.</p> <p>Workaround: Limit use of the Count method if possible – or move the Count to the end of your VRP</p>
Localizations	Create Alarm Shape	<p>If the translated titles of an Alarm Type are exactly the same for different Alarm Types, raising an alarm with the Create Alarm Shape using the localized title may raise the incorrect Alarm Type. This is also true in non-translated Control Center if the non-localized titles for multiple Alarm Types are exactly the same.</p> <p>Workaround. Make sure translated titles for alarm types are unique.</p>
Translated GUIs	Federation	<p>When upgrading Control Center, if a child site is an older version than a parent site, GUI and Object translations are not seen on the child site.</p> <p>Workaround: You must upgrade sender and receiver sites at the same time for localizations to automatically federate or be published. If a parent site is upgraded before a child site, the objects need to be modified after the child site has been upgraded, before their localizations will be published.</p>
Control Center Server	Control Center Services	<p>When logging in to Control Center, if your connection is unstable, causing the Failover dialog to be displayed, this can sometimes cause your Control Center services to increase their memory usage.</p> <p>Workaround: Log out of Control Center and restart Control Center Services.</p>

Product Area	Feature	Known Issue									
Audit Viewer	Compare Previous	<p>If there is a complex change in the audit XML related to the last audit event, when you select Compare Previous, the Difference screen may treat some nodes which have not changed as moved (meaning removed and re-added elsewhere in the XML) rather than unchanged. A moved node in the XML has an underlined title, which is a hyperlink to the corresponding removed/re-added node on the other side of the Difference screen.</p> <p>Workaround: None.</p>									
Audit Viewer	Extra Info	<p>Note the following when viewing XML in Extra Info column in Audit Viewer.</p> <table border="1" data-bbox="613 747 1409 1255"> <thead> <tr> <th data-bbox="613 747 846 810">Object</th> <th data-bbox="846 747 1073 810">Feature</th> <th data-bbox="1073 747 1409 810">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="613 810 846 1045">Scene Geographic</td> <td data-bbox="846 810 1073 1045">Feature Layer Trail Path Geofences</td> <td data-bbox="1073 810 1409 1045">The following properties are left blank: Layer Name Layer Device Type</td> </tr> <tr> <td data-bbox="613 1045 846 1255">Scene Schematic</td> <td data-bbox="846 1045 1073 1255">CAD background</td> <td data-bbox="1073 1045 1409 1255">The GUID of the CAD file is displayed instead of the name of the CAD background.</td> </tr> </tbody> </table> <p>Workaround: None.</p>	Object	Feature	Description	Scene Geographic	Feature Layer Trail Path Geofences	The following properties are left blank: Layer Name Layer Device Type	Scene Schematic	CAD background	The GUID of the CAD file is displayed instead of the name of the CAD background.
Object	Feature	Description									
Scene Geographic	Feature Layer Trail Path Geofences	The following properties are left blank: Layer Name Layer Device Type									
Scene Schematic	CAD background	The GUID of the CAD file is displayed instead of the name of the CAD background.									

Product Area	Feature	Known Issue
Video Export	Video Export jobs	<p>If you have:</p> <ol style="list-style-type: none"> 1. changed the time zone on your Control Center server and client machines to Eastern Time (ET) 2. created a new video export job 3. closed the video export scheduler <p>when you reopen the video export scheduler after a period of time, your video export job is not displayed.</p> <p>Note: The video export jobs are still displayed as expected under the Queued and Completed tabs.</p> <p>Workaround:</p> <p>You can see your export job if you do either of the following:</p> <ol style="list-style-type: none"> 1. Select appropriate status or time frame filter. 2. Close and reopen video export scheduler.
Graphical User Interfaces	Drop-down list	<p>The data binding property Value title is misleading. The Value property is used only to bind the Selected Value to another control, for example, binding to a Data Navigator control. When the Data Navigator is scrolled, the drop-down list's Selected Value is updated to be the one selected by the Data Navigator. When the Text value is bound (without requiring any Value binding), the underlying Value property is automatically bound to the primary key of the database table where the Text comes from (or the given Text if no Primary Key column is found).</p> <p>Workaround: You must use the drop-down list control with controls like Data Navigator.</p>

Product Area	Feature	Known Issue
Graphical User Interfaces	Date Time Picker control	<p>If you have a GUI configured with a datetime picker control that has not been themed on a themed panel, you may see some extra lines to the right-hand side of the control when you upgrade to this version of Control Center.</p> <p>Workaround: You can:</p> <ol style="list-style-type: none"> 1. Log off and log on again, stop and restart the Control Center services. The datetime picker control is displayed correctly. 4. Edit your GUI and delete the datetime picker control, then add a new one.
Mapping	GIS Feature Layer	<p>When a feature layer is dynamically updated, tooltips do not update to show the new property values unless you reload the scene in Control Center.</p> <p>Workaround: None.</p>
Mapping	GIS Feature Layer	<p>If you delete a feature layer, the changes do not take effect unless you reload your scene in Control Center.</p> <p>Workaround: None.</p>
Mapping	GIS Feature Layer	<p>If you update Polling Interval when configuring a GIS feature layer, the changes do not take effect unless you log out and login again to Control Center.</p> <p>Workaround: None.</p>
Instant Messenger	Chat	<p>If you are logged into Control Center as, for example, user1, then you login to System Configuration as a user with higher permissions, for example, root, when you log root out of System Configuration by selecting System > Log off elevated user, user1 can no longer search for other users or create new chats.</p> <p>Workaround: Log off and login again to Control Center.</p>

Product Area	Feature	Known Issue
Control Center Extensions	Installation	<p>If you were previously using IPSecurityCenter, and you uninstall IPSecurityCenter and install Control Center, your existing Extensions remain in C:\Program Files (x86)\CNL Software\IPSecurityCenter\AddonPackages. This means Control Center cannot read them and therefore does not use them.</p> <p>Workaround: Perform one of the following workarounds:</p> <ol style="list-style-type: none"> 1. You must manually copy the Extension files from: C:\Program Files (x86)\CNL Software\IPSecurityCenter\AddonPackages to C:\Program Files (x86)\Everbridge\Control Center\AddonPackages 5. Uninstall the Extensions using Control Panel > Programs and Features > Add or remove programs. Reinstall the Extensions by browsing to the location of your extension packages and running the Extensions installer.
System Objects	Date/Time Schedule Object	<p>In the following scenario:</p> <ol style="list-style-type: none"> 1. From System Configuration > System Objects, navigate to Date/Time Schedule. 2. Double-click 24 x 7 allow. 3. Scroll with the mouse scroll wheel. The following exception message displays: <p>Control Center has encountered an unexpected problem, details of the problem are shown below.</p> <p>Authentic operation resulted in an overflow.</p> <p>A copy of the error report is available in the Windows Event Log. As this is an unexpected condition is recommended that you restart Control Center before continuing.</p> <p>Would you like to close Control Center now?</p> <p>Workaround: You should use the scroll bar rather than the mouse scroll wheel.</p>

Product Area	Feature	Known Issue
System Explorer	Icons	<p>If you select a different icon set in System Configuration > Enterprise Settings > Global Settings > Primary Icon Set, then the icons for button controls in existing custom GUIs are not updated to use the new icon set.</p> <p>Workaround: You must edit the icon for the button control in the GUI. For the changes to take effect, you must select a different icon for the button control and then select the icon you want. To do this:</p> <ol style="list-style-type: none"> 1. In System Configuration, open your custom GUI for editing. 2. From Design Surface tab, select the button control to display the Properties pane. 3. Navigate to Image/Background Appearance and select Icon Name. 4. Select . The Icon Picker is displayed. 5. From Icon Picker, select a different icon, then select OK. 6. Select . The Icon Picker is displayed. 7. From Icon Picker, select the icon you want, then select OK. The button control displays the icon you want.
Mapping	Images	<p>Images must be a maximum of 23170 pixels. A security scan of Control Center identified that the GIS Server service was using an outdated component that referenced OpenSSL. Now, the GIS Server Service no longer references this outdated component. This change means that there is now a maximum size limit for high resolution images that you can import to Control Center. The maximum size (height * width *) must be less than Int.MaxValue. For example, 23170* 23170* is valid; 23171* 23170* is not. Existing images are not affected. However, if you try to regenerate a tile cache for existing images larger than the maximum size, this fails. More information can be provided on request.</p> <p>Workaround: None.</p>

Product Area	Feature	Known Issue
Federated	Status Dashboard	<p>When setting the Show Disabled Sites and/or Show Disabled Subsystems to False, the behavior is not as expected.</p> <p>The Show Disabled Sites will show the site as being online despite every subsystem being in an offline state as shown below. This is achieved by disabling the RFS object. Show Disabled Subsystems is behaving in a way that the disabled subsystem still appears even when the subsystem is disabled.</p>

<p>Dashboards</p>	<p>System Dashboard</p>	<p>On upgrading to this version of Control Center, the Device States by Device Type widget no longer displays correctly in System dashboard.</p> <p>Workaround: Complete the following steps:</p> <ol style="list-style-type: none"> 1. From System Configuration, navigate to the System Objects folder. 6. From Dashboard, double-click System Dashboard to open it in the Dashboard Designer. 7. Select the Device States by Device Type widget. The widget configuration options are displayed. 8. Click Select data... The Configuring a data source dialog is displayed. 9. Click Select an existing data source. 10. Select os data source. 11. Select Next. The Select a table from the data source dialog is displayed. 12. Select By Device Type. 13. Select Next. 14. Select Finish. The Configuring data source dialog closes. 15. From the widget configuration options, in Number of columns, type 5. 16. Configure the columns as follows: <ul style="list-style-type: none"> • Column 1. For Columns Heading and Text, select Type. • Column 2. For Columns Heading and Text, select Offline. • Column 3. For Columns Heading and Text, select Pending. • Column 4. For Columns Heading and Text, select Online. • Column 5. For Columns Heading and Text, select Failed.
--------------------------	-------------------------	---

Product Area	Feature	Known Issue
Federated Control Center	Dashboards	<p>Dashboards cannot be federated across sites.</p> <p>Workaround: If you want a dashboard to be displayed at all your sites, you must create the dashboard at each site.</p>
Federated Control Center	Alarm Process Check	<p>Control Center 5.45 introduced background monitoring of all elements in the alarm process to make sure that users are alerted if there are interruptions or significant delays that can affect when a user is made aware of new alarms. One of the steps in this process periodically queries the alarm table. In a federated setup, synchronizing resolved alarms from site and interfere with this check, resulting in a failure to synchronize alarms. When you upgrade to 5.49 from a version older than 5.45, the alarm check will be disabled by default. If you upgrade from a newer version, it is recommended to disable the alarm check if it is a federated system. You can enable/disable it by updating the ServiceBrokerTestInterval value to 0 (disabled) or 60,000 in the Alarm Types Service config file. When you upgrade to 5.50, the check will become enabled again with a performance improvement to fully resolve the issue.</p>
GIS Layer Manager	Feature Layer	<p>If you have added a feature layer that uses a GeoJSON file that contains point data, the point data does not display on the map.</p> <p>Workaround. In GIS Layer Manager, when adding a feature layer, you must ensure that Show feature as icon is selected. This enables the point data to be displayed on the map.</p>
GIS Layer Manager	Feature Layer	<p>GIS Feature layers cannot be federated across sites.</p> <p>Workaround: If you want to display a GIS feature layer at all your sites, you must add the feature layer at each site.</p>

Product Area	Feature	Known Issue
Alarm Management	Alarm Type	<p>You can import more than one alarm type object into a Control Center environment. This means that events are evaluated against multiple sets of alarm definitions. In this scenario, you cannot define the order in which the alarm types are used and when an event is raised, you do not know which alarm type will be raised.</p> <p>Workaround: When importing, make sure you only have one enabled alarm type object in a system.</p>
Theming	Fonts	<p>When using themes in Control Center, some font styling is not applied to the following controls:</p> <ol style="list-style-type: none"> 1. Link labels - Underline does not display correctly. 17. Paragraph text- Underline, Strikeout, Bold, and Italic do not display correctly. 18. Paragraph title - No font styling is applied. <p>Workaround: None.</p>
System Tree	Event Page	<p>If an event page has been created for Device Selected in the System Tree control, this will be disconnected from the event because a new variable has been added.</p> <p>Workaround: To resolve this, select the Device Selected event, recreate the event page, and reconfigure the logic from the disconnected page.</p>
Mapping	Geofence	<p>Pan and Zoom to Asset on scene does not apply to Geofence objects.</p>
User Interface	Display Areas	<p>If you unpin and float a display area, then click its Close button, nothing happens. This is a limitation of the underlying component and will be resolved when the supplier updates their control.</p> <p>See https://docs.telerik.com/devtools/wpf/controls/raddocking/how-to/disable-the-close-button.</p> <p>Workaround: None.</p>

Product Area	Feature	Known Issue
Import/Export	Cameras	<p>The Import and Export feature does not import devices such as cameras if you only import the device without the server device.</p> <p>Workaround: Make sure to export the server objects when exporting devices.</p>
Control Center Client	Main Menu	<p>The Modern Client Main Menu containers render with the text below the button, so the button size may need tweaking to be visible.</p> <p>Workaround: The recommended workaround is to reduce the size of the commissioned buttons to prevent buttons from disappearing.</p>
Alarm Management	Alarm Stack	<p>When you have unpinned an alarm stack with multiple views in it, the user expects to see a counter of alarms being generated to be displayed on each view tab. Currently the counter is shown against all views but for the view that was selected before minimizing the alarm stack. That view remains selected even after minimizing. This is because the alarm stack thinks you can see the view as it has been selected and, therefore, does not have to display the alarm count.</p> <p>Workaround: The only way to see the alarms for the selected view is to hover the mouse over it to temporarily expand the alarm stack or click the view and pin it to view the alarm stack.</p>