



Gallagher Command Centre

Regulated Zones Feature 9.10

C12639

Release Note

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2025. All rights reserved.

Copyright Notice

The software contains proprietary information of Gallagher Group Limited; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Gallagher Group Limited and the client and remains the exclusive property of Gallagher Group Limited. If you find any problems in the documentation, please report them to us in writing. Gallagher Group Limited does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Gallagher Group Limited.

Contents

1	Introduction	4
2	Installation	9
3	Configuration	10
4	Regulated Zone status.....	33
5	Regulation events	35
6	Reconfiguration.....	37
7	Upgrading	38
8	Uninstallation.....	40
9	Considerations	41
10	Examples.....	42
11	Predictive Cumulative Duration Examples	44
12	Break Duration Scenarios.....	46
13	Shift Management Scenarios	49

1 Introduction

About this release note This release note is for the 'Regulated Zones' v9.10.055 feature of Gallagher Command Centre.

1.1 Purpose

What this feature does The 'Regulated Zones' feature has been created for managing Cardholders' time on site.

This feature introduces a new 'Regulated Zone' Command Centre item for monitoring Cardholders. The Regulated Zone is separate from Access Zones (but potentially encompasses one or multiple Access Zones), and is used to define the on-site area that is monitored by pre-configured time limits.

Regulated Zone Rules The 'Regulated Zones' feature will monitor Cardholders using the following parameters (rules):

Cumulative duration	Used to monitor Cardholders' accumulated time on site across multiple shifts. An event is raised when a Cardholder has been inside the Regulated Zone for a period greater than the configured cumulative shift duration, within a specified period of time. Example: You can configure a Cumulative duration rule to raise an alarm when a Cardholder stays in a Zone for more than 50 hours within five days.
Break duration	Used to monitor Cardholders' minimum break periods between shifts. An event is raised when a Cardholder re-enters the Regulated Zone within the minimum break period. A temporary exit grace period can be configured to define a period of time a Cardholder is allowed off-site before they are considered to be between shifts. Example: You can configure a Break duration rule to raise an alarm when a Cardholder enters a Zone and has not had a 48-hour break in the last 5 days. For more examples, refer to section 10 " Examples " later in this release note.
Maximum duration	Used to monitor Cardholders' time on site within a single shift (period of time). An event is raised when a Cardholder has been inside the Regulated Zone for a period of time greater than the configured shift length. Example: You can configure a Maximum duration rule to raise an alarm when a Cardholder stays in a Zone for longer than 10 hours. For more examples, refer to section 10 " Examples " later in this release note.

Continued on next page

<p>Predictive cumulative duration</p>	<p>Used to monitor Cardholder accumulated time on site across multiple shifts and predict if a Cardholder will exceed the cumulative limit (total time limit across shifts). When a Cardholder enters the Zone, a rule is checked: will the Cardholder end up at or above the cumulative limit if they stayed in the Regulated Zone for the Expected shift duration. If yes, a predictive alarm is raised.</p> <p>After the Cardholder exits the Zone, the rule checks whether they have already exceeded the cumulative limit or whether re-entering the Zone immediately would violate the predictive rule. If yes, then any configured Competency is disabled.</p> <p>Example: You can configure a Predictive cumulative duration rule to raise an alarm when a Cardholder enters a Zone, and if staying in the Zone for 10 hours would take their total time on site above 50 hours. For more examples, refer to section 11 "Predictive Cumulative Duration Examples" later in this release note.</p> <p>Note: If the Cardholder is already in breach of the Cumulative predictive duration rule and the Cardholder enters the Zone, a predictive alarm is not raised. However, after the Cardholder exits the Zone, the Competency re-enablement time is re-calculated.</p>
<p>Shift management</p>	<p>Used to monitor Cardholders' shift patterns and optionally enforce Cardholders' compliance with shift patterns. An alarm is raised when a Cardholder enters the Regulated Zone before the first day of their shift. An alarm is also raised when a Cardholder does not exit site when their shift ends. Grace periods can be configured to allow Cardholders to enter site one, two or three days before their shift starts, and leave one, two or three days after their shift ends.</p> <p>Shift patterns are composed of a Start Shift Date, an End Shift Date (optional) and Shift Pattern (e.g. 7x7). Shift Patterns define how many days a Cardholder is granted site access for before having their access disabled (their shift), and how many days must pass before they are again granted site access (their rest period).</p> <p>Example: A Cardholder has a shift pattern of 7 days working and 7 days break (7x7), with a grace period of 1 day. You can configure a Shift management rule to raise an alarm when the Cardholder enters site earlier than one day before their shift starts, or when the Cardholder has not left site after 8 days (7 days plus grace period) have passed since their shift started.</p>
<p>Maximum entries</p>	<p>Used to monitor and restrict how many times a Cardholder can enter an area within a specified time period. An alarm is raised when a Cardholder enters the Regulated Zone more than the maximum allowed times within the specified time period.</p> <p>Example: You can configure a Maximum entries rule to raise an alarm when a Cardholder enters a Zone more than 3 times within 8 hours.</p>

Disabling Competencies

An operator can configure a Regulated Zone to automatically disable a Competency upon a rule violation. The Competency can be disabled immediately or after a configured delay. For the Break duration and the Predictive cumulative duration rules, re-enablement of the Competency will occur automatically once the Cardholder is no longer in violation of that particular rule.

Activity Reports

An operator can configure an Activity Report to report on Regulated Zone events over a specified period of time, for all Cardholders or specific Cardholders only. Refer to the topic "*Creating Reports*" in the Gallagher Command Centre Help.

Notifications about Regulated Zone events

An operator can configure a Notifications Filter to notify Cardholders when a regulated zone event occurs. The Notifications Feature is a licensed feature of Command Centre. Refer to the topic "*Creating a Notifications Filter*" in the Gallagher Configuration Client Help.

1.2 New in v9.10.053 (and later 9.10 versions)

Increased Shift management Competency action frequency

The 'Daily action time' for a Shift management rule's Competency is now supplemented with a 'Then action every n hours' setting (where n is configurable). The rule then checks for necessary changes to its Cardholders' Competencies at the 'Daily action time', plus every n hours after and before the 'Daily action time', each day.

For details, see [Shift management \(page 26\)](#).

1.3 Compatibility

Support for this feature

This feature supports and has been tested with the following:

New software	RegulatedZones v9.10.053
Supported Gallagher software	<ul style="list-style-type: none">• Gallagher Command Centre: vEL9.10.1005 (or later vEL9.10 release)• Gallagher Controller 6000, 7000, and 7000 Single Door: vCR9.10.240404a (or later vCR9.10 release)• Gallagher Mobile Reader
Tested Microsoft software	Command Centre Server: Windows Server 2022, Windows 11 Command Centre Workstation: Windows 10 (64-bit) Database: SQL Server 2019 Express

Multi-server support

This feature has been tested in a Command Centre multi-server environment.

Mobile Reader support

Gallagher Mobile Readers are supported. Access and/or exit events are generated when a Cardholder is moved between Access Zones via a Mobile Reader.

Tagboard movement support

This feature only tracks Tagboard movements (i.e. moving Cardholders between Zones) if the Regulated Zone is configured using Access Zone(s).

1.4 Security considerations

Using Regulated Zone Rules to restrict access

A Cardholder may still be able to access a Regulated Zone after they have breached a Regulated Zone Rule for two reasons: Competency configuration and Controllers going offline.

Competency configuration: Some configuration factors must be in place for Competencies to be used to deny access when a Rule is breached:

- The Competency must be assigned to the Regulated Zone Rule as well as all required Access Zones and Cardholders.
- The Competency must be 'Enforced' on the required Access Zones.

With this configuration in place, a Cardholder may still access a Regulated Zone for some time after breaching a Rule if a 'Competency action delay' is configured on the Rule. The 'Competency action delay' setting creates a delay between the Rule being breached and the Competency being disabled.

Controller offline: If a Cardholder's Competency is disabled (e.g. by a Regulated Zone Rule) while a Controller is offline, the state of the Cardholder's Competency on the Controller remains in the state it was when the Controller went offline (potentially active) until the Controller comes online again.

2 Installation

Upgrading from a previous version If a previous version of this feature is installed, or the Gallagher 'Fatigue Management' feature is installed, this must be removed before installing this version. Refer to section 7 "[Upgrading](#)" later in this release note.

First-time installation To install this feature for the first time, perform the following procedure on the Command Centre Server:

Step	Action	Description
1	Backup	Perform a backup of your Command Centre system.
2	Licence file	Ensure your licence file contains the following entry: [Limits] Regulated Zones=X (where X is a number) [Customisations] RegulatedZones=1
3	Licence folder	Store the licence file in the following folder: C:\ProgramData\Gallagher\Command Centre.
4	Stop Command Centre and Services	Exit Command Centre and stop the Command Centre Services.
5	Install Command Centre	On the Command Centre Server and all Command Centre Workstations, install Gallagher Command Centre vEL9.10.1005 (or later vEL9.10 release) if not already installed.
6	Unzip folder	Unzip the folder you have been provided for this feature.
7	Run installation file	Run the installation file RegulatedZonesSetup_9.10.xx.msi on the Command Centre Server and all non- ClickOnce * Configuration Client Workstations.
8	Start Services and Command Centre	Restart the Command Centre Services and Command Centre.
9	Verify installation	To ensure this feature has been installed correctly, check the following: From the Gallagher Configuration Client menu bar, go to Help > About Command Centre . 'RegulatedZones v9.10.xxx' should be displayed in the Customisations field. Open Programs and Features from the Windows Control Panel on the Command Centre Server. 'Gallagher Regulated Zones' should be listed as installed.

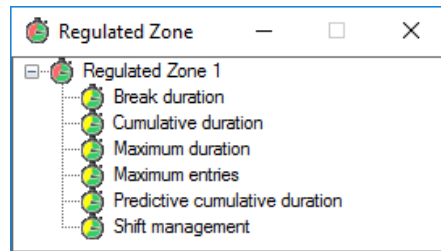
***ClickOnce installation** Do not install this feature on ClickOnce Workstations. Workstations deployed via ClickOnce automatically download this feature from the Command Centre Server.

3 Configuration

About Regulated Zones configuration

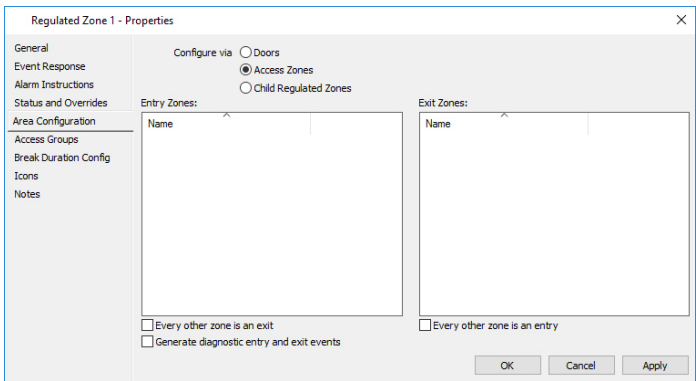
Regulated Zones identify the Access Zones and/or Doors that will be monitored. The Regulated Zone Rules that can be created are Break duration, Cumulative duration, Maximum duration, Predictive cumulative duration, Shift management, and Maximum entries. Assign the rules as child items to the appropriate Regulated Zones.

The Regulated Zone List Window with a Regulated Zone and several Regulated Zone Rules configured:



3.1 Creating a Regulated Zone

Procedure To create a Regulated Zone, perform the following procedure:

Step	Action	Description
1	Open the Regulated Zone List Window	Click Configure from the menu bar, then Regulated Zones . The Regulated Zone List Window opens (in grid view).
2	Create a new Regulated Zone	Right-click and select New... > Regulated Zone . The General tab displays.
3	General fields	Complete the general fields as required.
4	Event Response tab	Click the Event Response tab and configure as required.
5	Alarm Instructions tab	Click the Alarm Instructions tab and configure as required.
6	Click the Area Configuration tab	Click the Area Configuration tab. 

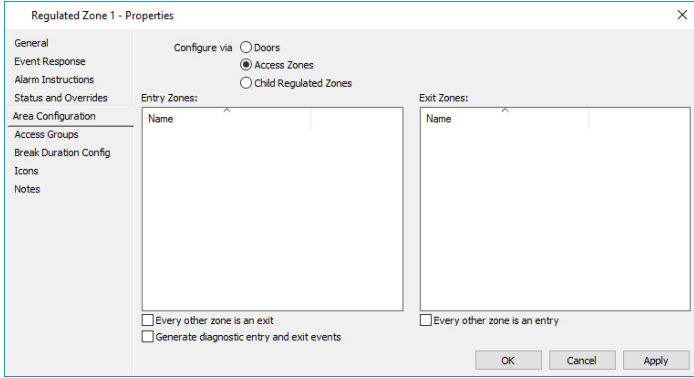
Continued on next page

7	Choose a Configuration method	Regulated Zones can be configured in three ways.		
		Configuration method	Description	For this method, go to step...
		Doors	Regulated Zones are configured using Doors as entry and exit points.	8
		Access Zones	Regulated Zones are configured using Access Zones as entry and exit points.	11
Child Regulated Zones	Regulated Zones are configured using other Regulated Zones (parent/child relationship). Notes: <ul style="list-style-type: none"> The Access Groups of any Regulated Zones added as 'children' are ignored, and the 'parent' zone becomes responsible for membership filtering. The 'child' zones determine the physical boundaries of the parent Regulated Zone. You can (optionally) limit the rules to only apply to Cardholders who travel between child zones. 	14		

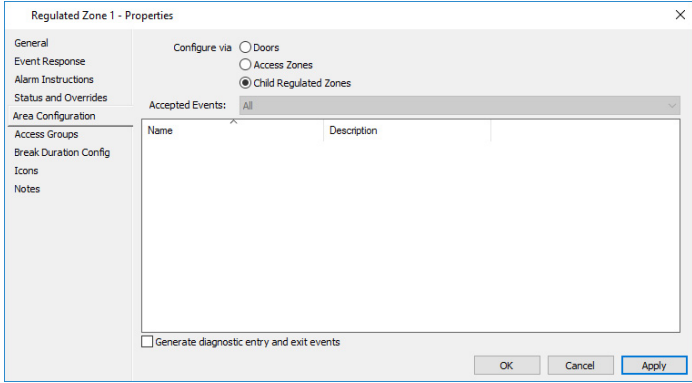
Configure Regulated Zones using Doors

8	Select the 'Doors' radio button	Select the Doors radio button.	

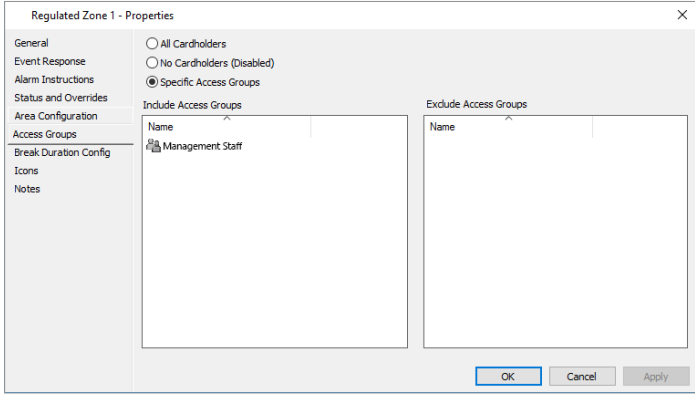
Continued on next page

9	Drag Doors into the grid	<p>Drag and drop the appropriate Doors into the grid.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Entering a Door will result in the Cardholder entering the Regulated Zone. • Leaving through a Door will result in the Cardholder exiting the Regulated Zone. • The Cardholder will also leave the Regulated Zone when they leave to go outside (i.e. exit through a <i>non-listed</i> door that does <i>not</i> have an Exit Zone assigned). • If no doors are specified, any entry or exit event will move the Cardholder in and out of the Regulated Zone.
10	Go to Step	Go to Step 17.
Configure Regulated Zones using Access Zones		
11	Select the 'Access Zones' radio button	<p>Select the Access Zones radio button.</p> 
12	Drag Access Zones into the grid	<p>Drag the appropriate Access Zones into the grids as appropriate.</p> <p>Notes:</p> <ul style="list-style-type: none"> • When a Cardholder enters a listed Entry Zone, they enter the Regulated Zone. Conversely, when a Cardholder enters a listed Exit Zone, they leave the Regulated Zone. • The Cardholder will also leave the Regulated Zone when they leave to go outside (i.e. exit through a door that does not have an Exit Zone assigned). • If you populate either the Entry Zone or the Exit Zone list and select the Every other zone is an ... check box below the populated grid, all other available Access Zones are treated as being in the unpopulated grid.
13	Go to Step	Go to Step 17.

Continued on next page

Configure Regulated Zones using Child Regulated Zones										
14	Select the 'Child Regulated Zones' radio button	<p>Select the Child Regulated Zones radio button.</p> 								
15	Accepted Events	<p>Select an option from the Accepted Events drop-down list:</p> <table border="1" data-bbox="687 824 1382 1153"> <thead> <tr> <th>Option...</th> <th>means that rules of the 'parent' zone apply...</th> </tr> </thead> <tbody> <tr> <td>All</td> <td>at all times.</td> </tr> <tr> <td>Passed through Doors / Zones in different Regulated Zones</td> <td>when the Cardholder moves between child Zones (of the same parent).</td> </tr> <tr> <td>Did not pass through Doors / Zones in different Regulated Zones</td> <td>if the Cardholder stays within one child Zone.</td> </tr> </tbody> </table>	Option...	means that rules of the 'parent' zone apply...	All	at all times.	Passed through Doors / Zones in different Regulated Zones	when the Cardholder moves between child Zones (of the same parent).	Did not pass through Doors / Zones in different Regulated Zones	if the Cardholder stays within one child Zone.
Option...	means that rules of the 'parent' zone apply...									
All	at all times.									
Passed through Doors / Zones in different Regulated Zones	when the Cardholder moves between child Zones (of the same parent).									
Did not pass through Doors / Zones in different Regulated Zones	if the Cardholder stays within one child Zone.									
16	Drag Regulated Zones into the grid	<p>Drag and drop the appropriate Regulated Zones into the grid.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Entering a child Zone will result in the Cardholder entering the parent Regulated Zone. • Entering a child Zone will generate an entry event (one for each zone if multiple are accessed in succession). • Leaving a child Zone will result in the Cardholder exiting the parent Regulated Zone unless they have entered another child Zone belonging to the same parent. 								
17	Generate diagnostic entry and exit events	<p>Ensure the Generate diagnostic entry and exit events check box is unchecked (unless you want to test your configuration).</p>								

Continued on next page

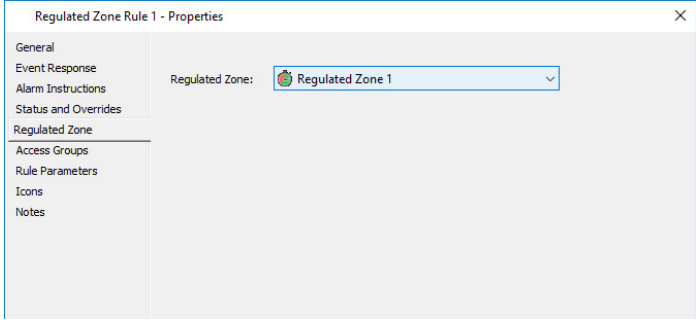
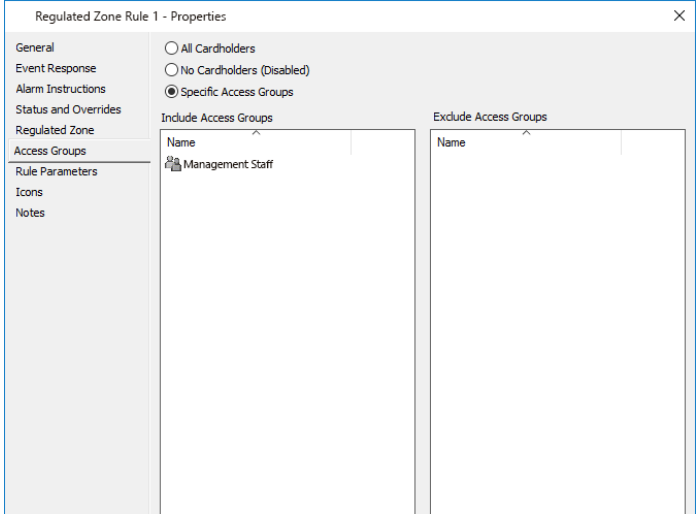
18	<p>Click the Access Groups tab</p>	<p>Click the Access Groups tab.</p> 								
19	<p>Select Access Group configuration method</p>	<p>Select which Access Groups are included in this Regulated Zone:</p> <table border="1" data-bbox="687 775 1385 1160"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>All Cardholders</td> <td>When selected, all Cardholders are included, whether they are members of any Access Groups or not.</td> </tr> <tr> <td>No Cardholders (Disabled)</td> <td>When selected, all Cardholders are excluded, whether they are members of any Access Groups or not.</td> </tr> <tr> <td>Specific Access Groups</td> <td>When selected, the Include Access Groups and Exclude Access Groups grids are enabled, and Access Groups can be added to the grids</td> </tr> </tbody> </table>	Option	Description	All Cardholders	When selected, all Cardholders are included, whether they are members of any Access Groups or not.	No Cardholders (Disabled)	When selected, all Cardholders are excluded, whether they are members of any Access Groups or not.	Specific Access Groups	When selected, the Include Access Groups and Exclude Access Groups grids are enabled, and Access Groups can be added to the grids
Option	Description									
All Cardholders	When selected, all Cardholders are included, whether they are members of any Access Groups or not.									
No Cardholders (Disabled)	When selected, all Cardholders are excluded, whether they are members of any Access Groups or not.									
Specific Access Groups	When selected, the Include Access Groups and Exclude Access Groups grids are enabled, and Access Groups can be added to the grids									
20	<p>Configure 'Specific Access Groups'</p>	<p>If you selected 'Specific Access Groups', drag and drop the appropriate Access Groups into the Include Access Groups and/or Exclude Access Groups grids.</p> <table border="1" data-bbox="687 1301 1385 1805"> <thead> <tr> <th>Grid</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Include Access Groups</td> <td>Only Cardholders who are members of the included Access Groups but not members of the excluded Access Groups are included. If the grid is left empty (i.e. no Access Group is added to the Include Access Groups grid), then all Cardholders are included except those who are a member of the excluded Access Group(s).</td> </tr> <tr> <td>Exclude Access Groups</td> <td>All cardholders are included except those that are members of the excluded Access Groups. If the grid is left empty (i.e. no Access Group is added to the Exclude Access Groups grid), all Cardholders who are not a member of the included Access Group(s) are excluded.</td> </tr> </tbody> </table> <p>Cardholder in both grids: If a Cardholder is a member of multiple Access Groups and they are in both the Include and Exclude grids, the Cardholder will be <i>excluded</i> from the Zone and/or the rule. Exclusion takes priority over inclusion.</p>	Grid	Description	Include Access Groups	Only Cardholders who are members of the included Access Groups but not members of the excluded Access Groups are included. If the grid is left empty (i.e. no Access Group is added to the Include Access Groups grid), then all Cardholders are included except those who are a member of the excluded Access Group(s).	Exclude Access Groups	All cardholders are included except those that are members of the excluded Access Groups. If the grid is left empty (i.e. no Access Group is added to the Exclude Access Groups grid), all Cardholders who are not a member of the included Access Group(s) are excluded.		
Grid	Description									
Include Access Groups	Only Cardholders who are members of the included Access Groups but not members of the excluded Access Groups are included. If the grid is left empty (i.e. no Access Group is added to the Include Access Groups grid), then all Cardholders are included except those who are a member of the excluded Access Group(s).									
Exclude Access Groups	All cardholders are included except those that are members of the excluded Access Groups. If the grid is left empty (i.e. no Access Group is added to the Exclude Access Groups grid), all Cardholders who are not a member of the included Access Group(s) are excluded.									

Continued on next page

21	Break Duration Config tab	Click the Break Duration Config tab to view, add or remove a Break duration rule for this Regulated Zone.								
22	Add, remove, or open a rule	<p>What do you want to do?</p> <table border="1"> <thead> <tr> <th>To...</th> <th>then...</th> </tr> </thead> <tbody> <tr> <td>Add a new rule</td> <td> <p>a. Click the Add Rule button. A new Regulated Zone rule displays.</p> <p>b. To configure this rule, refer to section 3.2 "Creating a Regulated Zone Rule" later in this release note.</p> <p>Note: You can also add an unassigned rule to the Regulated Zone by dragging and dropping it on this grid.</p> </td> </tr> <tr> <td>Remove a rule</td> <td> <p>a. Right-click on the rule you want to remove from this Regulated Zone.</p> <p>b. Select Remove from list. The Rule is detached from the Regulated Zone and removed from the grid.</p> </td> </tr> <tr> <td>Open a rule</td> <td> <p>c. Double-click on the rule you want to open. The rule's properties display.</p> </td> </tr> </tbody> </table>	To...	then...	Add a new rule	<p>a. Click the Add Rule button. A new Regulated Zone rule displays.</p> <p>b. To configure this rule, refer to section 3.2 "Creating a Regulated Zone Rule" later in this release note.</p> <p>Note: You can also add an unassigned rule to the Regulated Zone by dragging and dropping it on this grid.</p>	Remove a rule	<p>a. Right-click on the rule you want to remove from this Regulated Zone.</p> <p>b. Select Remove from list. The Rule is detached from the Regulated Zone and removed from the grid.</p>	Open a rule	<p>c. Double-click on the rule you want to open. The rule's properties display.</p>
To...	then...									
Add a new rule	<p>a. Click the Add Rule button. A new Regulated Zone rule displays.</p> <p>b. To configure this rule, refer to section 3.2 "Creating a Regulated Zone Rule" later in this release note.</p> <p>Note: You can also add an unassigned rule to the Regulated Zone by dragging and dropping it on this grid.</p>									
Remove a rule	<p>a. Right-click on the rule you want to remove from this Regulated Zone.</p> <p>b. Select Remove from list. The Rule is detached from the Regulated Zone and removed from the grid.</p>									
Open a rule	<p>c. Double-click on the rule you want to open. The rule's properties display.</p>									
23	Icons tab	Click the Icons tab if you want to change the Icon Set for this Regulated Zone.								
24	Notes tab	Click the Notes tab if you want to add any notes about this Regulated Zone.								
25	Click OK	Click OK to close and save your changes.								

3.2 Creating a Regulated Zone Rule

Procedure To create a Regulated Zone Rule, perform the following procedure:

Step	Action	Description
1	Open the Regulated Zone List Window	From the menu bar, go to Configure > Regulated Zones . The Regulated Zone List Window opens (in grid view).
2	Create a new Regulated Zone Rule	Right-click and select New... > Regulated Zone Rule . The General tab displays.
3	General fields	Complete the general fields as required.
4	Event Response	Click the Event Response tab and configure as required.
5	Alarm Instructions	Click the Alarm Instructions tab and configure as required.
6	Click the Regulated Zone tab	Click the Regulated Zone tab. 
7	Select Regulated Zone	From the drop-down list, select the Regulated Zone that this rule will apply to.
8	Click the Access Groups tab	Click the Access Groups tab. 

Continued on next page

9	Select Access Group configuration method	<p>Select which Access Groups are included in this Regulated Zone Rule:</p> <p>Note: Adding Access Groups to the Regulated Zone Rule adds another level of conditions Cardholders need to meet in order to be tracked via Regulated Zones.</p> <table border="1" data-bbox="691 454 1385 842"> <thead> <tr> <th data-bbox="691 454 922 495">Option</th> <th data-bbox="922 454 1385 495">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="691 495 922 600">All Cardholders</td> <td data-bbox="922 495 1385 600">When selected, all Cardholders who are members of any Access Group are included.</td> </tr> <tr> <td data-bbox="691 600 922 705">No Cardholders (Disabled)</td> <td data-bbox="922 600 1385 705">When selected, all Cardholders who are members of any Access Group are excluded.</td> </tr> <tr> <td data-bbox="691 705 922 842">Specific Access Groups</td> <td data-bbox="922 705 1385 842">When selected, the Include Access Groups and the Exclude Access Groups grids are enabled and Access Groups can be added to the grids.</td> </tr> </tbody> </table>	Option	Description	All Cardholders	When selected, all Cardholders who are members of any Access Group are included.	No Cardholders (Disabled)	When selected, all Cardholders who are members of any Access Group are excluded.	Specific Access Groups	When selected, the Include Access Groups and the Exclude Access Groups grids are enabled and Access Groups can be added to the grids.
Option	Description									
All Cardholders	When selected, all Cardholders who are members of any Access Group are included.									
No Cardholders (Disabled)	When selected, all Cardholders who are members of any Access Group are excluded.									
Specific Access Groups	When selected, the Include Access Groups and the Exclude Access Groups grids are enabled and Access Groups can be added to the grids.									
10	Configure 'Specific Access Groups'	<p>If you selected 'Specific Access Groups', drag and drop the appropriate Access Groups into the Include Access Groups and/or Exclude Access Groups grids.</p> <table border="1" data-bbox="691 981 1385 1485"> <thead> <tr> <th data-bbox="691 981 831 1021">Grid</th> <th data-bbox="831 981 1385 1021">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="691 1021 831 1272">Include Access Groups</td> <td data-bbox="831 1021 1385 1272"> <p>Only Cardholders who are members of the included Access Groups but not members of the excluded Access Groups are included.</p> <p>If the grid is left empty (i.e. no Access Group is added to the Include Access Groups grid), then all Cardholders are included except those who are a member of the excluded Access Group(s).</p> </td> </tr> <tr> <td data-bbox="691 1272 831 1485">Exclude Access Groups</td> <td data-bbox="831 1272 1385 1485"> <p>All cardholders are included except those that are members of the excluded Access Groups.</p> <p>If the grid is left empty (i.e. no Access Group is added to the Exclude Access Groups grid), all Cardholders who are not a member of the included Access Group(s) are excluded.</p> </td> </tr> </tbody> </table> <p>Cardholder in both grids: If a Cardholder is a member of multiple Access Groups and they are in both the Include and Exclude grids, the Cardholder will be <i>excluded</i> from the Zone and/or the rule. Exclusion takes priority over inclusion.</p>	Grid	Description	Include Access Groups	<p>Only Cardholders who are members of the included Access Groups but not members of the excluded Access Groups are included.</p> <p>If the grid is left empty (i.e. no Access Group is added to the Include Access Groups grid), then all Cardholders are included except those who are a member of the excluded Access Group(s).</p>	Exclude Access Groups	<p>All cardholders are included except those that are members of the excluded Access Groups.</p> <p>If the grid is left empty (i.e. no Access Group is added to the Exclude Access Groups grid), all Cardholders who are not a member of the included Access Group(s) are excluded.</p>		
Grid	Description									
Include Access Groups	<p>Only Cardholders who are members of the included Access Groups but not members of the excluded Access Groups are included.</p> <p>If the grid is left empty (i.e. no Access Group is added to the Include Access Groups grid), then all Cardholders are included except those who are a member of the excluded Access Group(s).</p>									
Exclude Access Groups	<p>All cardholders are included except those that are members of the excluded Access Groups.</p> <p>If the grid is left empty (i.e. no Access Group is added to the Exclude Access Groups grid), all Cardholders who are not a member of the included Access Group(s) are excluded.</p>									
11	Click the Rule Parameters tab	Click the Rule Parameters tab.								

3.3 Configuring a Regulated Zone Rule

Types of Regulated Zone Rules

Regulated Zones can be configured using five different rules.

Rule	Description
Cumulative duration	Used to monitor Cardholders' accumulated time on site across multiple shifts.
Break duration	Used to monitor Cardholders' minimum break period between shifts.
Maximum duration	Used to monitor Cardholders' time on site within a single shift (period of time).
Predictive cumulative duration	Used to monitor Cardholders' accumulated time on site across multiple shifts and predict if a Cardholder will exceed the cumulative limit.
Shift management	Used to monitor Cardholders' shift patterns.
Maximum entries	Used to monitor the maximum number of times a Cardholder can enter a Regulated Zone within a period.

Rule conflicts

Be careful not to configure a rule that conflicts with another rule for the Regulated Zone. Rule conflicts that can occur are:

- The temporary exit **Grace period** and/or **Competency action delay** must be less than the maximum time limit within one shift and less than the **Break period**.
- The **Maximum duration** must be less than the **Total time limit across shifts**.
- The **Total time limit across shifts** value must be less than the value of **Within last**.
- The **Time in zone** value must be less than the value of **Within last**.

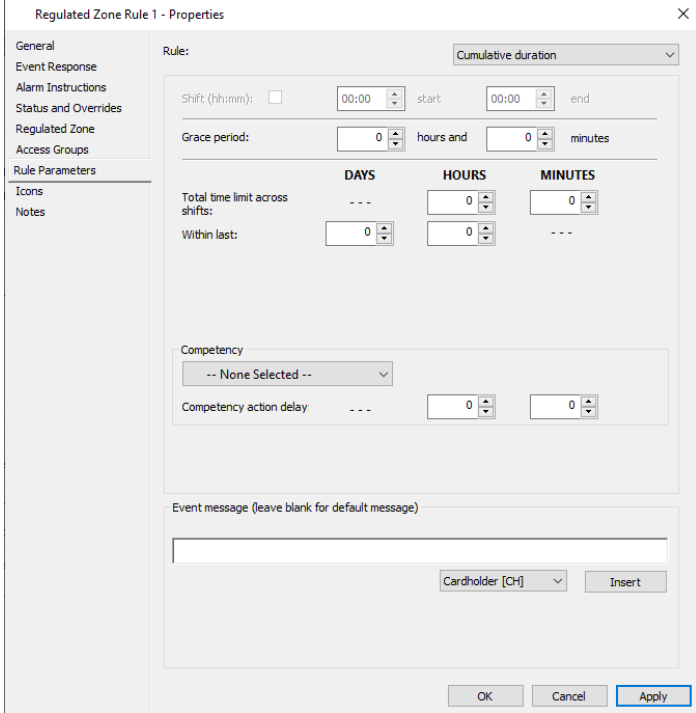
In this section

Refer to the appropriate procedure in this section to configure the different types of Regulated Zone Rules:

To configure a Regulated Zone Rule using...	Go to...
Cumulative duration	page 19
Break duration	page 21
Maximum duration	page 23
Predictive cumulative duration	page 24
Shift management	page 26
Maximum entries	page 30

Cumulative duration

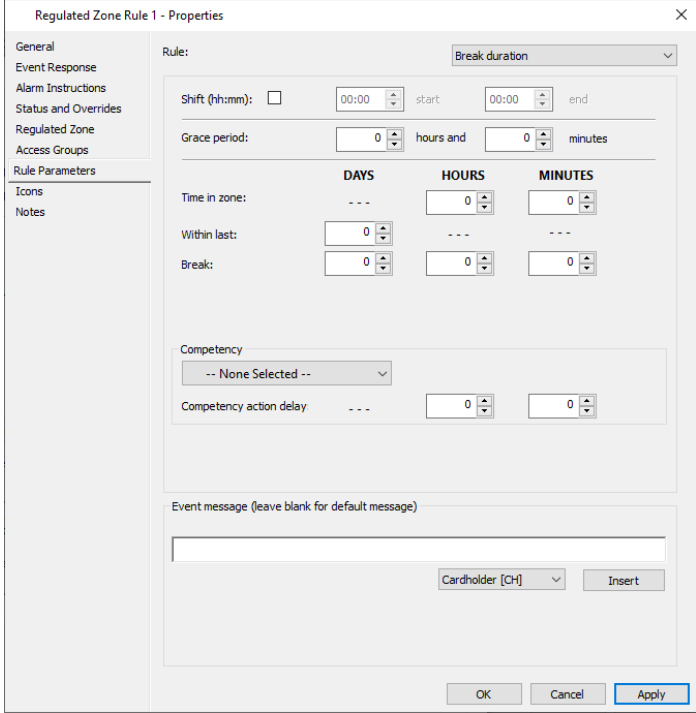
To configure a Regulated Zone Rule using Cumulative duration, perform the following procedure. Required fields are indicated by a *.

Step	Action	Description
1	Select 'Cumulative duration'	<p>Select the 'Cumulative duration' rule from the 'Rule' drop-down list.</p> 
2	Grace Period	<p>In the 'Grace Period' field, enter the duration for ignoring out-of-regulated-zone exit and re-entry events for the purpose of monitoring regulated hours.</p> <p>Example: Cardholders leave the site for a break and are usually away for no longer than 10 minutes. Command Centre will ignore the exit and re-entry events, for the purpose of monitoring on-site regulated hours.</p>
3	*Total time limit across shifts	<p>In the 'Total time limit across shifts' field, enter the total length of time across multiple shifts before a <i>Regulation Cumulative duration breach</i> alarm is raised.</p> <p>Example: Cardholders must not exceed 70 hours on-site within a week. If a Cardholder is on-site for more than 70 hours within one week, a <i>Regulation Cumulative Shift breach</i> alarm is raised.</p>
4	*Within last	<p>In the 'Within last' field, enter the total length of time during which a Cardholder can only be in the Regulated Zone for the cumulative limit without breaching the rule.</p> <p>Example: within the last 5 days, a Cardholder can only work 70 hours.</p>

Continued on next page

5	Competency	<p>From the 'Competency' drop-down list, select the Competency that will be automatically disabled upon rule violation. The Competency is disabled (after the 'Competency action delay') for a Cardholder when the Cardholder is in violation, and can be manually re-enabled by an Operator.</p> <p>Use case: The Competency can be used to deny access to a Cardholder who is in breach of a rule, or to deny access during Break duration period.</p>
6	Competency action delay	In the 'Competency action delay' field, enter how long a Cardholder can be in violation before their Competency is disabled.
7	Event message	<p>In the 'Event message' field, enter an event message for the rule. Type in text, and insert fields by selecting them from the Event details drop-down list and clicking the Insert button.</p> <p>If left blank, the default event message is:</p> <p><i>"Cardholder <Last Name>, <First Name> exceeded their cumulative shift duration within the Regulated Zone <Regulated Zone 1>"</i></p>
8	Icons tab	Click the Icons tab if you want to change the Icon Set for this Regulated Zone Rule.
9	Notes tab	Click the Notes tab if you want to add any notes about this Regulated Zone Rule.
10	Click OK	Click OK to close and save the Cumulative duration Rule.

Break duration To configure a Regulated Zone Rule using Break duration, perform the following procedure. Required fields are indicated by a *.

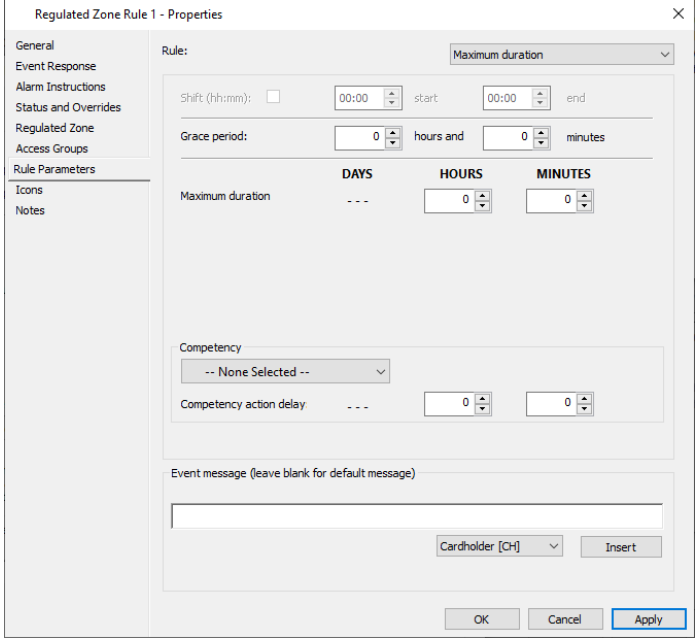
Step	Action	Description
1	Select 'Break duration'	Select the 'Break duration' rule from the 'Rule' drop-down list. 
2	Shift	In the 'Shift' field, enter the spanned time period that the rule applies within. Select the Shift check box to enable start and end fields. If the start and end values are the same (i.e. Start: 18:00, End:18:00), then the rule applies at all times.
3	Grace Period	In the 'Grace Period' field, enter the duration for ignoring out-of-regulated-zone exit and re-entry events for the purpose of monitoring regulated hours. Example: Cardholders leave the site for a break and are usually away for no longer than 10 minutes. Command Centre will ignore the exit and re-entry events, for the purpose of monitoring on-site regulated hours.
4	Time in zone	In the 'Time in zone' field, enter the minimum number of hours a Cardholder is in the Regulated Zone during a single shift.
5	Within last	In the 'Within last' field, enter the total number of days a Cardholder can be in the Regulated Zone before being required to take a break. Specifically, the maximum number of days a Cardholder can be in the Regulated Zone since 'Time in zone' during a Shift has been reached.

Continued on next page

6	*Break	<p>In the 'Break' field, enter the minimum length of time the Cardholder must take as a break between shifts before a <i>Regulation Break duration violation</i> alarm is raised.</p> <p>Example: Cardholders must have at least 10 hours off-site between shifts before they can come back on-site. If a Cardholder re-enters the site within these 10 hours, a <i>Regulation Break duration violation</i> alarm is raised.</p>
7	Competency	<p>From the 'Competency' drop-down list, select the Competency that will be automatically disabled upon rule violation.</p> <p>If a Cardholder is in violation of the rule, the Competency is disabled (after the 'Grace period' and 'Competency action delay') when the Cardholder exits the Regulated Zone.</p> <p>The competency is re-enabled after the Break duration period.</p> <p>Use case: The Competency can be used to deny access to a Cardholder who is in breach of a rule, or to deny access during Break duration period.</p>
8	Competency action delay	<p>In the 'Competency action delay' field, enter how long a Cardholder can be in violation before their Competency is disabled.</p>
9	Event message	<p>In the 'Event message' field, enter an event message for the rule. Type in text, and insert fields by selecting them from the Event details drop-down list and clicking the Insert button.</p> <p>If left blank, the default event message is:</p> <p><i>"Cardholder <Last Name>, <First Name> entered the Regulated Zone <Regulated Zone 1> before the minimum break duration"</i></p>
10	Icons tab	<p>Click the Icons tab if you want to change the Icon Set for this Regulated Zone Rule.</p>
11	Notes tab	<p>Click the Notes tab if you want to add any notes about this Regulated Zone Rule.</p>
12	Click OK	<p>Click OK to close and save the Break duration Rule.</p>

Maximum duration

To configure a Regulated Zone Rule using Maximum duration, perform the following procedure. Required fields are indicated by a *.

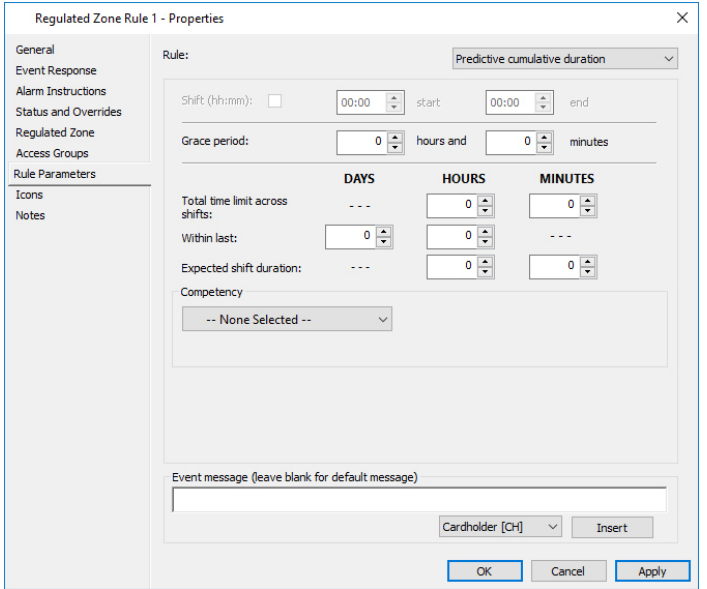
Step	Action	Description
1	Select 'Maximum duration'	<p>Select the 'Maximum duration' rule from the 'Rule' drop-down list.</p> 
2	Grace Period	<p>In the 'Grace Period' field, enter the duration for ignoring out-of-regulated-zone exit and re-entry events for the purpose of monitoring regulated hours.</p> <p>Example: Cardholders leave the site for a break and are usually away for no longer than 10 minutes. Command Centre will ignore the exit and re-entry events, for the purpose of monitoring on-site regulated hours.</p>
3	*Maximum duration	<p>In the 'Maximum duration' field, enter the maximum length of time for a single shift before a Regulation Shift length breach alarm is raised.</p> <p>Example: Cardholders are allowed on-site for 14 hours. If a Cardholder is on-site for more than 14 hours, a Regulation Maximum duration breach alarm is raised.</p>
4	Competency	<p>From the 'Competency' drop-down list, select the Competency that will be automatically disabled upon rule violation.</p> <p>The Competency is disabled (after the 'Competency action delay') when the Cardholder is in violation, and can be manually re-enabled by an Operator.</p> <p>Use case: The Competency can be used to deny access to a Cardholder who is in breach of a rule, or to deny access during Break duration period.</p>

Continued on next page

5	Competency action delay	In the 'Competency action delay' field, enter how long a Cardholder can be in violation before their Competency is disabled.
6	Event message	In the 'Event message' field, enter an event message for the rule. Type in text, and insert fields by selecting them from the Event details drop-down list and clicking the Insert button. If left blank, the default event message is: <i>"Cardholder <Last Name>, <First Name> exceeded their time within the Regulated Zone <Regulated Zone 1>"</i>
7	Icons tab	Click the Icons tab if you want to change the Icon Set for this Regulated Zone Rule.
8	Notes tab	Click the Notes tab if you want to add any notes about this Regulated Zone Rule.
9	Click OK	Click OK to close and save the Maximum duration Rule.

Predictive cumulative duration

To configure a Regulated Zone Rule using Predictive cumulative duration, perform the following procedure. Required fields are indicated by a *.

Step	Action	Description
1	Select 'Predictive cumulative duration'	Select the 'Predictive cumulative duration' rule from the 'Rule' drop-down list. 

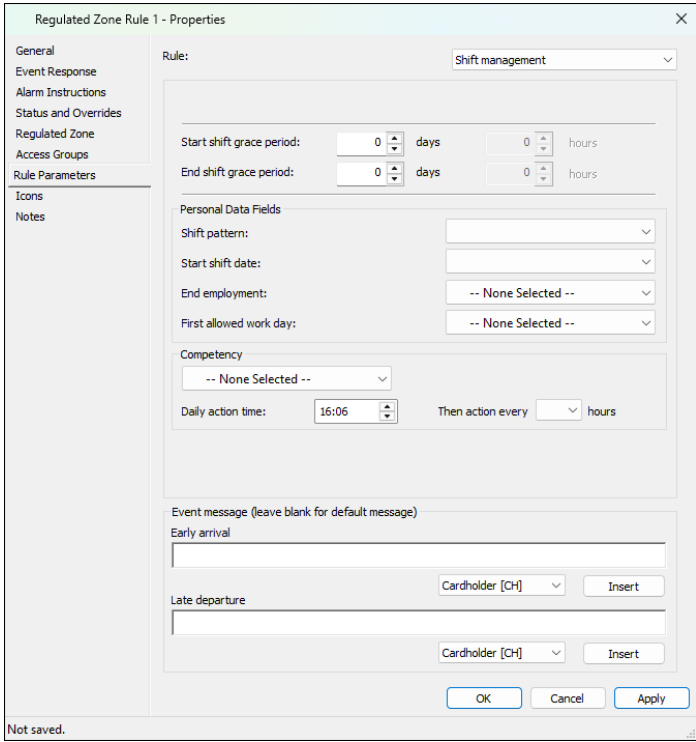
Continued on next page

2	Grace Period	<p>In the 'Grace Period' field, enter the duration for ignoring out-of-regulated-zone exit and re-entry events for the purpose of monitoring regulated hours.</p> <p>Example: Cardholders leave the site for a break and are usually away for no longer than 10 minutes. Command Centre will ignore the exit and re-entry events, for the purpose of monitoring on-site regulated hours.</p>
3	*Total time limit across shifts	<p>In the 'Total time limit across shifts' field, enter the total length of time across multiple shifts.</p> <p>Example: Cardholders must not exceed 70 hours on-site within one week.</p>
4	*Within last	<p>In the 'Within last' field, enter the length of time during which a Cardholder can only be in the Regulated Zone for the cumulative limit.</p> <p>Example: to limit a Cardholder to 70 hours in 5 days, set the 'Within last' to 5 days.</p>
5	*Expected Shift duration	<p>In the 'Expected Shift duration' field, enter the total number of hours a Cardholder is expected to be in a zone during one shift.</p>
6	Competency	<p>From the 'Competency' drop-down list, select the Competency that will be automatically disabled upon rule violation when the Cardholder is predicted to exceed the cumulative limit.</p> <p>If a Cardholder is in violation of the rule, the Competency is disabled (after the 'Competency action delay') when the Cardholder exits the Regulated Zone.</p> <p>The Competency is re-enabled once the Cardholder cannot possibly spend more than the Total time limit across shifts inside the zone within the Within last period, even if they spent the entire remainder of the Within last period inside the zone. For examples, see section 11 "Predictive Cumulative Duration Examples" later in this release note.</p> <p>Use case: The Competency can be used to deny access to a Cardholder who is in breach of a rule.</p>
7	Event message	<p>In the 'Event message' field, enter an event message for the rule. Type in text, and insert fields by selecting them from the Event details drop-down list and clicking the Insert button.</p> <p>If left blank, the default event message is:</p> <p><i>"Cardholder <Last Name>, <First Name> predicted to exceed their cumulative shift duration within the Regulated Zone <Regulated Zone 1>"</i></p>
8	Icons tab	<p>Click the Icons tab if you want to change the Icon Set for this Regulated Zone Rule.</p>
9	Notes tab	<p>Click the Notes tab if you want to add any notes about this Regulated Zone Rule.</p>
10	Click OK	<p>Click OK to close and save the Predictive cumulative duration Rule.</p>

Shift management To configure a Regulated Zone Rule using Shift management, perform the following procedure. Required fields are indicated by a *.

Step	Action	Description										
1	Create PDFs	<p>Before you configure a Regulated Zone using Shift management, ensure you have configured the following Personal Data Fields (PDFs). If required, refer to the topic "<i>Creating a new Personal Data Field</i>" in the Gallagher Configuration Client Help.</p> <table border="1"> <thead> <tr> <th>PDF name</th> <th>Configuration</th> </tr> </thead> <tbody> <tr> <td>'Shift pattern'</td> <td> <p>Create the PDF of 'Text' Data type or 'Text-List' Data type as required for the Shift patterns of your Cardholders.</p> <p>If using 'Text' Data type, Gallagher recommends that you use the following regular expression: <code>^\d\d?x\d\d?(x\d\d?x\d\d?)?\$</code></p> <p>If using 'Text-List' Data type, add the List Values for all shift patterns that you want to be possible (e.g. 7x7, 10x10 etc.).</p> </td> </tr> <tr> <td>'Start shift date'</td> <td>Create the PDF of 'Date' Data type as required for the Start shift dates (first day of employment) of your Cardholders.</td> </tr> <tr> <td>'End employment'</td> <td>Create the PDF of 'Date' Data type as required for the End employment dates (last day of employment) of your Cardholders. This PDF is optional.</td> </tr> <tr> <td>'First allowed work day'</td> <td>Create the PDF of 'Date' Data type as required for the First allowed work day dates of your Cardholders. This PDF is only required if the First allowed work day is a later date than the Start shift date (may occur when changing a Cardholder's Shift pattern).</td> </tr> </tbody> </table>	PDF name	Configuration	'Shift pattern'	<p>Create the PDF of 'Text' Data type or 'Text-List' Data type as required for the Shift patterns of your Cardholders.</p> <p>If using 'Text' Data type, Gallagher recommends that you use the following regular expression: <code>^\d\d?x\d\d?(x\d\d?x\d\d?)?\$</code></p> <p>If using 'Text-List' Data type, add the List Values for all shift patterns that you want to be possible (e.g. 7x7, 10x10 etc.).</p>	'Start shift date'	Create the PDF of 'Date' Data type as required for the Start shift dates (first day of employment) of your Cardholders.	'End employment'	Create the PDF of 'Date' Data type as required for the End employment dates (last day of employment) of your Cardholders. This PDF is optional.	'First allowed work day'	Create the PDF of 'Date' Data type as required for the First allowed work day dates of your Cardholders. This PDF is only required if the First allowed work day is a later date than the Start shift date (may occur when changing a Cardholder's Shift pattern).
PDF name	Configuration											
'Shift pattern'	<p>Create the PDF of 'Text' Data type or 'Text-List' Data type as required for the Shift patterns of your Cardholders.</p> <p>If using 'Text' Data type, Gallagher recommends that you use the following regular expression: <code>^\d\d?x\d\d?(x\d\d?x\d\d?)?\$</code></p> <p>If using 'Text-List' Data type, add the List Values for all shift patterns that you want to be possible (e.g. 7x7, 10x10 etc.).</p>											
'Start shift date'	Create the PDF of 'Date' Data type as required for the Start shift dates (first day of employment) of your Cardholders.											
'End employment'	Create the PDF of 'Date' Data type as required for the End employment dates (last day of employment) of your Cardholders. This PDF is optional.											
'First allowed work day'	Create the PDF of 'Date' Data type as required for the First allowed work day dates of your Cardholders. This PDF is only required if the First allowed work day is a later date than the Start shift date (may occur when changing a Cardholder's Shift pattern).											

Continued on next page

2	Select 'Shift management'	<p>Select the 'Shift management' rule from the 'Rule' drop-down list.</p> 
3	Start shift grace Period	In the 'Start shift grace Period' field, enter the duration (in days) for ignoring early site access, to allow Cardholders to arrive on-site up to three days early.
4	End shift grace Period	In the 'End shift grace Period' field, enter the duration (in days) for ignoring late site exit, to allow Cardholders to leave the site up to three days late.
5	*Shift pattern	From the 'Shift pattern' drop-down list, select the configured Personal Data Field (PDF) for the various shift patterns of Cardholders. Each Cardholder needs their own data entry for their Shift pattern (e.g. 7x7).
6	*Shift start date	From the 'Shift start date' drop-down list, select the configured PDF for the shift start dates of Cardholders. Each Cardholder needs their own data entry for their Shift start date (e.g. 06/04/2021).
7	End employment	From the 'End employment' drop-down list, select the configured PDF for the last day of employment (if known) for Cardholders. If a Cardholder has this date set, they will not be able to access the site without raising an alarm after this date.

Continued on next page

8	First allowed work day	<p>From the 'First allowed work day' drop-down list, select the configured PDF for the first day a Cardholder will be allowed site access. Cardholders need only have a data entry for this PDF when it is a later date than the Start shift date.</p> <p>Example: if a Cardholder was changing Shift pattern from 7x7 to 5x2, according to their new Shift pattern they only need a two-day break after finishing their last seven-day shift. First allowed work day should be set to ensure that they still have seven days off after finishing the last shift of their 7x7 Shift pattern, before they begin the 5x2 pattern.</p>
9	Competency	<p>From the 'Competency' drop-down list, select the Competency that will be automatically disabled when a Cardholder's shift - including the End shift grace period - has finished, and enabled at the start of the Start shift grace period.</p> <p>Use case: The Competency can be used to deny access to a Cardholder whose shift has not yet started.</p>
10	Daily action time	<p>In the 'Daily action time' field, enter the time of day (in 24-hour time) when the rule checks all affected Cardholders for necessary expiries, disablements, or re-enablements of the Competency. Any required expiries, disablements or re-enablements are made at this time.</p>
11	Then action every ...	<p>From the 'Then action every <i>n</i> hours' field, select a frequency for how often the rule checks Competencies after the 'Daily action time'. These checks are identical to the 'Daily action time' check.</p> <p>The 'Daily action time' provides a baseline time, from which the other action times are determined depending on the frequency.</p> <p>Example: If you enter 10:00 in the 'Daily action time' and select a frequency of 6, it will check Competencies at 10:00 and every 6 hours after 10:00, meaning checks will happen at 10:00, 16:00, 22:00, and 04:00 every day.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Daily action time: <input type="text" value="10:00"/> Then action every <input type="text" value="6"/> hours</p> </div>
12	Event message	<p>In the 'Event message' fields, enter event messages for the rule. For Shift management, 'Event message' has separate messages for Early arrival and Late departure. Enter messages for both, one of, or neither event types. Type in text, and insert fields by selecting them from the Event details drop-down list and clicking the Insert button.</p> <p>If either field is left blank, the default event messages are:</p> <ul style="list-style-type: none"> • Early arrival: "Cardholder <Last Name>, <First Name> arrived too early into Regulated Zone <Regulated Zone 1>" • Late departure: "Cardholder <Last Name>, <First Name> has not departed from Regulated Zone <Regulated Zone 1>"

Continued on next page

13	Icons tab	Click the Icons tab if you want to change the Icon Set for this Regulated Zone Rule.
14	Notes tab	Click the Notes tab if you want to add any notes about this Regulated Zone Rule.
15	Click OK	Click OK to close and save the Break duration Rule.

Competency action times

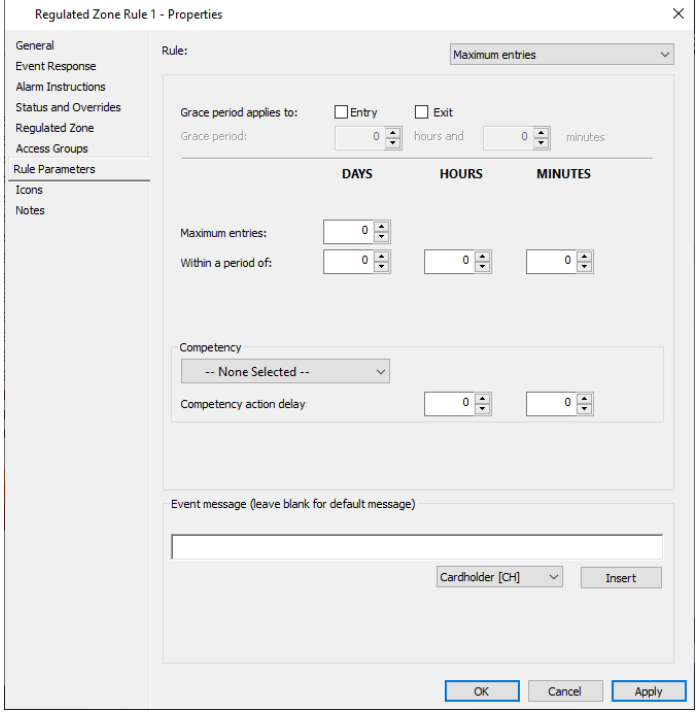
A Shift Management Regulated Zone Rule checks affected Cardholders for necessary expiries, disablements, or re-enablements of its Competency at times defined by the 'Daily action time' and 'Then action every *n* hours' settings, as described in the previous procedure.

At each of these action times:

If...	then...
the Cardholder is in their break period	the rule ensures that the Cardholder's Competency: <ul style="list-style-type: none"> • is currently disabled • will re-enable at the time and date that their working period begins, including the start shift grace period.
the Cardholder is in their working period	the rule ensures that the Cardholder's Competency: <ul style="list-style-type: none"> • is currently enabled • will expire at the time and date that their break working period ends, including the end shift grace period.

If an operator makes changes to a Cardholder's Competency (e.g. changes its expiry date), the rule will overwrite the changes as per the above table at the next action time.

Maximum entries To configure a Regulated Zone Rule using Maximum entries, perform the following procedure. Required fields are indicated by a *.

Step	Action	Description
1	Select 'Maximum entries'	Select the 'Maximum entries' rule from the 'Rule' drop-down list. 
2	Grace period applies to	The 'Grace period' (see below for details) can apply to Entry events, Exit events, or both. Select the check boxes as per your requirements. If neither check box is checked, the Grace period is disabled.

Continued on next page

3	Grace period	<p>The 'Grace Period' field defines different things depending on which 'Grace period applies to' check boxes are checked.</p> <p>Exit readers: Grace period functionality requires exit to be controlled by Readers (not push buttons) so Command Centre knows whether a Cardholder has exited a Regulated Zone or not.</p> <p>If the Grace period applies to Entry events, the Grace period defines how long a Cardholder can enter and stay in the Regulated Zone before it counts as one of the Cardholder's limited entries.</p> <p>If the Grace period applies to Exit events, the Grace period defines how long a Cardholder can exit and stay outside the Regulated Zone before it counts as the end of one of the Cardholder's limited entries.</p> <p>If the Grace period applies to both Exit and Entry events, both of the above statements are true.</p> <p>Examples:</p> <ul style="list-style-type: none"> • The 'Entry' check box is checked and the Grace period is set to 3 minutes. A Cardholder enters the break room (the Regulated Zone) and leaves 1 minute later. Command Centre will ignore the entry and exit events; the Cardholder did not use one of their limited entries. • The 'Exit' check box is checked and the Grace period is set to 5 minutes. A Cardholder leaves the break room (the Regulated Zone) for 4 minutes to use the bathroom. Command Centre will ignore the exit and re-entry events; the Cardholder did not use one of their limited entries when they entered the break room again.
4	*Maximum entries	<p>In the 'Maximum entries' field, enter the maximum number of times a Cardholder can enter the Regulated Zone within the specified time period without raising a <i>Regulation maximum entries breach</i> alarm. The minimum value is 1.</p> <p>Example: Cardholders are allowed to enter the break room 3 times per 8-hour period. If a Cardholder enters the break room 4 times within 8 hours, a <i>Regulation maximum entries breach alarm</i> is raised.</p>
5	*Within a period of	<p>In the 'Within a period of' field, enter the time period that Cardholders are restricted to a maximum number of entries within.</p> <p>Example: If 'Maximum entries' is set to '3' and 'Within a period of' is set to 8 hours, Cardholders can enter the Regulated Zone 3 times within 8 hours without breaching the rule. If a Cardholder enters a 4th time within 8 hours, an alarm is raised. Once more than 8 hours have passed since they first entered the zone, they have only entered the zone twice within the last 8 hours, so they can enter the zone again.</p>

Continued on next page

6	Competency	<p>From the 'Competency' drop-down list, select the Competency that will be automatically disabled upon rule violation.</p> <p>The Competency is disabled (after the 'Competency action delay') when the Cardholder has reached the maximum entries allowed within the specified time period, and can be manually re-enabled by an Operator.</p> <p>The competency is automatically re-enabled once enough time has passed such that within the specified time period, the Cardholder has not entered the maximum number of times.</p> <p>Use case: The Competency can be used to deny access to a Cardholder who has used up all of their entries in a period. If a T20 Reader is used, a Competency message can display to tell the Cardholder why they have been denied access.</p>
7	Competency action delay	<p>In the 'Competency action delay' field, enter how much time will pass after a Cardholder uses their last allowed entry before their Competency is disabled.</p> <p>The Competency action delay starts counting down to disable the Competency from the moment a Cardholder enters the Regulated Zone for their last allowed time; <i>not</i> from when the Cardholder is in breach of the Rule. If the Cardholder leaves the Zone within the Grace period (so the entry does not count), then the Competency action is cancelled.</p> <p>Example: The 'Grace period' is set to 5 minutes and the 'Competency action delay' is set to 10 minutes. A Cardholder enters the Zone for their last allowed time, and the Competency action delay starts counting down. If they spend less than 5 minutes in the Zone and then leave, the Competency action is cancelled (the entry did not count). If they spend 5 minutes in the Zone, they are in breach of the Rule. A further 5 minutes later (10 minutes after they entered the Zone), their Competency is disabled.</p>
8	Event message	<p>In the 'Event message' field, enter an event message for the rule. Type in text, and insert fields by selecting them from the Event details drop-down list and clicking the Insert button.</p> <p>If left blank, the default event message is:</p> <p><i>"Cardholder <Last Name>, <First Name> exceeded their maximum entries for Regulated Zone <Regulated Zone name>"</i></p>
9	Icons tab	Click the Icons tab if you want to change the Icon Set for this Regulated Zone Rule.
10	Notes tab	Click the Notes tab if you want to add any notes about this Regulated Zone Rule.
11	Click OK	Click OK to close and save the Maximum entries Rule.

4 Regulated Zone status

Adding Regulated Zones to Status Tiles







To view the status of the Regulated Zone and the Regulated Zone Rules in Command Centre, you need to add the Regulated Zone and the Regulated Zone Rules to a Status Tile. Refer to the topic "*Configuring a Status Tile*" in the Gallagher Command Centre Help.

Notes:

- Gallagher recommends that you order items in the Status tile so that the rules applicable for a Zone are placed directly below that Zone.
- There may be a short time delay between Cardholders' movements and the Status tile updating to reflect those movements.

Status Tile example

The following example shows a Regulated Zone and its Rules in a Status Tile:

Status		
Name	Status	Updated
 Regulated Zone 1	Cardholders inside the Regulated Zone: 0	10/01/2020 11:20:55
 Break Duration	Break duration. Cardholders monitored and without violations: 0. In exit grace period: 0. In rule violation: 0. Monitored by break duration: 0.	10/01/2020 11:20:58
 Predictive Cumulative Duration	Cumulative duration. Cardholders monitored and without violations: 0. In exit grace period: 0. In rule violation: 0.	10/01/2020 11:20:58
 Cumulative Duration	Cumulative duration. Cardholders monitored and without violations: 0. In exit grace period: 0. In rule violation: 0.	10/01/2020 11:20:58
 Maximum Duration	Maximum duration. Cardholders monitored and without violations: 0. In exit grace period: 0. In rule violation: 0.	10/01/2020 11:20:58
 Shift Management	Shift management. Cardholders monitored and without violations: 0. In rule violation: 0.	10/01/2020 11:20:58

Status descriptions

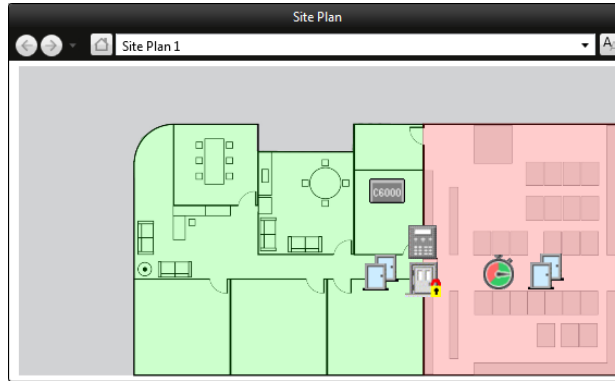
The following table describes the Regulated Zone Command Centre Item status:

Status	Description
Cardholders inside the Regulated Zone [x]	Displays the number of Cardholders within the Regulated Zone.
Maximum duration [x]	Displays the number of Cardholders within the Regulated Zone that are currently exceeding the maximum time limit for a single shift.
Cumulative duration [x]	Displays the number of Cardholders within the Regulated Zone that are currently exceeding the total time limit across multiple shifts.
Break duration [x]	Displays the number of Cardholders within the Regulated Zone who have breached the Break duration rule upon starting their current shift.
Predictive cumulative duration [x]	Displays the number of Cardholders within the Regulated Zone who have breached the Predictive cumulative duration rule upon starting their current shift.
Shift management [x]	Displays the number of Cardholders within the Regulated Zone who have accessed the Zone before their Start shift grace period or have not left since the end of their End shift grace period.
Maximum entries [X]	Displays the number of Cardholders within the Regulated Zone that are currently exceeding the Maximum entries within the specified period.
[x] In exit grace period	Displays the number of Cardholders who have exited the Regulated Zone, but are within the temporary exit grace period.

Adding Regulated Zones to Site Plans

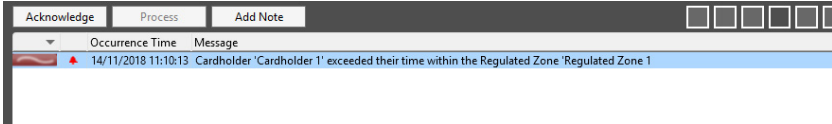
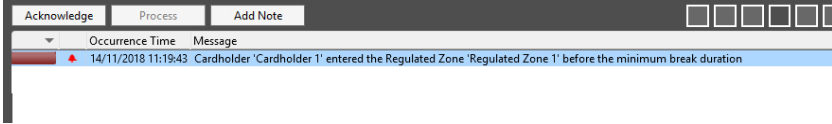
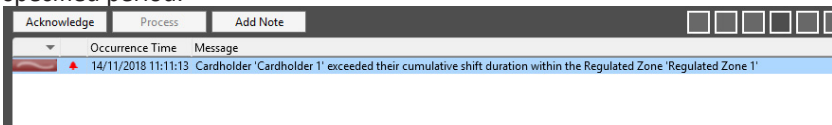
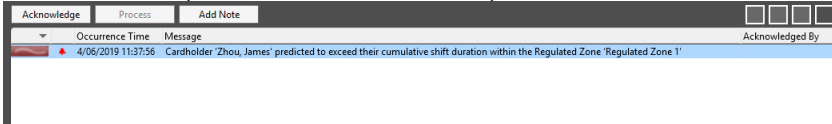
Additionally, a Regulated Zone item can be added to a Site Plan. Refer to the topic *"Editing a Site Plan"* in the Gallagher Configuration Client Help.

The example below monitors Cardholders' time in the chiller:

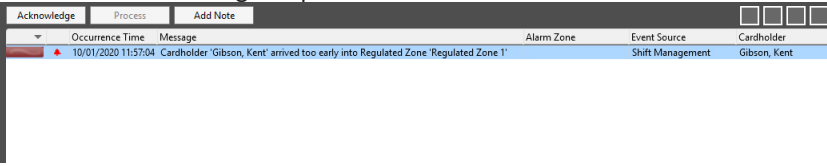
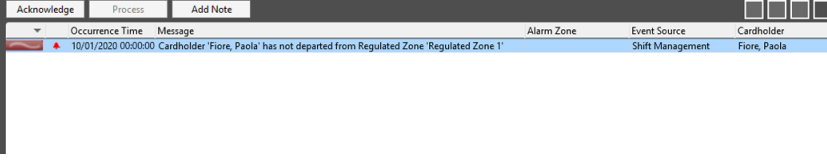
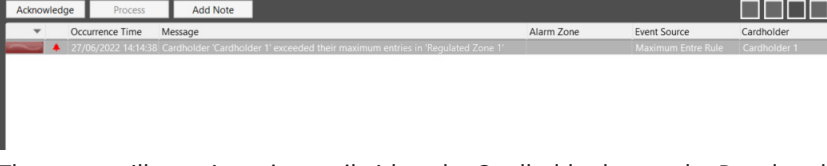
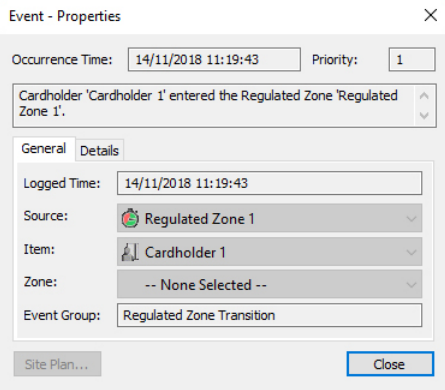
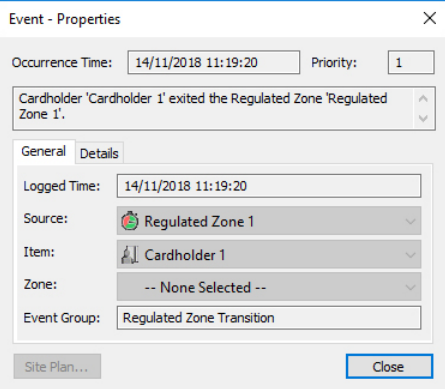


5 Regulation events

Introduced events This feature introduces the following regulation events:

Event	Description
Regulation Maximum duration breach	<p>This event is raised when a Cardholder has been inside the Regulated Zone for a period of time greater than the configured Maximum duration.</p>  <p>The event will remain active until the Cardholder leaves the Regulated Zone and the temporary exit grace period has expired.</p>
Regulation Break duration breach	<p>This event is raised when a Cardholder re-enters the Regulated Zone after the temporary exit grace period has expired, but before the Break duration has ended.</p>  <p>The event will remain active until the Cardholder leaves the Regulated Zone and the temporary exit grace period has expired.</p>
Regulation Cumulative duration Shift breach	<p>This event is raised when a Cardholder has been inside the Regulated Zone for a period greater than the configured Cumulative shift duration, within a specified period.</p>  <p>The event will remain active until the Cardholder leaves the Regulated Zone and the temporary exit grace period has expired.</p>
Regulation Cumulative predictive duration breach	<p>This event is raised when a Cardholder is predicted to exceed the configured cumulative limit (total time limit across shifts).</p>  <p>The event will remain active until the Cardholder leaves the Regulated Zone and the temporary exit grace period has expired.</p>

Continued on next page

<p>Regulation Shift management breach - Early arrival</p>	<p>This event is raised when a Cardholder enters the Regulated Zone before the start of the Start shift grace period.</p>  <p>The event will remain active until the Cardholder leaves the Regulated Zone.</p>
<p>Regulation Shift management breach - Late departure</p>	<p>This event is raised when a Cardholder has not left the Regulated Zone before the end of the End shift grace period.</p>  <p>The event will remain active until the Cardholder leaves the Regulated Zone.</p>
<p>Regulation Maximum entries breach</p>	<p>This event is raised when a Cardholder has exceeded their Maximum entries for the Regulated Zone within the specified period.</p>  <p>The event will remain active until either the Cardholder leaves the Regulated Zone or enough time has passed such that within the specified time period, the Cardholder has no longer exceeded the maximum entries.</p>
<p>Entry Diagnostic event</p>	
<p>Exit Diagnostic event</p>	

6 Reconfiguration

About this section	This section highlights the behaviours that result from certain reconfigurations.
Rule changed for empty Zone	If a rule is changed and no Cardholders are in the Regulated Zone, the status becomes unknown.
Rule changed for occupied Zone	If a rule is changed and a Cardholder is in the Regulated Zone, the status is updated and the rule will come into effect shortly afterwards.
Grace time changed while Cardholder within it	If a Cardholder has a violation and is within the grace time when the grace time is changed, the violation will use the previous grace time (i.e. the grace time as it was set when it started).
Adding to a Regulated Zone's Area Configuration	Adding to the list of Doors, Access Zones or Child Regulated Zones only affects future events. Historical events at those Doors or Zones are not re-introduced into the system.
Adding to a Regulated Zone's Access Groups	Removing excluded Access Groups from the Regulated Zone only affects future events. Historical events for Cardholders that are no longer excluded are not re-introduced into the system if the event has already been processed.
Adding a Rule that a Cardholder is in violation of	Activating a rule while a Cardholder is outside the affected Regulated Zone and in violation of that rule will not raise an event until they move through a Door.

7 Upgrading

If upgrading from Regulated Zones v7.40

Before upgrading this feature from v7.40, note the following:

- In the 7.40 version of this feature, the rules are configured within the Regulated Zone item. However, in the 7.50 version and onwards, the rules are configured as separate items assigned to the Regulated Zone. If you are upgrading this feature from 7.40, Regulated Zone items will be automatically created in Command Centre for any rules that had previously been enabled. The upgrade will automatically append a unique digit to the name of each rule to distinguish it from other rules. The rule description will state "Auto-created during upgrade". After upgrading, you can rename the rules or create additional rules as required.
 - In the 7.40 version of this feature, when the shift duration (now known as Maximum duration) rule is breached, an active alarm is raised; and when an inter-shift (now known as Break duration) or consecutive shift (now known as Cumulative duration) rule is breached, an inactive alarm is raised. After upgrading, all active Maximum duration alarms will become inactive. The system will re-calculate the rule violation and raise a new active alarm for each rule breach.
-

7.1 Upgrading from vEL9.00 (or earlier) to vEL9.10

Procedure

To upgrade Command Centre and this feature to v9.10, perform the following procedure:

Step	Action	Description
1	Backup	Perform a backup of your Command Centre system.
2	Stop Command Centre and Services	Exit Command Centre, stop the Command Centre Services, and stop the FTCAPI Router Service.
3	Uninstall this feature	Using the Windows Programs and Features utility, remove the program 'Gallagher Regulated Zones' from the Command Centre Server and all Command Centre Workstations.
4	Upgrade Command Centre	Upgrade Command Centre to vEL9.10.1005 (or later vEL9.10 release). Refer to the document " <i>3E0068 Release Note Command Centre vEL9.10 (Upgrade Procedures).pdf</i> " located on the Command Centre installation media.
5	Install new version	Install the new 'Gallagher Regulated Zones' feature you have been provided. Refer to section 2 " <i>Installation</i> " earlier in this release note.

7.2 Upgrading on vEL9.10

Procedure If Command Centre vEL9.10 is already installed, perform the following procedure to upgrade this feature to v9.10:

Step	Action	Description
1	Backup	Perform a backup of your Command Centre system.
2	Stop Command Centre and Services	Exit Command Centre, stop the Command Centre Services, and stop the FTCAPI Router Service.
3	Uninstall this feature	Using the Windows Programs and Features utility, remove the program 'Gallagher Regulated Zones' from the Command Centre Server and all Command Centre Workstations.
4	Install new version	Install the new 'Gallagher Regulated Zones' feature you have been provided. Refer to section 2 " Installation " earlier in this release note.

8 Uninstallation

Procedure To uninstall this feature, perform the following procedure:

Step	Action	Description
1	Backup	Perform a backup of your Command Centre system.
2	Delete Regulated Zone items	Delete all Regulated Zone Command Centre Items. IMPORTANT: If you do not delete all Regulated Zone items before uninstalling this feature, the Command Centre services can fail to start. If you encounter this issue, reinstall Regulated Zones, delete the items, then uninstall it again.
3	Stop Command Centre and Services	Exit Command Centre and stop the Command Centre Services.
4	Uninstall this feature	Using the Windows Programs and Features utility, remove the program 'Gallagher Regulated Zones' from the Command Centre Server and all Command Centre Workstations.
5	Start Services and Command Centre	Restart the Command Centre Services and Command Centre.

9 Considerations

Leaving many alarms unprocessed

If a large number of alarms remain unprocessed, this may result in performance issues. Gallagher advises that alarms are processed accordingly.

Turning Rules on and off

To turn a Regulated Zone Rule ON or OFF, you must remove the Regulated Zone assignment from the Regulated Zone Rule (when removed, the rule will display as un-configured; a blue jigsaw overlay appears on the icon).

Conflicting Rules

Be careful not to configure a rule that conflicts with another rule for the Regulated Zone. The system does not check all rule conflicts between rule items.

The system operator

If you log on as "system operator" in a Command Centre multi-server environment, you will see alarms from all Servers. To view local alarms only, configure a local operator group for the local Server.

Changing the 'Configuration via' option

If you change the **Configuration via** option on a Regulated Zone (between Access Zones, Doors, or Child Regulated Zones), the new configuration will immediately take effect, but the items set in the previous **Configuration via** grid(s) will remain linked to the Regulated Zone.

If you try to delete a Child Regulated Zone, Access Zone, or Door that isn't used by the Regulated Zone anymore but is still linked to the previous **Configuration via** option, you may get an error message such as "this item cannot be deleted as there is a Regulated Zone that depends upon it for proper operation". The item you are trying to delete is still a child of the Regulated Zone, even though the Regulated Zone has been reconfigured. If you want to delete an item that is in use by a Regulated Zone, follow this procedure:

1. Change the **Configuration via** option of the Regulated Zone to use the item type you are trying to delete (e.g. if you want to delete a Door, reconfigure the Regulated Zone to use Doors).

Do not click Apply yet.

2. Remove the item (e.g. the Door) that you want to delete.
 3. Change the **Configuration via** option back to how it was before.
 4. Click **OK**.
 5. Delete the item from the system.
-

10 Examples

The following examples provide an explanation of how the Maximum duration and Break duration rules work when both applied to a local Access Zone.

Key:

- ↔ Working
- ↔ Resting
- ↓ Maximum duration rule Competency is disabled
- ↓ Alarm raised
- ↑ Break duration rule Competency is enabled
- ↓ Break duration rule Competency is disabled
- ↔ 2 hours Grace Period
- ↔ 8 hours

Example 1

The site is configured to have 14 hours of work time followed by 10 hours of rest time.

Configuration

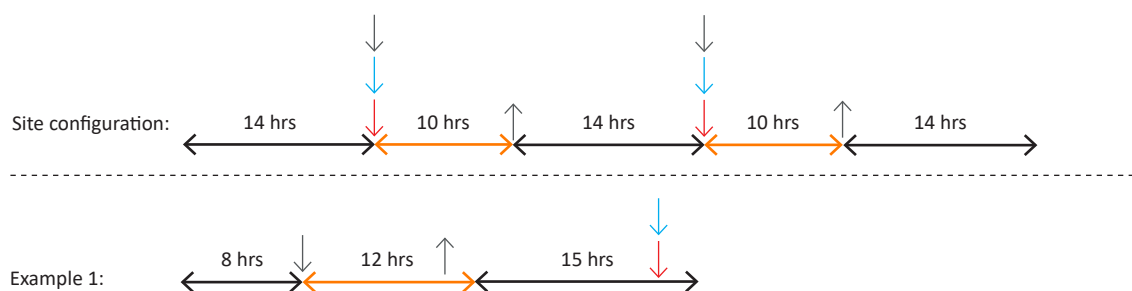
Two different rules are configured.

1. Break duration

Shift	Time in zone	Within last	Break
			10 hrs

2. Maximum duration

Maximum duration
14 hrs



The Cardholder works for 8 hours, rests for 12 hours, then works for 15 hours. An alarm is raised due to the Cardholder working longer than the set 14 hours during a shift.

- 0900h Cardholder starts work
- 1600h Cardholder leaves; Break duration rule Competency disables
- 0200h Break duration rule Competency enables
- 0400h Cardholder starts work
- 1900h Maximum duration rule Competency disables; alarm is raised

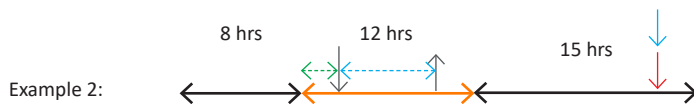
Example 2

As in Example 1, the site is configured to have 14 hours of work time followed by 10 hours of rest time; and the Cardholder works for 8 hours, rests for 12 hours, then works for 15 hours.

The Break duration Grace Period is 2 hours.

When the Cardholder badges out after 8 hours, the 2-hour Break duration Grace Period starts. At the end of the Grace Period, the Break duration rule Competency is disabled, and re-enables after another 8 hours.

An alarm is raised due to the Cardholder working longer than 14 hours during a shift.



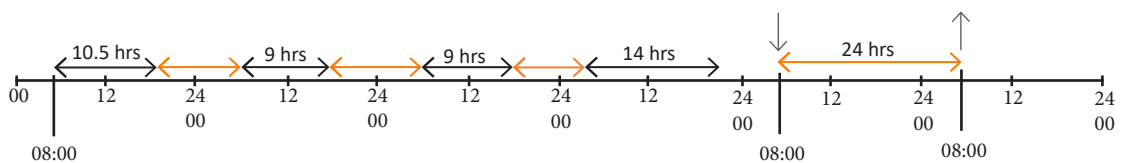
- 0900h Cardholder starts work
- 1600h Cardholder leaves; grace period starts
- 1900h Break duration rule Competency disables; grace period ends
- 0200h Break duration rule Competency enables
- 0400h Cardholder starts work
- 1900h Maximum duration rule Competency disables; alarm is raised

Break duration (only)

The site is configured to have 10 hours (or longer) of work between 07:00 and 17:00. After 4 days, 24 hours of rest is required.

Note: In this example, there is no Maximum duration rule configured.

Shift	Time in zone	Within last	Break
07:00-19:00	10 hours	4 days	24 hours



- 0800h Cardholder starts work
- 1830h Cardholder leaves; Break duration rule Competency stays enabled
- 0900h Cardholder starts work
- 1800h Cardholder leaves; Break duration rule Competency stays enabled
- 0900h Cardholder starts work
- 1800h Cardholder leaves; Break duration rule Competency stays enabled
- 0700h Cardholder starts work
- 2100h Cardholder leaves; Break duration rule Competency stays enabled
- 0800h Break duration rule Competency disables; alarm is raised

Note: In this example, all the rest periods between the shifts are less than 24 hours. Since the Cardholder went 4 days with no 24-hour break and did at least one shift longer than 10 hours between 07:00 and 19:00 during this time, the Cardholder is required to take a 24-hour break.

11 Predictive Cumulative Duration Examples

Key:

↔ Working

↔ Resting

↓ Alarm raised

↑ Predictive cumulative duration rule Competency is enabled

↓ Predictive cumulative duration rule Competency is disabled

■ A period during which a Competency is disabled, and the Cardholder should be off-site

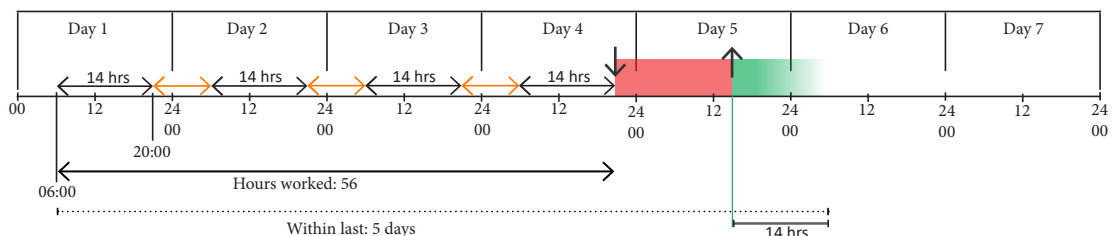
■ A period during which a Zone can be entered without breaching the rule

Example 1: Configured using Competency

The site is configured as:

Parameter	Value
Total time limit across shifts	70 hours
Within last	5 days
Expected shift duration	14 hours
Competency	Yes - Competency 1

Note: You can configure a Competency against the Predictive cumulative duration rule to assist with the enforcement of the rule. The Competency is disabled when the Cardholder is predicted to exceed the Total time across multiple shifts, therefore denying access to the Cardholder (if the Competency is used on the Access Zone).



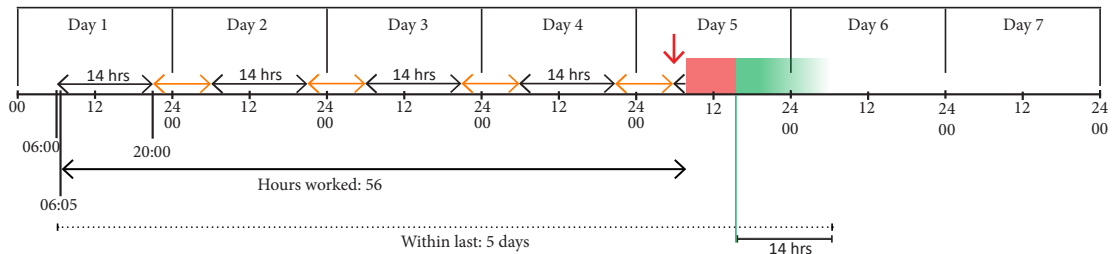
- Day 1** 0600h Cardholder starts work
- 2000h Cardholder leaves; Predictive Cumulative Duration rule Competency stays enabled
- Day 2** 0600h Cardholder starts work
- 2000h Cardholder leaves; Predictive Cumulative Duration rule Competency stays enabled
- Day 3** 0600h Cardholder starts work
- 2000h Cardholder leaves; Predictive Cumulative Duration rule Competency stays enabled
- Day 4** 0600h Cardholder starts work
- 2000h Cardholder leaves, Cardholder has been in the Zone for 56 hours; Predictive cumulative duration rule Competency disables
- Day 5** 1600h After 20 hours off-site; Predictive cumulative duration rule Competency is enabled. At this time, the Cardholder can not possibly spend more than 70 hours in the zone within 5 days of when they entered on day 1, even if they spend all the remaining 14 hours of the 5-day period in the zone. They are therefore predicted to not violate the rule.

Example: Configured without a Competency

The site is configured as:

Parameter	Value
Total time limit across shifts	70 hours
Within last	5 days
Expected shift duration	14 hours
Competency	No

Note: When the Predictive rule is configured without a Competency, then a Competency is not disabled when a Cardholder is predicted to exceed the limit or when the Predictive rule is breached. Therefore, such configuration should only be used if you do not need to deny access to the site when the Predictive rule is breached.



- Day 1** 0600h Cardholder starts work
- 2000h Cardholder leaves
- Day 2** 0600h Cardholder starts work
- 2000h Cardholder leaves
- Day 3** 0600h Cardholder starts work
- 2000h Cardholder leaves
- Day 4** 0600h Cardholder starts work
- 2000h Cardholder leaves; The Cardholder is predicted to exceed the 70 hour limit if they enter again before 5 days have passed since they entered on day 1.
- Day 5** 0600h Cardholder enters the Zone; Predictive cumulative duration alarm is raised
- 0605h Cardholder leaves
- Day 5** 1605h Cardholder can enter the Zone without violating the rule. At this time, the Cardholder can not possibly spend more than 70 hours in the zone within 5 days of when they entered on day 1, even if they spend all the remaining 14 hours of the 5-day period in the zone. They are therefore predicted to not violate the rule.

12 Break Duration Scenarios

Scenario	Time in zone	Shift	Within last	Break
1	10 hours	18:00-06:00	4 days	24 hours
2	6	18:00-06:00		12 hours
3	32		3 days	24 hours
4	14 hours			10 hours
5		18:00-06:00	6 days	12 hours
6		18:00-06:00		6 hours
7			5 days	48 hours
8				24 hours

Scenario	Time in zone	Shift	Within last	Break
1	10 hours	18:00-06:00	4 days	24 hours

If a Cardholder does a 10-hour shift or longer, between 18:00 and 06:00, and it has been 4 days since the Cardholder took a 24-hour break, then the Cardholder must take 24 hours break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

1. When the Cardholder exits the Regulated Zone, the Competency is disabled for 24 hours.
2. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
3. After 24 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

Scenario	Time in zone	Shift	Within last	Break
2	6	18:00-06:00		12 hours

If a Cardholder does a 6-hour shift or longer, between 18:00 and 06:00, then the Cardholder must take 12 hours break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

1. When the Cardholder exits the Regulated Zone, the Competency is disabled for 12 hours.
2. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
3. After 12 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

Scenario	Time in zone	Shift	Within last	Break
3	32		3 days	24 hours

If a Cardholder does a 32-hour shift or longer, and it has been 3 days since the Cardholder took a break of 24 hours, then the Cardholder must take 24 hours break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

1. When the Cardholder exits the Regulated Zone, the Competency is disabled for 32 hours.
2. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
3. After 32 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

Scenario	Time in zone	Shift	Within last	Break
4	14 hours			10 hours

If a Cardholder does a 14-hour shift or longer, then the Cardholder must take 10 hours break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

1. When the Cardholder exits the Regulated Zone, the Competency is disabled for 10 hours.
2. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
3. After 10 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

Scenario	Time in zone	Shift	Within last	Break
5		18:00-06:00	6 days	12 hours

If a Cardholder spends any time in the Regulated Zone, between 18:00 and 06:00, and it has been 6 days since the Cardholder took a break of 12 hours, then the Cardholder must take 12 hours break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

4. When the Cardholder exits the Regulated Zone, the Competency is disabled for 12 hours.
5. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
6. After 12 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

Scenario	Time in zone	Shift	Within last	Break
6		18:00-06:00		6 hours

If a Cardholder spends any time in the Regulated Zone, between 18:00 and 06:00, then the Cardholder must take 6 hours break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

1. When the Cardholder exits the Regulated Zone, the Competency is disabled for 6 hours.
2. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
3. After 6 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

Scenario	Time in zone	Shift	Within last	Break
7			5 days	48 hours

If a Cardholder spends any time in the Regulated Zone, and it has been 5 days since the Cardholder took a break of 48 hours, then the Cardholder must take 48 hours break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

1. When the Cardholder exits the Regulated Zone, the Competency is disabled for 48 hours.
2. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
3. After 48 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

Scenario	Time in zone	Shift	Within last	Break
8				24 hours

If a Cardholder spends any time in the Regulated Zone, then the Cardholder must take a 24-hour break after exiting the Regulated Zone.

As soon as the condition above is met, then the following events take place:

1. When the Cardholder exits the Regulated Zone, the Competency is disabled for 24 hours.
2. If a Competency is not configured against the rule, and the Cardholder enters the zone before the break period ends, then an alarm is raised.
3. After 24 hours, the Competency is enabled to allow the Cardholder to access the Regulated Zone.

13 Shift Management Scenarios

Scenario 1:

In this scenario, the Cardholder has a 7x7 Shift pattern (seven days work, seven days break).

Start shift grace period	1 day	First allowed work day	
End shift grace period	1 day	Competency	Site Access
Shift pattern	7x7	Daily action time	23:00
Start shift date	06/04/2021	Early arrival	
End employment		Late departure	

With the Cardholder assigned the above values, if the Cardholder has had the Site Access Competency manually assigned to them before their Start shift date, they can access the Regulated Zone with no alarms raised until they are set to start on 06/04/2021. After this date, the Site Access Competency is only enabled for them during their shifts and grace periods.

If the Cardholder accesses the Regulated Zone on 05/04/2021 (Start shift grace period), and they work from 06/04/2021 to the end of 12/04/2021 (seven days work), they need to leave the Regulated Zone before the end of 13/04/2021 (i.e. 00:00 on 14/04/2021) when their End shift grace period ends. At the end of their End shift grace period, their competency is disabled. If they do not leave the Regulated Zone before this time, an alarm is raised.

After a further six days have passed (their break, less the Start shift grace period), on 19/04/2021 at 00:00 (12:00 a.m.) their Site Access competency is re-enabled.

Scenario 2:

In this scenario, the Cardholder is changing from Shift pattern 1 (7x7) to Shift pattern 2 (5x2).

Shift pattern 1:

Start shift grace period	1 day	First allowed work day	
End shift grace period	1 day	Competency	Site Access
Shift pattern	7x7	Daily action time	23:00
Start shift date	06/04/2021	Early arrival	
End employment		Late departure	

Shift pattern 2:

Start shift grace period	1 day	First allowed work day	20/04/2021
End shift grace period	1 day	Competency	Site Access
Shift pattern	5x2	Daily action time	23:00
Start shift date	15/04/2021	Early arrival	
End employment		Late departure	

The Cardholder has worked one shift from their first Shift pattern, and is now, on 13/04/2021, changing their Shift pattern to 5x2. The new Shift pattern states the Cardholder requires two days break, so can start after having two days break after his past shift has ended (last day of past shift was 12/04/2021, break for two days, start on 15/04/20). He should, however, take a seven-day break because this is what was required of his last Shift pattern.

First allowed work day (20/04/2021) has been set, as required, after seven days break after his last shift ended on 12/04/2021. The Cardholder will not be able to access the Regulated Zone until 00:00 (12:00 a.m.) on 19/04/2021; the day before First allowed work day (due to Start shift grace period).