GALLAGHER Security

Command Centre v9.40

Feature Summary

security.gallagher.com



Contents

1 Introduction 3

2 Compatibility 4
- 2.1 Upgrading Command Centre 4
- 2.2 Easy upgrade from Controller 6000 to Controller 7000 6
- 2.3 Check reader compatibility for mobile wallets with the FT Support tool 6
- 2.4 Supported operating systems 6
- 2.5 Supported databases 7
- 2.6 Command Centre licensing 7
- 2.7 Command Centre Mobile app compatibility 7
- 2.8 Command Centre Mobile Connect app compatibility 8
- 2.9 Command Centre Web browser compatibility 8
- 2.10 FIDO2 compatibility 9

3 Command Centre Features and Enhancements 9
- 3.1 AccessNow – available early 2026 9
- 3.2 Bulk random selection 10
- 3.3 Manual Access Events 14
- 3.4 Half Cycle Lock Type 15
- 3.5 Jacques intercom monitoring 17
- 3.6 Automatic Workstation Routing 18
- 3.7 Workstation Disablement 19
- 3.8 Encoding Kiosk application 20
- 3.9 Non-English language support 21
- 3.10 Diagnostics install by default 23
- 3.11 Apple shareable keys 24
- 3.12 Entra ID single sign on 25

4 Perimeter Fence Controllers 26
- 4.1 F5/F6 Fence Controllers – available early 2026 26

5 Controller 7000 28
- 5.1 Lock cycle counting 28
- 5.2 Licensed support for up to 24 doors per Controller 7000 30
- 5.3 Platform health – Linux upgrades 33
- 5.4 Enhanced web server architecture for Controller 7000 33
- 5.5 Identify controller override 35
- 5.6 Dual ethernet – Phase 1 36
- 5.7 Increase HBUS readers from 20 to 48 37
- 5.8 Increase OSDP readers from 16 to 32 37
- 5.9 Increase inter-controller comms from 60 to 100 38

6 Minor Enhancements 40
- 6.1 Nedap ANPR Lumo and Nedap DESFire Boosters in Core 40
- 6.2 Mobile Credentials support with SALTO wired Readers 41
- 6.3 MorphoWave XP2 supported with Command Centre v9.40 41

1 Introduction

Welcome to the latest version of Gallagher Command Centre.
Sit back and take a moment to review the latest features and enhancements in this release.

Note: This document details the new features within Command Centre v9.40 and does not describe the entirety of Command Centre.

2 Compatibility

This section contains important notices that must be read when considering Command Centre v9.40.

2.1 Upgrading Command Centre

Changes made to Command Centre v9.40 may impact on the configuration of sites upgrading from earlier versions. Refer to the document '3E0068 Release Note Command Centre vEL9.40.XXXX (Upgrade Procedures).pdf' for further details.

Supported upgrade paths

- Command Centre v9.0 – Command Centre v9.40
- Command Centre v9.10 – Command Centre v9.40
- Command Centre v9.20 – Command Centre v9.40
- Command Centre v9.30 - Command Centre v9.40

CONTROLLER FIRMWARE COMPATIBILITY

Command Centre v9.40 supports the Controller 6000 and Controller 7000 firmware vCR9.30. Command Centre v9.40 is compatible with older versions of firmware for upgrade purposes only. No configuration changes should be made on the Controller 6000 and Controller 7000 running pre v9.40 versions once Command Centre has been upgraded. It is recommended to upgrade all controller firmware to the latest version as soon as possible.

GBUS OBSOLESCENCE - UPGRADE TO HBUS DEVICES



Important: From Command Centre v9.10, GBUS devices will no longer be supported. Customers will need to upgrade to HBUS devices to be able to continue upgrading past Command Centre v9.00.

In answer to the industry's need for an improved device communications protocol, Gallagher released HBUS in 2012 for improved speed, data protection, and automated scalability. These considerable enhancements are a key driver behind our decision to remove software support of GBUS, which was released over 20 years ago.

Supporting GBUS costs valuable development time with every release of Command Centre. Once removed, this time can be better used in delivering ongoing value to our customers.

IDEMIA LEGACY (MA2G) OBSOLESCENCE - UPGRADE TO NATIVE (MA5G) DEVICES



Important: From Command Centre v9.30, IDEMIA Legacy (MA2G) devices will no longer be supported. Customers will need to upgrade to Native (MA5G) devices to be able to continue upgrading past Command Centre v9.30.

Due to a new IDEMIA SDK, which does not support Legacy (MA2G) and is required for supporting the VisionPass SP in Command Centre v9.30, we have removed the support for Legacy (MA2G) communication protocol in Command Centre v9.30. IDEMIA stopped supporting the Legacy (MA2G) communication protocol since January 2022, and as such, we will no longer continue to support the MA2G communication protocol. Please see the Product Advisory for more information.

Please read the below pre-upgrade information before upgrading to v9.40

PRE-UPGRADE VALIDATION TOOL V9.40

Gallagher has developed the 'Pre-Upgrade Validation Tool'. This utility can be run on the Command Centre server to identify site compatibility issues prior to upgrading, including Controllers running customizations and/or custcard.dlls and legacy hardware. This utility can be found with the installation files (Utilities folder) or downloaded from the Gallagher Security File Transfers site in the 'Command Centre and Associated Files > Utilities' folder. This utility should be run prior to upgrade.

Link for Security File Transfers site - https://security.gallagher.com/downloads

If your site has customizations running on a Controller, these must be removed prior to upgrading the Controllers to v9.40. Once the Controller is upgraded to the new controller code, vCR9.20 (Linux OS) the newer version of the customizations will need to be re-installed.

All custcard DLLs prior to v8.20 are not compatible with Controller vCR8.20 or later. Once the Controller is upgraded to the new Controller version, updated DLLs may be required. Please contact Tech Support for assistance.

PRE-V7.10 CONTROLLERS

Pre-v7.10 Controllers are not supported from v8.50 or later of Command Centre.

The Windows TLS stack cannot communicate with pre-v7.10 Controllers due to the combination of SSLv3 and AES. Pre-7.10 Controllers will need to be upgraded to v7.10 or above before they are connected to v8.50 or later.

To eliminate the chance of a site upgrading to v9.10 and then finding their Controllers are not compatible, the installer will check for pre-v7.10 Controllers. If they exist, the installer will halt and inform the technician that upgrade of the Controllers is first required. The Gallagher Pre-Upgrade Validation Tool will also identify pre-v7.10 Controllers.

UPGRADING A CONTROLLER TO VCR9.40

Controllers running v8.20 or later (Linux) can be upgraded to v9.40 in less than two minutes. Controllers running v8.10.179 onwards (WinCE) can be migrated directly to v9.10 Linux, which could take up to four minutes. Controllers with software older than v8.10.179 will go through a two-step upgrade which could take up to seven minutes.

It is recommended that sites re-sync Controller databases when they are first migrated to Linux OS (v8.20 or later).

Refer to the document **3E2203 Release Note Command Centre vEL9.40.XXXX (Upgrade Procedures).pdf** for further details.

2.2 Easy upgrade from Controller 6000 to Controller 7000

We've made it easy to upgrade from Controller 6000 to Controller 7000 with our Upgrader Tool. The tool automatically configures a C7000 with your existing C6000 configuration, reducing your set-up time.

Upgrading to Command Centre v9.00+ unlocks the Controller 7000, which offers streamlined upgrades, advanced cyber protection, and will take you into the future with confidence.

2.3 Check reader compatibility for mobile wallets with the FT Support tool

Mobile wallets are only supported on Gallagher Multi Tech readers. Support for mobile wallets is based on technical capability of the reader, with a change to a chipset that supports ECP occurring around 2018 (date of manufacture), the 2018 date is provided as a guideline only.

From Command Centre v8.90 readers report their device attributes. The FT Support Tool can be used to report all readers that are wallet capable, their assigned door(s), and controller. The FT Support Tool is included with the Command Centre installation software in the Utilities\FT Support Tool directory.

2.4 Supported operating systems

Gallagher supports the below operating systems and follows Microsoft's lifecycle. Please refer to https://docs.microsoft.com/en-us/lifecycle/faq/windows

COMMAND CENTRE SERVER

- Windows 11 Pro/Enterprise
- Windows 10 Pro/Enterprise
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

COMMAND CENTRE WORKSTATION

- Windows 11 Pro/Enterprise
- Windows 10 Pro/Enterprise

Note: Command Centre is supported on a virtual server. However, due to virtual server environment configuration variability, if an initial fault resolution is inconclusive, Gallagher reserves the right to request customer replication of any errors in a non-virtual environment. Resources should be dedicated to the virtual environment. Command Centre installation is not supported on a Windows domain controller.

2.5 Supported databases

Important: Windows Server 2016, SQL Server 2016, and SQL Server 2017 are approaching the end of Extended Support under Microsoft's Fixed Lifecycle Policy. Microsoft will also cease support for Windows 10 Professional from 14th October 2025, under their Modern Lifecycle Policy.

What this means for you?

- Command Centre v9.40 will be the final version to support Windows Server 2016, SQL Server 2016, and SQL Server 2017.
- Command Centre v9.40 will also be the final version to support Windows 10 Professional and 32-bit operating systems.

2.6 Command Centre licensing

A valid license file is required to install or upgrade Command Centre.

Any new sites created after Full Release will have the latest version by default.

Sites upgrading to Command Centre v9.40 from a previous version (v9.30 or earlier) will require an updated Command Centre license file. To obtain an updated license file from Sales or Technical Support, the site must have an active Software Maintenance Agreement.

When Gallagher is requested by a Certified Channel Partner to update the key devices in a site license file, due to failure or removal of the key device from that site, the key device is required to be returned to the nearest Gallagher regional sales office within 30 days. Should the Channel Partner not be able to return the key device, Gallagher reserves the right to invoice the Channel Partner for the full cost of the site's Gallagher Command Centre software based on the price list in effect at the date of invoice.

2.7 Command Centre Mobile app compatibility

A valid license file is required to install or upgrade Command Centre.

Any new sites created after Full Release will have the latest version by default.

Sites upgrading to Command Centre v9.40 from a previous version (v9.10 or earlier) will require an updated Command Centre license file. To obtain an

Device	Operating System
iPhone 8 or later	iOS 15 or later
Android	7.0 or later

2.8 Command Centre Mobile Connect app compatibility

Device	Operating System
iPhone 8 or later	iOS 15 or later
Android	7.0 or later

2.9 Command Centre Web browser compatibility

- Google Chrome version 122+
- Microsoft Edge version 122+

- Safari 17+

2.10 FIDO2 compatibility

FIDO2 logon requires Windows 10 version 1903 or later.

3 Command Centre Features and Enhancements

3.1 AccessNow – available early 2026

Business value: AccessNow makes getting access simple. Users request what they need, the right people approve it, and access is granted automatically, all in minutes, not days.

DESCRIPTION

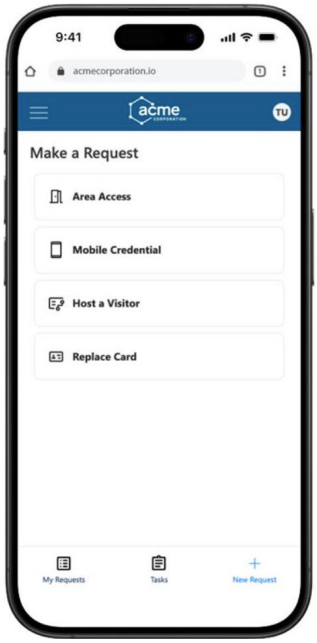
AccessNow is Gallagher's new cloud-native platform that automates the entire access and credential request process. It enables users to request access from any device, instantly routes requests to the right approvers, and provisions access automatically in Command Centre once approved.

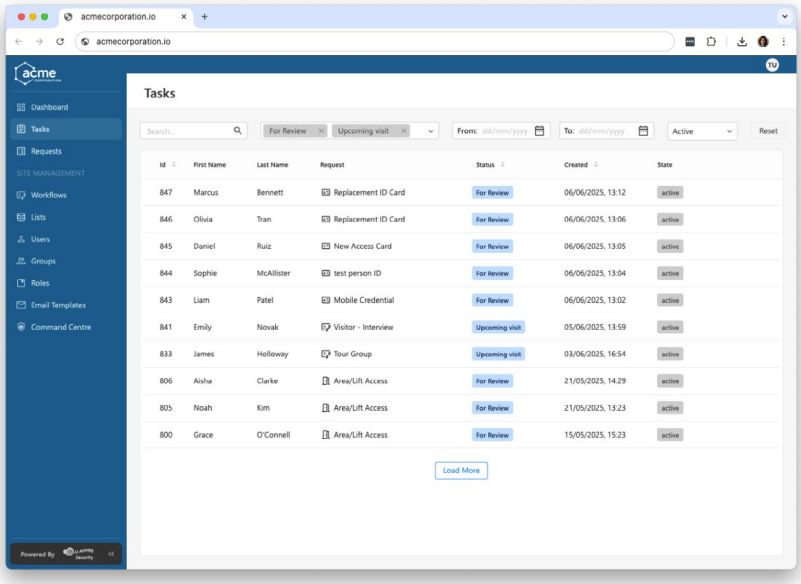
With its intuitive, no-code workflow builder, security teams can easily design and customise automation for every type of request they receive.

BENEFITS

AccessNow makes getting access simple. Users request what they need, the right people approve it, and access is granted automatically, all in minutes, not days.

Security teams no longer waste time on repetitive admin, approvals are accurate and traceable, and everyone enjoys a faster, smoother experience.





ACCESSNOW ANNUAL SUBSCRIPTION OVERVIEW

AccessNow is provided as an annual subscription service with a two-part pricing structure:

- **Workflow Licensing (each)** Charges apply for each automated use case (also referred to as a workflow), such as employee credential issuance, or access request and provisioning etc.
  - C16110 – ACCESSNOW WORKFLOW (EACH) – Includes a Workflow, 1000 Requests, and one-off integration with the Command Centre.
  - [Feature] AccessNow Command Centre Integration = 1
- **Request Packs** Charges also apply based on the volume of requests processed through AccessNow Available packs include:
  - C16111 – ACCESSNOW SMALL REQUEST PACK (1000) – Pack of 1,000 requests.
  - C16112 – ACCESSNOW LARGE REQUEST PACK (30000) – Pack of 30,000 requests.

ACCESSNOW REQUIREMENTS AND CONSTRAINTS

To learn about the requirements and constraints of the service visit: https://help.security.gallagher.com/enterprise/help-resources/accessnow-requirements-and-constraints

ACCESSNOW ACCOUNT SETUP INSTRUCTIONS

AccessNow is a SaaS platform that requires an account to be created before use. This account is then linked to Command Centre via an API key. To request a new account, please follow these steps:

- **Contact your Gallagher Business Development Manager** to initiate the request.
- **Submit a Purchase Order (PO)** for the service.

Complete the onboarding form available at: https://forms.office.com/r/ujj7pTCMtS

Once these steps are completed, your account will be provisioned and integrated accordingly.

3.2 Bulk random selection

Business value: Ensure site compliance by randomly selecting Cardholders without bias for random Drug and Alcohol testing.

DESCRIPTION

Bulk Random Selection enhances Gallagher's existing controller-based random selection solution, adding support for ad-hoc, scheduled, and event driven server-based random selection of filtered cardholders.

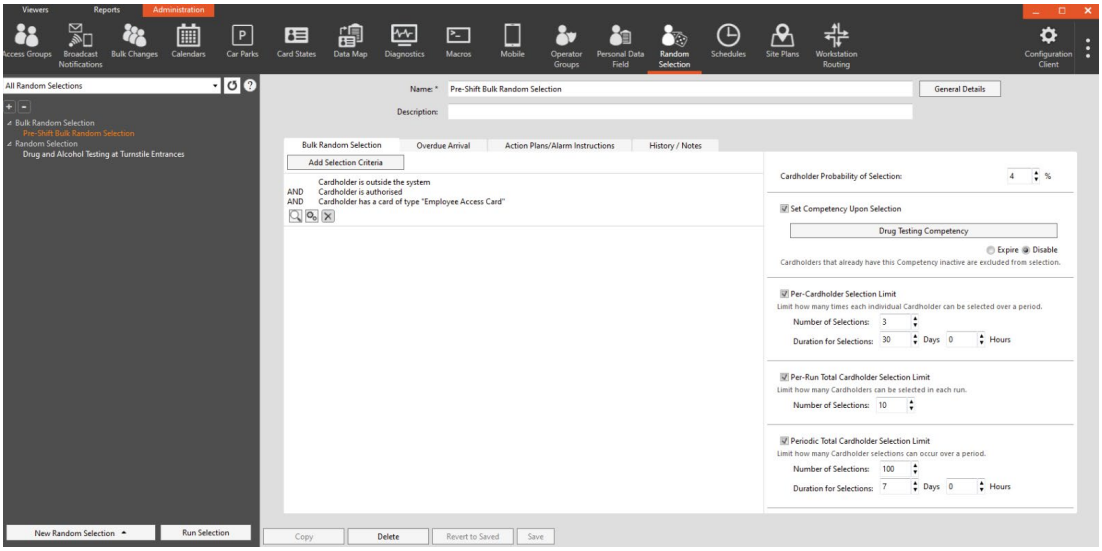
BENEFITS

Cardholders can be randomly selected pre-shift or mid-shift ensuring sites comply with Health and Safety regulations. Gallagher's rich cardholder filtering and randomised selection algorithm can select Cardholders without bias, for Drug and Alcohol testing independent from selection at a reader.

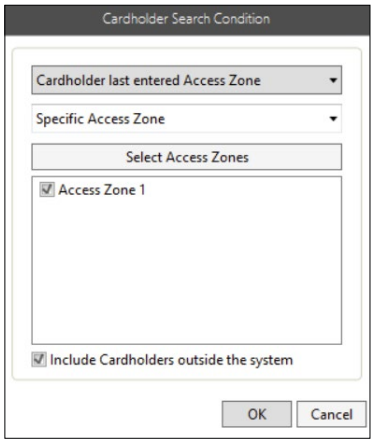
DETAILS

Random Selection was introduced in Command Centre v8.30 as a controller-based feature to randomly select Cardholders as they accessed a site area at a Gallagher reader.

Bulk Random Selection complements the original Random Selection feature by independently selecting Cardholders from a pool of filtered Cardholders. The rich filtering (also available in Cardholder Bulk Change, Reporting, and Cardholder Viewer Advanced Search) can select Cardholders by Division, Access Group, Location, Competency Status, Personal Data Field, and many other attributes.



The Cardholder last entered Access Zone filter has been modified to optionally (or exclusively) include Cardholders who are Outside the System. This filter allows selection of Cardholders based on their current location. Sites can therefore randomly select Cardholders before, during, or after attendance at the workplace.



OPERATION

A privileged operator can run a Bulk Random Selection from:

- The Random Selection admin viewer
- A Status tile
- A Site Plan viewer
- A Site Plan tile
- A Macro

PRIVILEGES

- An operator requires Run Bulk Random Selection in the division of the Bulk Random Selection item, to run a bulk random selection, and if required change the probability of selection, and the maximum Cardholders selected.
- An operator requires Edit Random Selection (existing privilege) in the division of the Bulk Random Selection item to create, edit or delete a Bulk Random Selection item.
- An operator requires View Random Selection (existing privilege) in the division of the Bulk Random Selection item to view a Bulk Random Selection item.
- An operator requires Edit Macros and Run Bulk Random Selection in the division of the Bulk Random Selection item to create, edit or delete a macro used to run a Bulk Random Selection.

REPORTING

The Cardholder report includes Random Selection columns that now support both controller-based Random Selection and Bulk Random Selection:

- Random Selection Name
- Last Selected Time
- Last Selected Event Summary
- Last Selected Time (Random Selection Name)

Note: It is highly recommended that reports using these Random Selection columns are not combined with event columns or event filters.

Two filters also support both types of random selection:

- Cardholder Random Selection
- Cardholder Last Random Selection Time

This allows two reports to be configured.

The first report example shows data in 'per selection' format where data on the same row is related to the selection event. This report can be grouped.

Last Selected Event Summary Bulk Random Selection

Cardholder Name	Random Selection Name	Last Selected Time	Last Selected Event Summary
Anderson, Alan	Drug Testing	25/08/2025 9:11:08 am	Cardholder "Alan Anderson" was selected by Bulk Random Selection "Drug Testing"
Batty, Barbara	Drug Testing	25/08/2025 9:11:08 am	Cardholder "Barbara Batty" was selected by Bulk Random Selection "Drug Testing"
Blake, Barney			
Caskey, Colin	Health Check Testing	25/08/2025 9:05:52 am	Cardholder "Colin Caskey" was selected by Bulk Random Selection "Night Shift"
Dixon, Donald	Drug Testing	25/08/2025 9:11:08 am	Cardholder "Donald Dixon" was selected by Bulk Random Selection "Drug Testing"
Dixon, Donald	Health Check Testing	25/08/2025 9:05:52 am	Cardholder "Donald Dixon" was selected by Bulk Random Selection "Night Shift"

The second report example shows data in a flat structure where each row contains multiple random selection items. It is not recommended to group this report. A requirement exists to add Access Group or Card Type columns when filtering by these items.

Last Selected Time Bulk Random Selection

Cardholder Name	Access Group	Last Selected Time (Drug Testing)	Last Selected Time (Health Check Testing)
Anderson, Alan	Day Shift	25/08/2025 9:11:08 am	
Batty, Barbara	Day Shift	25/08/2025 9:11:08 am	
Blake, Barney	Day Shift		
Caskey, Colin	Night Shift		25/08/2025 9:05:52 am
Dixon, Donald	Night Shift	25/08/2025 9:11:08 am	25/08/2025 9:05:52 am

LICENSING

Bulk Random Selection is included in the existing controller-based Random Selection license.

3.3 Manual Access Events

Business value: EImprove Tagboard and Evacuation Report location, and correct fatigue management calculations.

DESCRIPTION

Privileged operators can now initiate historical movement events from a Cardholder Viewer.

BENEFITS

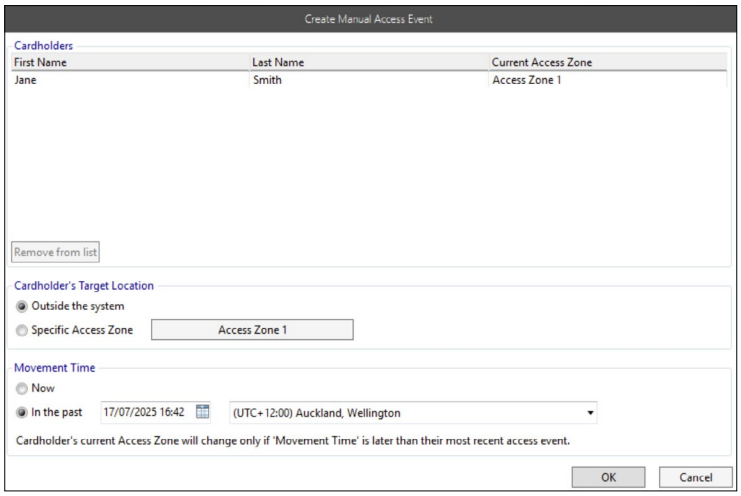
When cardholders tailgate entering or exiting a site, manually creating historical movement events can help:

- Improve Tagboard and Evacuation Report location (when the event is the most recent movement).
- Correct fatigue management calculations to enforce required rest-from-work policies.

DETAILS

In the Cardholder Viewer, the previously named Action menu item 'Move to Location' has been renamed 'Create Manual Access Event'.

This control now supports moving Cardholders at the time of the action (Now), or historically (In the past). Historical movement actions will only update the Cardholder location if the event is the most recent movement event.



EVENTS

Two new events capture historical movement events and complement the two existing events:

- Operator moved Cardholder
- Operator moved Cardholder to outside of the system
- Operator moved Cardholder historically
- Operator moved Cardholder to outside of the system historically

PRIVILEGES

An operator requires Manage Historical Cardholder Location privilege in the division of the Cardholder and the target Access Zone (or any Access Zone when moving to Outside the system), to move a Cardholder historically.

LICENSING

Manually moving cardholders currently or historically does not require explicit licensing.

3.4 Half Cycle Lock Type

Business value: Reduce the risk of unauthorized access and accidental or unauthorized unlocking to increase control over secure areas.

DESCRIPTION

The Half-Cycle Lock is a security mechanism commonly used in correctional facilities.

When a Cardholder is granted access at a Half-Cycle door, the unlocking process is initiated. The lock completes a half-cycle, meaning the bolt is retracted, but the lock is not fully disengaged. The door must be opened by its handle, often with a key, to fully unlock.

When doors with the Half-Cycle Lock Type are unlocked (with a valid credential or override), they remain unlocked until the door is opened and then closed, or overridden to locked, upon which the door locks.

BENEFITS

The Half-Cycle Lock reduces risk of unauthorized access. The mechanism prevents accidental or unauthorized unlocking, increasing control over secure areas.

The lock mechanism streamlines the unlocking and locking processes saving time and increasing efficiency at correctional facilities.

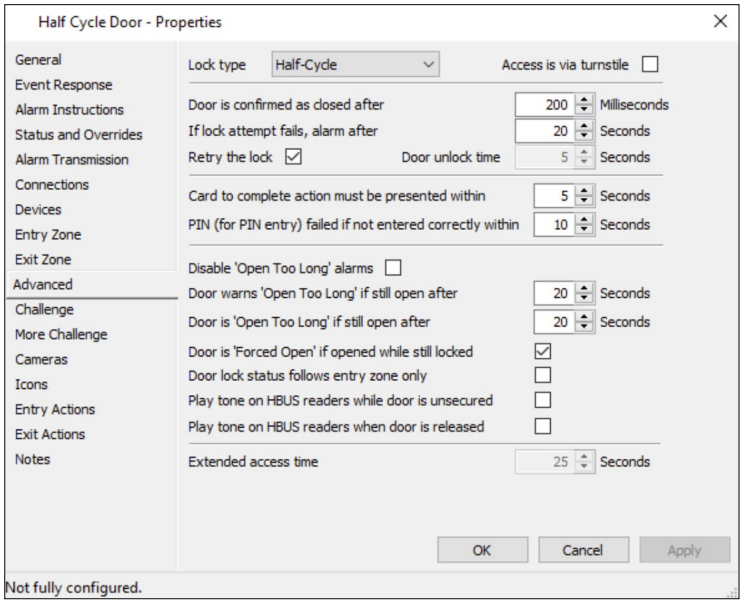
Half-Cycle locks help facilities meet regulatory requirements and industry standards.

DETAILS

Configuration

For doors configured with Half-Cycle lock type:

- Door Open Too Long warnings and alarms can optionally be disabled.
- Door unlock time and Extended access time settings are disabled and not applicable.
- Reader LEDs flash green on access granted but then revert to solid green` when doors are unlocked but remain closed. Note: T2x terminals will only exhibit this behaviour if configured as Cardax IV readers.



Overrides and Privileges

A new 'Lock Door' override and 'Override - Lock door' privilege have been introduced. An operator with this privilege in the Door's division can override a Half-Cycle lock type Door to locked. A Half-Cycle door will remain unlocked after access is granted until either it is opened and shut, or the Lock Door override is used.

The existing 'Open Door' override and 'Override - Open door' privilege can be used to override a Half-Cycle lock type Door to unlocked.

Licensing

Half-Cycle Lock Type is available with a standard Door license.

3.5 Jacques intercom monitoring

Business value: Discreetly monitor conversations and enhance surveillance in sensitive areas.

DESCRIPTION

Gallagher's Jacques Intercom integration now supports Intercom Monitoring allowing an operator to put an intercom into a listen-only state.

Intercoms can also be isolated from a Status tile and Site Plan tile (but not a Site Plan Viewer). Incoming intercom calls are blocked when an intercom is isolated.

BENEFITS

Operators can discreetly monitor conversations or other sounds from targeted areas.

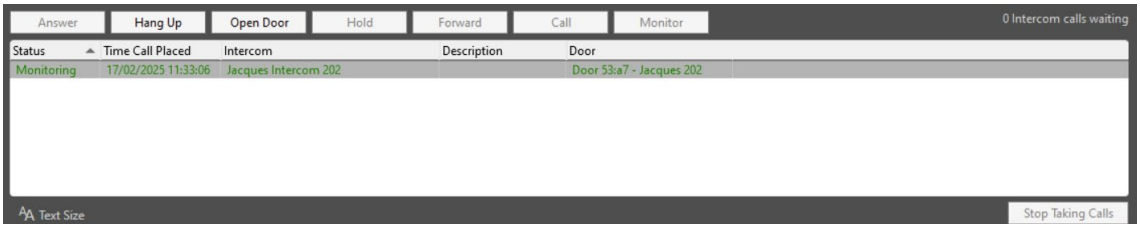
This feature enhances surveillance capabilities in sensitive areas.

DETAILS

An operator can initiate a monitoring call from a:

- Jacques Intercom Viewer
- Status tile
- Site Plan tile or Site Plan viewer

Monitor-only calls cannot be placed on hold, nor forwarded to other workstations/operators.



PRIVILEGES

An operator requires the 'Monitor Intercom' and 'View Site' privileges in the division of the intercom device to use this functionality.

LICENSING

Jacques intercom monitoring is included in the existing Jacques license.

3.6 Automatic Workstation Routing

Business value: Improve location handover procedures and minimize delays and errors.

DESCRIPTION

Workstation Routing was introduced in v7.30 allowing system handover between control rooms where responsibility for certain functions transfers between locations regularly.

Command Centre v9.40 introduces automation to the routing behaviour. When operators login to remote workstations, routing automatically transfers functions to the remote operators. When all operators are logged out of the remote locations, routing automatically returns function to the central/ local control room.

BENEFITS

Workstation Routing is used predominantly in the Corrections market, to transfer responsibility to and from remote control rooms at various times of day. Automation of routing ensures that responsibility coincides with operator presence improving location handover procedures and minimising delays and errors. Operators are assured of responsibility at time of login and logout.

DETAILS

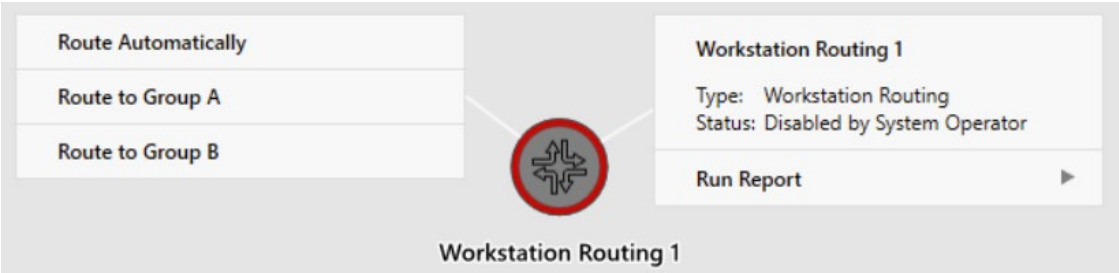
Previously, routing direction was interchangeable i.e., Group A and Group B were directionless.

With Automatic Workstation Routing the 'central' workstations are represented as Group A and the 'remote' workstations as Group B. The feature introduces a new 'Route Automatically' option actionable from:

- The Workstation Routing Viewer
- Site Plans (Tile and Viewer)
- Status Tile

When routing is configured automatically:

- When all Group B workstations are logged off Command Centre, routing to Group A (central) occurs automatically
- When at least one Group B workstation is logged onto Command Centre, routing to Group B (remote) occurs automatically.



Workstation Routing items can be configured to display the highest priority alarm from any configured division. While a Workstation Routing item is automatically routed to Group B, it displays on Site Plans the current highest priority alarm of all items in the Divisions assigned to its 'Alarm Alert Divisions' tab. The same applies to shapes with the Workstation Routing item as an Associated Item.

PRIVILEGES

An operator requires the 'Monitor Intercom' and 'View Site' privileges in the division of the intercom device to use this functionality.

Privileges	Description (and previous name)
Configure Workstation Routing	Configure Workstation Routing items (no change).
Manage Workstation Routing	Perform all Overrides on Workstation Routing items, including Disable Workstation Routing and Route Automatically (previously named Disable Workstation Routing).
Use Manual Workstation Routing	Perform Route to Group A and Route to Group B Overrides on Workstation Routing items (previously named Use Workstation Routing).

LICENSING

Automatic Workstation Routing is included in the existing Workstation Routing license.

3.7 Workstation Disablement

Business value: Disable and re-enable access to Command Centre or end active sessions when maintenance or security situations arise.

DESCRIPTION

Workstations can now be disabled and re-enabled by privileged operators to prevent access to Command Centre or to end active sessions.

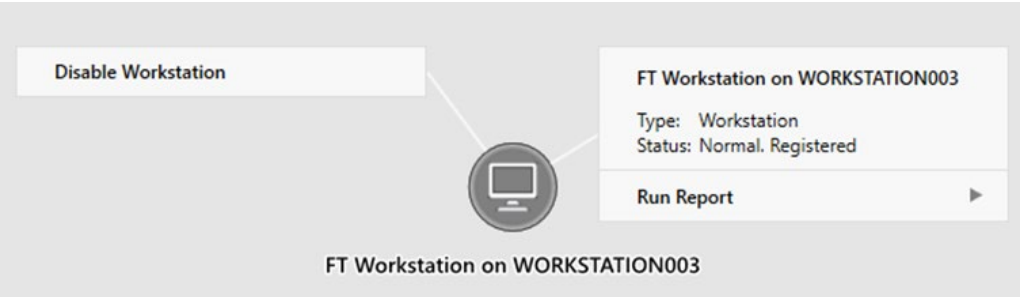
BENEFITS

Command Centre access can be prevented at remote control room locations when maintenance or security situations arise. Active workstation sessions can also be immediately terminated returning security control to privileged central operators.

DETAILS

Workstation access can be disabled and re-enabled in Command Centre from:

- The Status and Overrides property page of each workstation item
- Status Tiles
- Site Plan Viewers and Tiles
- Macros
- Operator Sessions window/tile (Disable only)



PRIVILEGES

The following privileges are required in the division of the workstation to disable and re-enable workstation access:

- Disable Workstation
- Enable Workstation

3.8 Encoding Kiosk Application

Business value: Read Gallagher or third-party (non-Gallagher) card data from MIFARE Classic and DESFire cards and encodes the equivalent data so that cards can be used at both third-party readers and Gallagher T-series readers.

DESCRIPTION

The Kiosk supports:

- reading Gallagher data and writing that data back to other Gallagher sectors/applications.
- reading Gallagher data and writing that data back to other sectors/applications with a configurable third-party card format (non-diversified).
- reading third-party data and writing that data back to other Gallagher sectors/applications.
- reading third-party data and writing that data back to other sectors/applications with a configurable third-party card format (non-diversified).

BENEFITS

This Kiosk Application can provision cards with a second Gallagher application to allow base building and tenant systems to be accessed with a single card.

The Kiosk can provision cards with a non-diversified application for use by non-Gallagher readers (e.g., elevators or key cabinets), eliminating the security risk of sharing keys.

During a reader changeover, cardholders can continue to use a single card at multiple readers.

DETAILS

The Encoding Kiosk Application has been designed to be used at a self-service "kiosk", with the intention that Cardholders will use it without assistance. The utility displays full-screen and does not require end users to physically interact with anything other than the USB card encoder.

Configuration of all keys with which your existing card sectors and applications have been encoded, as well as the keys to be used to encode new sectors and applications, is required. It is also possible to customize elements of the visible Application, including a logo, the background and text colours, and the error message displayed.



CONFIGURATION

For details of implementation recommendations and use of the configuration utility please review the C12950 Encoding Kiosk Application release note.

LICENSING

The following licenses are required to use the Encoding Kiosk Application:

[Features]

EncodingKioskApp=1

Encoding=1

[Configuration]

EncodingKioskFCs=<Xnnnnn>,<Ynnnnn>

Where Xnnnnn and Ynnnnn represent the facility codes able to be used by the Encoding Kiosk app.



This feature requires use of the Gallagher USB MIFARE encoder (C41007).



Important: The Encoding Application does not support the Gallagher MIFARE DESFire default key seed.

3.9 Non-English Language Support

Business value: Enable operators to use Command Centre in a language more familiar to them, and support compliance and regulatory requirements in certain regions where non-English support is mandatory.

DESCRIPTION

We have historically offered a variety of language packs which would be installed alongside Command Centre, providing non-English language support for the four desktop clients (Configuration Client, Command Centre Client, Visitor Management Client and Visitor Management Kiosk).

This feature introduces in-built language support to the core Command Centre product without the need to install language packs after the fact. All languages are provided at no additional cost and no longer require the relevant 'Languages' licence string.

BENEFITS

This capability will allow operators to use our software in a language that may be more familiar to them. It will also help with meeting compliance and regulatory requirements in certain regions where non-English language support is mandatory.

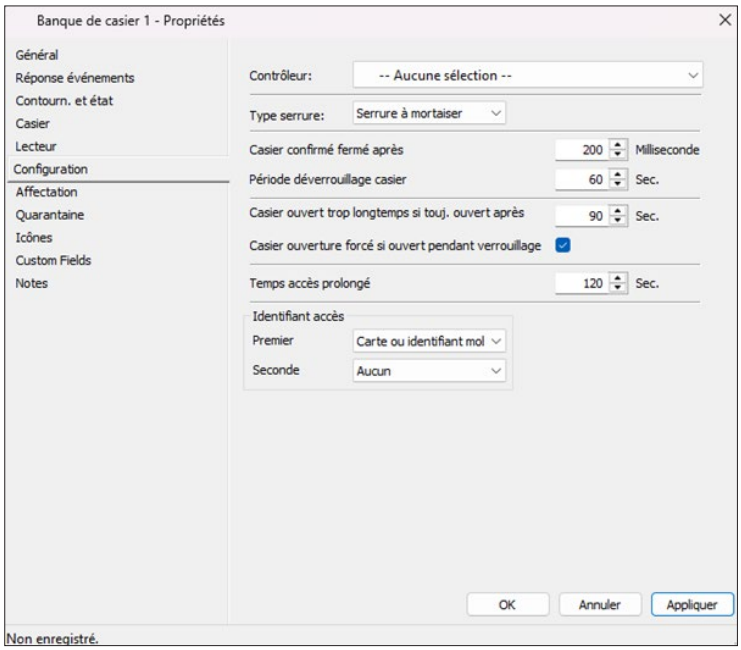
DETAILS

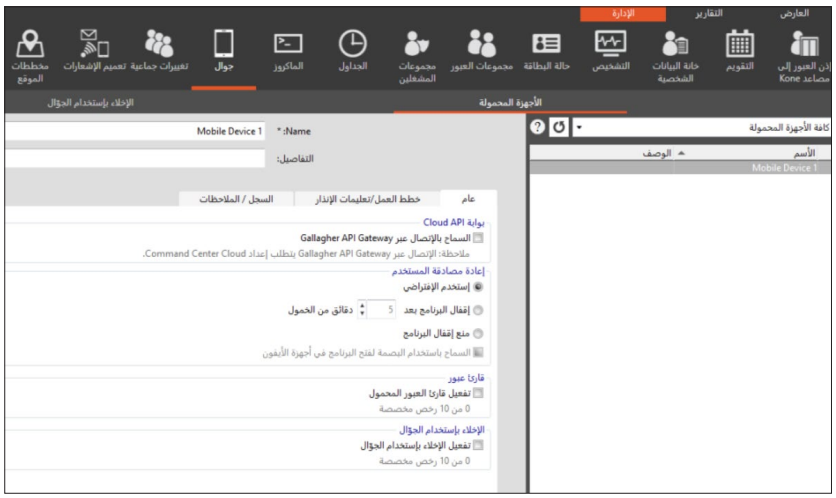
The supported languages are:

- Arabic
- Brazilian Portuguese
- Canadian French
- Chilean Spanish
- Dutch
- Simplified Chinese
- Swedish
- Traditional Chinese

The 'Languages' licence string is now obsolete and will not be used for anything going forward

New CEIP counters have been added to allow product uptake analysis of how many operators are using each language.





3.10 Diagnostics install by default

Business value: Collect diagnostic information without having to manually enable it.

DESCRIPTION

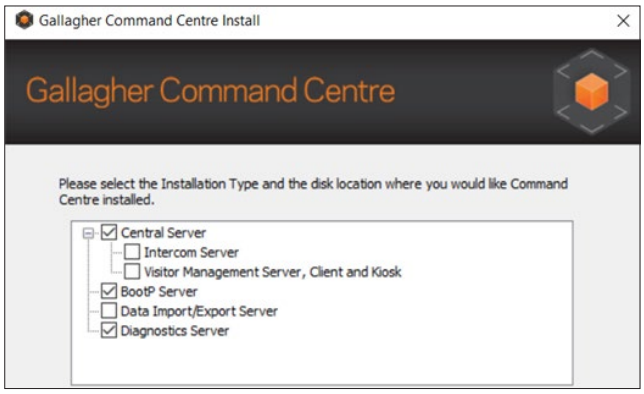
Command Centre 9.40 changes the way that the Diagnostics Service is installed from being opt-in to install and register, to being a core subproduct installed and registered as part of Command Centre.

BUSINESS VALUE

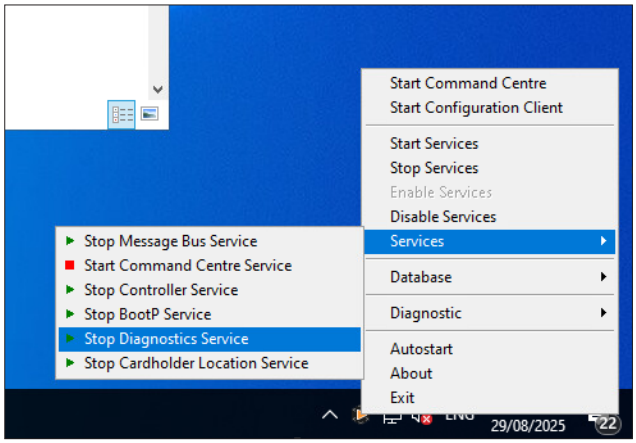
This feature will allow the diagnostics information to be collected without having to wait for the sites to enable it allowing the collection of improved trace data and workstation log aggregation.

DETAILS

Diagnostics server is included in the Installation Type and ticked by default.



Post installation Diagnostics Service is listed on the CCFT Service Manager utility



Diagnostics service will be automatically installed when Command Centre is installed unless the customer explicitly disables it

3.11 Apple Shareable Keys

Business value: Streamline access across your site and enable access via third-party readers.

DESCRIPTION

This feature enables the retrieval of an Apple Read Key from Command Centre. The key can then be programmed at a supported third-party reader, allowing Apple credentials to be read at the reader.

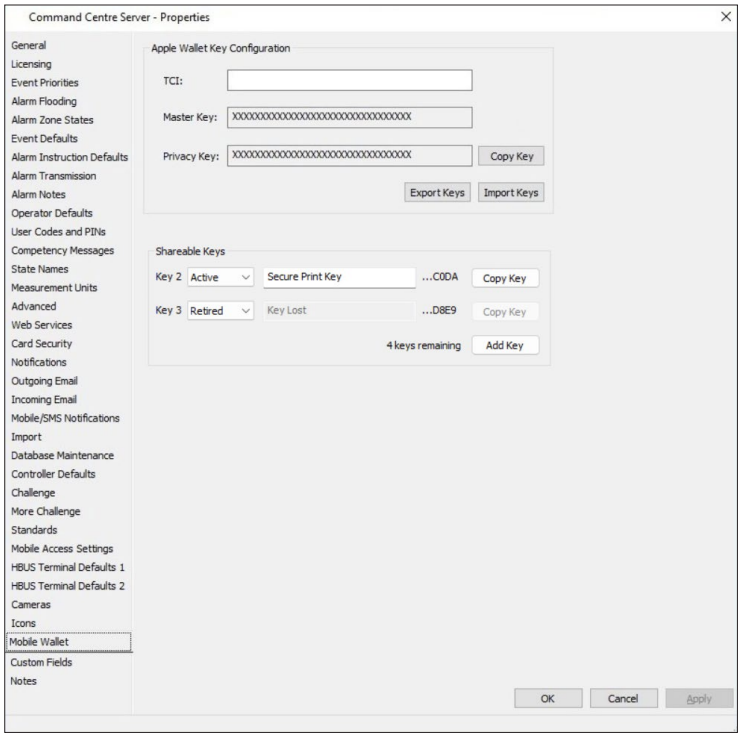
BENEFITS

Using Apple credentials, an employee can authenticate at all readers onsite.

DETAILS

An operator with the "Manage Keys" privilege can retrieve an Apple Read Key from Command Centre. Six Apple Read Keys can be retrieved. Operator events for key retrieval are supported. Key states "Active" and "Retired" allow an operator to track key usage. Each key shared must be labelled, (e.g. secure print key).

To program a supported third-party reader, enter the Apple TCI, Privacy Key, Read Key and Key Number into the reader configuration utility.



- Marking a key as "Retired" does not revoke the key. This state is to inform the operator not to share the key.
- Employee Badge in Apple Wallet is a licensed feature of Command Centre.

3.12 Entra ID single sign on

Business value: Enable secure and seamless authentication with Entra ID Single Sign On.

DESCRIPTION

Command Centre Client now supports integration with Microsoft Entra ID (formerly Azure AD) for single sign-on (SSO), enabling secure and seamless authentication using OpenID Connect.

BENEFITS

This integration allows customers to align with their organisation's cloud-first identity strategy, reduce reliance on legacy AD infrastructure, and benefit from centralised access control, multi-factor authentication, and conditional access policies — all managed through Microsoft Entra. It simplifies user management, enhances security, and supports smoother migration to modern identity platforms.

DETAILS

Gallagher Command Centre Client now supports Single Sign-On (SSO) using Microsoft Entra ID, enabling secure, centralised authentication for operators. This integration leverages modern identity protocols—OAuth 2.0 and OpenID Connect—via the Microsoft Authentication Library (MSAL), ensuring secure token exchange and seamless user experience.

From initial setup to migration, it's easy for IT teams to get started:

1. **Configure your Entra ID tenancy settings**

Quickly set up your Command Centre application in the Microsoft Entra Admin Portal with a few straightforward steps.

2. **Set up Entra ID SSO in Command Centre**

Enjoy full flexibility with global and individual cardholder-level controls—ideal for managing test groups and rolling out SSO in phases.

3. **Migrate from Active Directory SSO to Entra ID SSO**

For customers currently using Active Directory SSO, Command Centre supports running both systems in parallel, ensuring a smooth and disruption-free transition.

4. **Log in with Entra ID**

Once configured, users can select Microsoft Entra ID at login and authenticate successfully. From then on, access is seamless—Command Centre Client will automatically log them in using SSO, making day-to-day use simple and secure.

LICENSING

C12942 - LIC ENTRA ID SSO may be licenced in two ways:

- Included in the Entra ID Sync licence (no additional charge for Entra ID SSO).
- Individually licenced as follows:
  - [Features] EntraIDSingleSignOn=1

4 Perimeter Fence Controllers

4.1 F5/F6 Fence Controllers – available early 2026

Business value: Ensure network reliability with dual-port redundancy and increased bandwidth for uninterrupted system performance.

DESCRIPTION

The F5/F6 Fence Controllers utilize safety software to provide a product that complies with the latest energizer safety standards (IEC60335-2-76). While the F5/F6 models function similarly to their predecessors, there are key updates related to synchronisation and permitted installation scenarios.

KEY UPDATE: SMART SYNC

To meet the latest international safety standards (IEC 60335-2-76), Gallagher's F5 and F6 Fence Controllers now feature bi-directional synchronisation intelligence.

If synchronisation between energizers is lost, the system will automatically reduce its output energy to a safe level of 1.2 Joules per channel or less (no more than 2.5 Joules). Once synchronisation is restored, the controller resumes normal operation without any manual intervention. This safety response is fully automated and managed by the controller's onboard safety software. Any sync-related events are reported in Gallagher Command Centre, allowing customers to monitor and respond efficiently.

KEY UPDATE: PERMITTED INSTALLATION SCENARIOS

To maintain compliance, all installations must follow one of the approved configurations. These guidelines help ensure that every system is installed safely and performs as expected—whether it's a new site, an upgrade, or an extension.

SITES WITH F3 OR F4 FENCE CONTROLLERS

Gallagher has released an update to the synchronisation protocol that enables F3 and F4 Fence Controllers to synchronise with F5 and F6 series controllers using Smart Sync. This enhancement allows sites currently operating F3 or F4 controllers to function in the same manner as new installations, ensuring consistent and unified system performance across all controller generations.

Extensions to sites where an F3 or F4 Fence Controller is installed are allowed under the following conditions:

1. **Primary Synchronization Source:**

The F5 or F6 Fence Controller must act as the primary synchronization source.

2. **Firmware Update Requirement:**

The firmware of the F3/F4 Fence Controllers must be updated to support enhanced synchronization before activating the F5/F6.

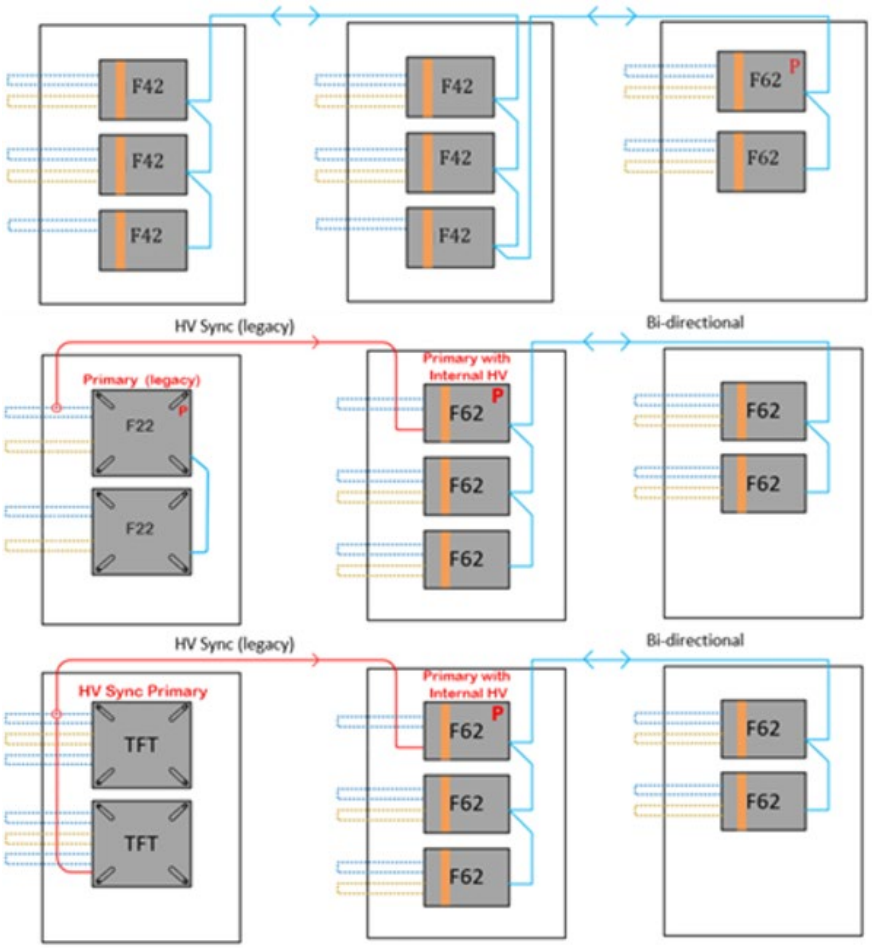
STAND-ALONE SITES:

If the site extension operates as a stand-alone system, the firmware update for the existing Fence Controllers must be performed via a temporary connection to Command Centre using a Controller 7000.

SITES WITH TROPHY FT & F22 FENCE CONTROLLERS

Trophy FT and F22 Fence Controllers are obsolete and cannot be updated to support the synchronisation protocol used by F5 and F6 Fence Controllers. For sites using Trophy FT or F22 that require expansion, it is strongly recommended to upgrade all fence controllers and the Command Centre to the latest generation (F5/F6). This approach is referred to as a Staggered Upgrade.

To ensure maximum safety during a staggered upgrade, fence zones powered by Trophy FT or F22 that border F5/F6 zones must operate at reduced power. This allows F5/F6 controllers to enforce safe limits, enhancing site safety in accordance with the latest IEC standards.



5 Controller 7000

5.1 Lock cycle counting

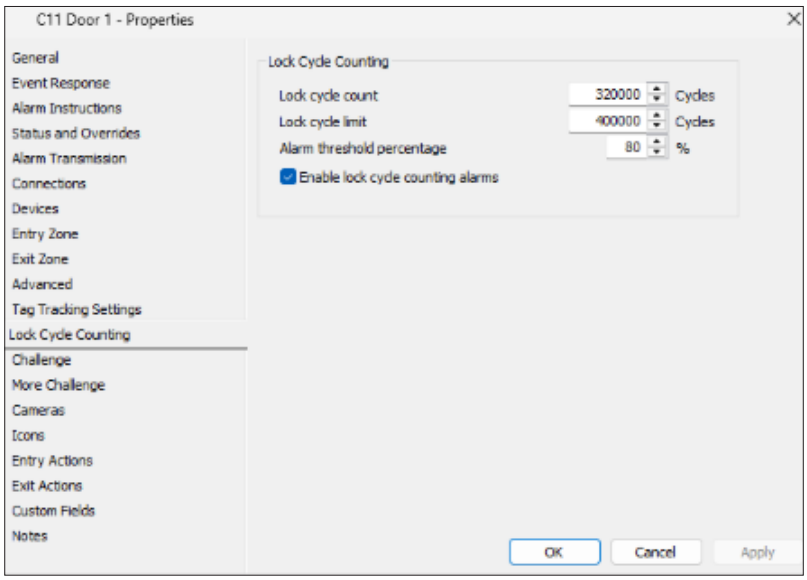
Business value: Prevent failures, reduce downtime, and plan replacements more effectively.

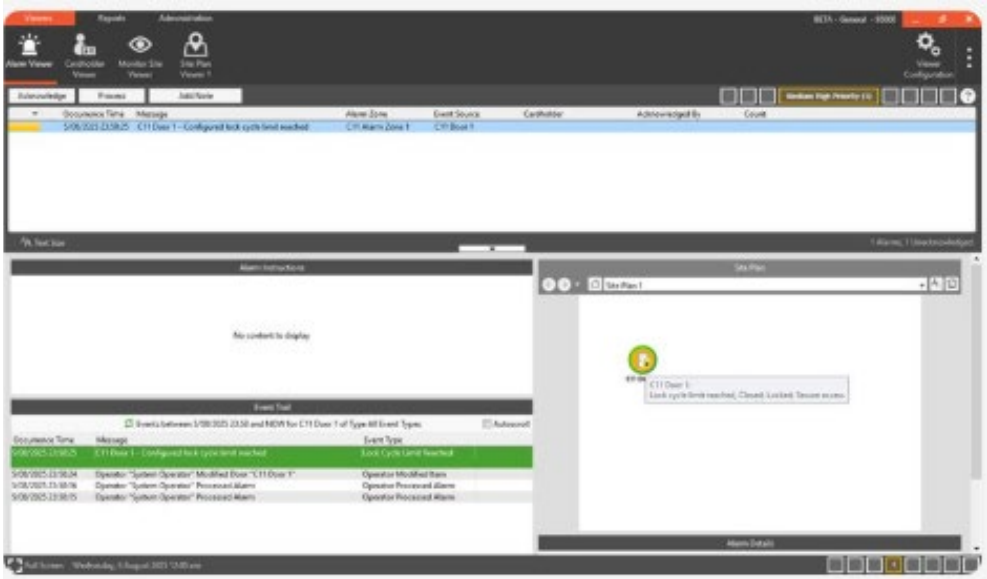
DESCRIPTION

This feature introduces proactive maintenance capabilities by tracking the number of lock/unlock cycles per door. It enables Channel Partners and site owners to monitor lock usage and receive alarms when locks approach their rated cycle limits, helping prevent failures, reduce downtime, and plan replacements more effectively.

PRODUCT AVAILABILITY

- **Preventative Maintenance:** Alerts when locks approach their cycle limits (default threshold: 80% configurable).
- **Data Persistence:** Cycle counts are stored both in the controller and Command Centre, surviving restarts and offline periods.
- **Customizable Thresholds:** Users can set the cycle limit and alarm percentage (e.g. 400,000 cycles with an 80% threshold).
- **Flexible Notifications:** Alarms can trigger emails or SMS alerts to site owners or Channel Partners.
- Controller-side persistence ensures counts are retained across reboots unless dipswitch 2 is activated.





DETAILS

- Command Centre v9.40 adds a new Lock Cycle Counting tab to the Door FTItem configuration page. This tab allows users to:
- Enable or disable lock cycle alarms.
- View and configure the lock cycle count, limit and alarm threshold.
- Receive notifications when a lock reaches a defined percentage of its cycle limit.
- The feature is off by default but continues counting in the background, allowing users to activate it later without losing historical data.

Key Benefits

- Preventive Maintenance: Alerts when locks approach their cycle limits (default threshold: 80%, configurable).
- Data Persistence: Cycle counts are stored both in the controller and Command Centre, surviving restarts and offline periods.
- Customizable Thresholds: Users can set the cycle limit and alarm percentage (e.g., 400,000 cycles with an 80% threshold).
- Flexible Notifications: Alarms can trigger emails or SMS alerts to site owners or Channel Partners.
- Controller-side persistence ensures counts are retained across reboots unless dipswitch 2 is activated UI Integration.
- Located between “Tag Tracking Settings” and “Challenge” in the Door FTItem.

Includes:

- Lock cycle count (read-only)
- Lock cycle limit (editable)
- Alarm threshold percentage (editable)
- Enable alarms checkbox (unticked by default)

Example Use Case

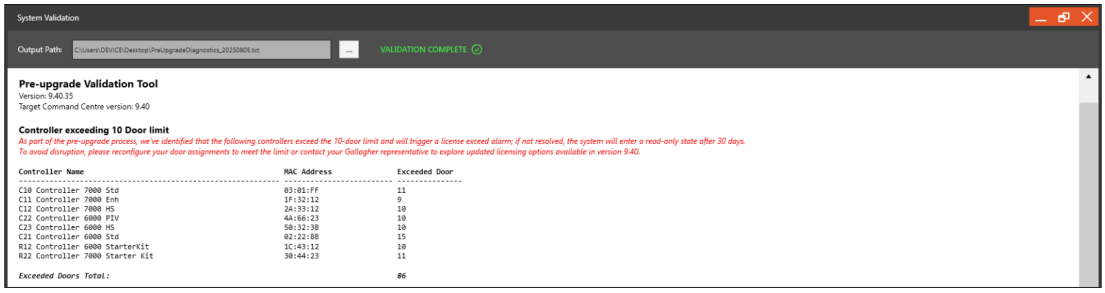
A Channel Partner receives an alert that a mortice lock has reached 90% of its rated 750,000 cycles. They proactively schedule a replacement, avoiding a failure during peak hours and strengthening customer trust.

5.2 Licensed support for up to 24 doors per Controller 7000

Business value: support larger installations, reduce infrastructure costs, and simplify system architecture.

DESCRIPTION

With Command Centre v9.40, variants of the Controller 7000 (Standard, Enhanced, High Security) can now support up to 24 doors. Sites will need to purchase an 'Extended Controller Door' license per additional door connected to a controller. Without these licenses, controllers will be hard limited to 10 doors and trigger alarms if exceeded upon upgrade.



BENEFITS

This enhancement expands Gallagher's controller capacity by allowing each Controller 7000 to support up to 24 doors, increased from the previous limit of 10. It enables larger installations, reduces infrastructure costs and simplifies system architecture - especially for high-density access control environments.

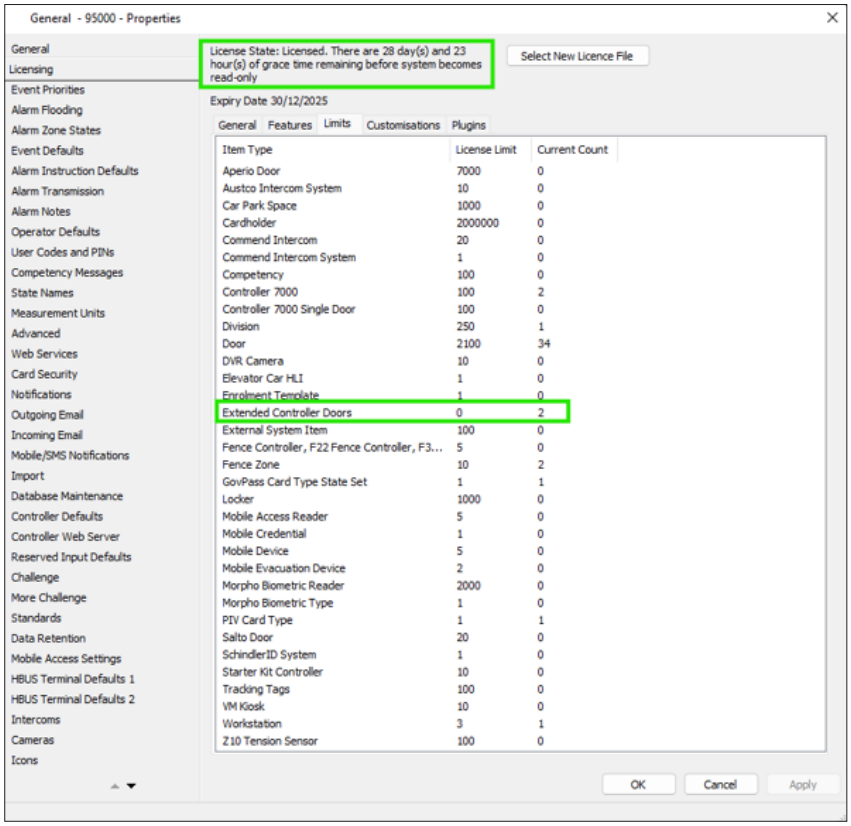
DETAILS

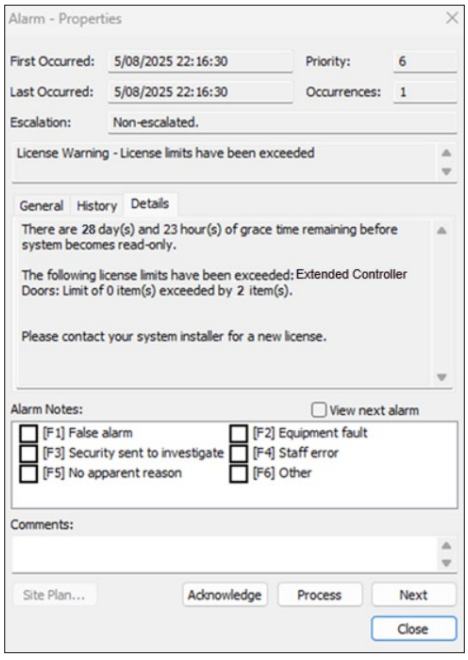
Key Benefits

- **Scalability:** Supports larger sites.
- **Cost Efficiency:** Reduces cost of network infrastructure, hardware and cabling.
- **Simplified Migration:** Eases transition from legacy systems with 10+ door configurations.
- **Performance Assurance:** C7000 controllers maintain access responsiveness even at full 24-door capacity.

Licensing Model

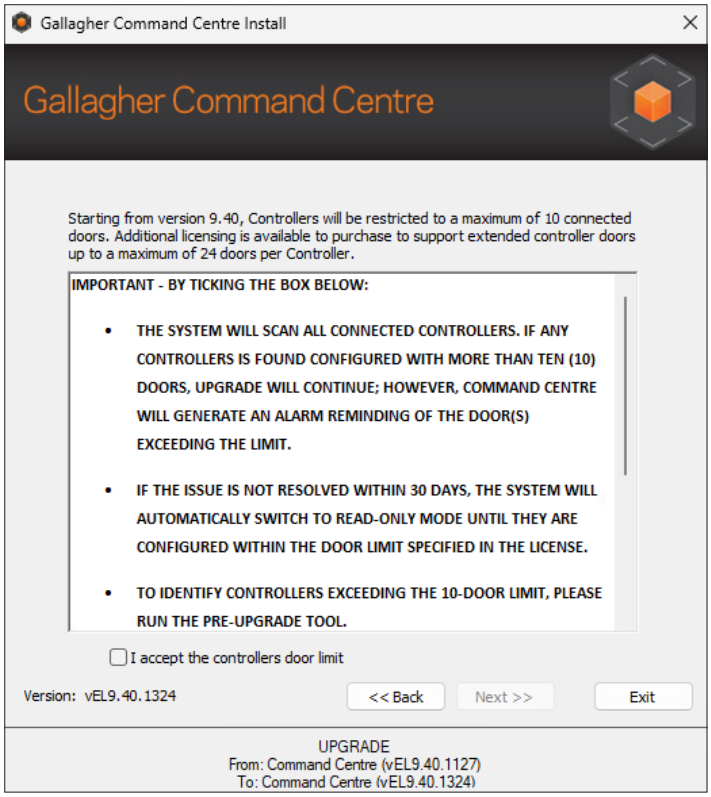
- Sites can purchase a pool of 'Extended Controller Doors' licenses, assignable to any controller exceeding 10 doors.
- A hard limit of 24 doors is enforced. Gallagher does not support configurations beyond this threshold.
- Licensing violations trigger a License Warning alarm, and unresolved violations will place the system in read-only mode after 30 days.



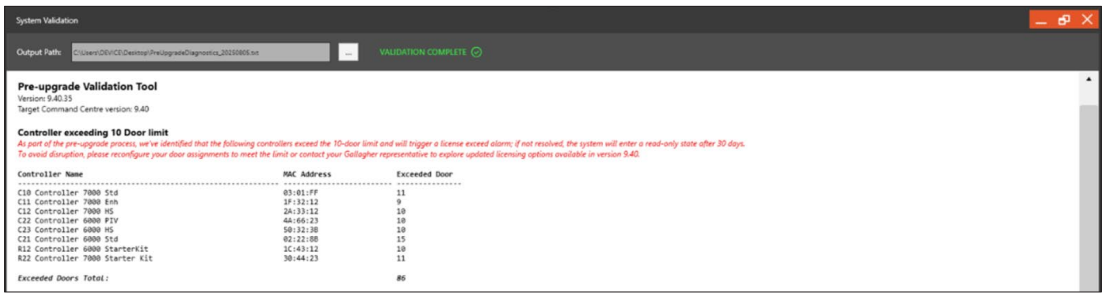


Upgrade Experience

During upgrade to v9.40, installers are prompted with a terms and conditions dialog acknowledging the new door limits.



The Pre-Upgrade Tool scans for controllers exceeding 10 doors and flags them for review.



Example Use Case

A large facility with 24 access points can now be managed by a single C7000 controller, streamlining deployment and reducing total cost of ownership.

Controller 6000 is not recommended for more than 10 doors due to performance constraints. A C6000 exceeding the ten-door limit should be reconfigured to reduce the doors, or an 'Extended Door License' purchased until the Controller can be upgraded to a C7000.

5.3 Platform health – Linux upgrades

Business value: Strengthened architecture to ensure long-term reliability, enhanced performance, and robust cyber security.

DESCRIPTION

As part of Gallagher's ongoing commitment to platform excellence, Command Centre v9.40 introduces a significant upgrade to the Linux kernel powering our Controller 6000 and Controller 7000 platforms. This update strengthens the foundation of our controller architecture, ensuring long-term reliability, enhanced performance and robust cyber security.

BENEFITS

- **Cyber Security First:** The upgraded kernel incorporates the latest protections and aligns with Gallagher's commitment to maintaining the highest standards of cyber security across all products.
- **Optimised Performance:** Improved system responsiveness and efficiency help ensure controllers operate smoothly in demanding environments.
- **Future-Ready Infrastructure:** Supports modern hardware components and prepares the platform for upcoming innovations and features.
- **Platform Health and Longevity:** Reinforces Gallagher's dedication to maintaining the health and resilience of its controller platforms over time.

WHAT THIS MEANS FOR YOU

Whether you're deploying new controllers or upgrading existing ones, this kernel enhancement ensures your Gallagher system remains secure, stable, and ready to evolve with your needs. It's another step in our mission to deliver trusted, high-performance solutions that stand the test of time.

5.4 Enhanced web server architecture for Controller 7000

Business value: Enhanced scalability to ensure our solutions are future-ready and meet the highest standards of cyber security.

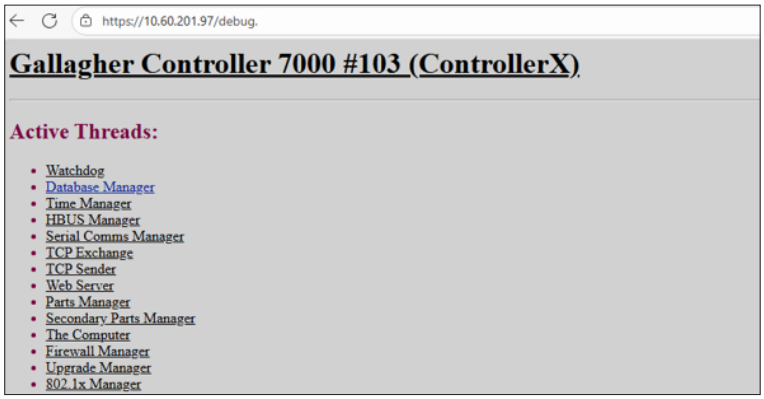
DESCRIPTION

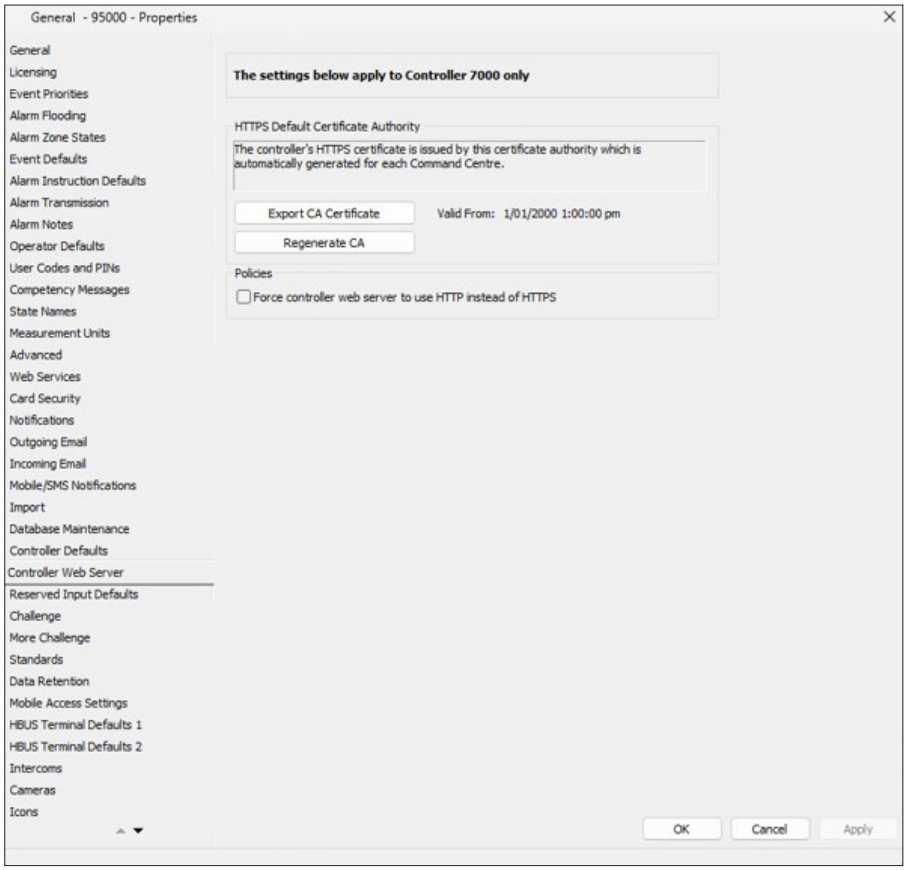
Command Centre v9.40 introduces a major upgrade to the web server architecture embedded in the Controller 7000.

This enhancement reflects Gallagher's commitment to delivering secure, scalable, and future-ready solutions, ensuring our controller platforms continue to meet the highest standards of cyber security and performance.

BENEFITS

This enhancement significantly boosts the scalability and flexibility of Controller deployments by allowing each C7000 controller to support up to 100 inter-controller communications, up from the previous limit of 60. This enables larger, more complex controller networks without compromising performance or manageability.





5.5 Identify controller override

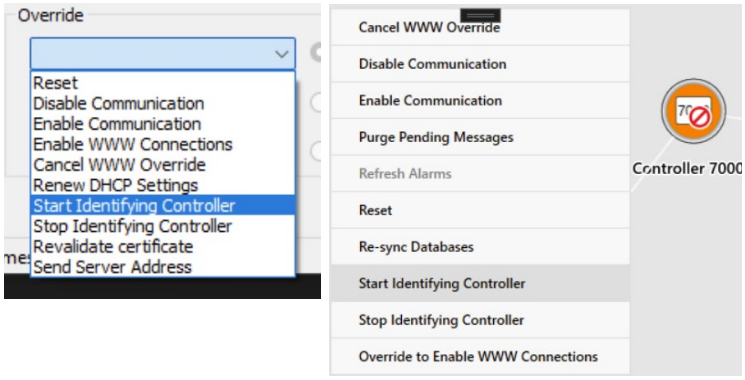
Business value: Improve installation efficiency and technician experience by allowing the identification of specific controllers when multiple units are installed in close proximity.

DESCRIPTION

This feature improves installation efficiency and technician experience by allowing physical identification of a specific Controller 7000 from within Command Centre. It eliminates confusion when multiple controllers are installed in close proximity, helping installers and site managers quickly locate the correct unit.

BENEFITS

- **Simplifies Installation:** Technicians can visually confirm which controller is being worked on.
- **No Event Raised:** The override does not affect controller status or generate events.
- **Privilege Controlled:** Only operators with View Site or Edit Site privileges can access the override.
- **UI Integration:** Available in the Controller Status and Override Page, Site Plan Viewer, Monitor Site Viewer, and View Status windows.



DETAILS

Command Centre v9.40 introduces a new override for Controller 7000 FT items:

- Stop Identifying Controller
- Start Identifying Controller

When activated, the controller's Run LED flashes five times, repeating every three seconds until stopped. This override mimics the existing "Identify HBUS Reader" functionality and uses the same Invalid Key LED flash pattern already available in firmware

Use with C7000 Single Door:

If the C7000 Single Door is configured to turn off the status LED when the cover is installed, Start Identifying Controller override takes higher priority.

- Only available for Controller 7000 models.
- Controller must be online to receive the override.
- Override does not persist or queue if the controller is offline.

Example Use Case

During a multi-controller installation, a technician at the head end can trigger the override while a colleague in the field watches for the flashing LED to confirm the correct controller is being configured.

5.6 Dual ethernet - Phase 1

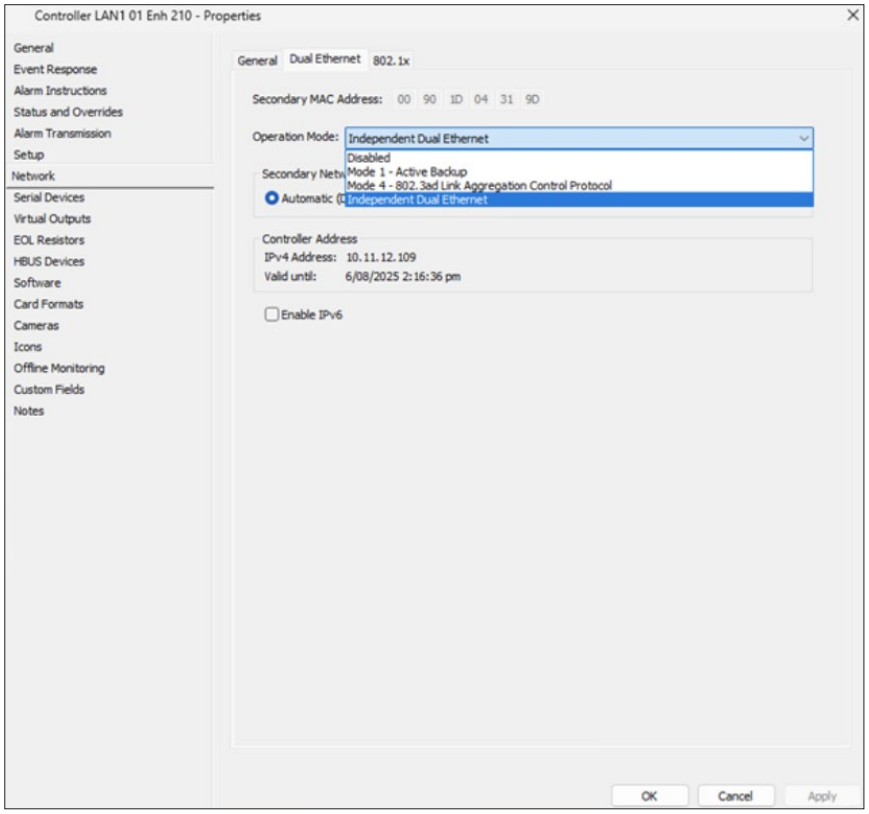
Business value: Enhance network reliability and deployment flexibility

DESCRIPTION

Phase 1 of the Independent Dual Ethernet feature on Controller 7000 introduces foundational capabilities that enhance network reliability and deployment flexibility.

BENEFITS

- **Cyber Security First:** All web server communications are now authenticated using short-lived tokens and verified through Gallagher's trusted public key infrastructure—ensuring secure and tamper-proof connections.
- **Smarter Session Management:** Operator sessions are now securely managed and automatically refreshed, providing a seamless experience without compromising security.
- **Modular Application Support:** The upgraded web server lays the foundation for future plug-in modules and app-based extensions, enabling faster innovation and easier deployment across Gallagher's ecosystem.
- **Platform Health and Resilience:** These changes reinforce Gallagher's long-term commitment to maintaining the health and reliability of its controller platforms, ensuring they remain robust and adaptable to evolving customer needs.



5.7 Increase HBUS readers from 20 to 48

Business value: Enhanced scalability to support larger sites, and increased cost efficiency by reducing additional controller and infrastructure costs.

DESCRIPTION

Command Centre v9.40 introduces support for up to 48 HBUS readers on all variants of the Controller 7000. This change applies to Standard, Enhanced, and High Security models. The previous limit of 20 readers has been lifted following successful performance testing across extended cable lengths up to 500m.

BENEFITS

This enhancement significantly increases the scalability of Gallagher's access control deployments by doubling the number of supported HBUS readers on the Controller 7000 - from 20 to 48. This will enable C7000s to support more doors.

- **Scalability:** Supports larger sites with more doors and devices per controller.
- **Cost Efficiency:** Reduces the need for additional controllers and associated infrastructure.

DETAILS

Licensing Notes

- No additional licensing is required for the increased HBUS reader count.
- Applies only to HBUS readers.

Example Use Case

A multi-building facility can now connect up to 48 HBUS readers to a single C7000 controller, streamlining access control across multiple entry points while maintaining centralized management.

5.8 Increase OSDP readers from 16 to 32

Business value: Enhanced support for high-density access control deployments, broader coverage, reduced hardware overheads, and support for more flexible site configurations.

DESCRIPTION

Command Centre v9.40 introduces support for up to 32 OSDP readers on all variants of the Controller 7000. Each RS485 port can support up to 16 OSDP readers, and with two ports available, the total capacity per controller is now doubled.

BENEFITS

This enhancement significantly improves Gallagher's ability to support high-density access control

deployments by increasing the number of supported OSDP readers per Controller 7000 from 16 to 32 readers. It enables broader coverage, reduces hardware overhead and supports more flexible site configurations.

- **Scalability:** Supports larger installations.
- **Cost Efficiency:** Reduces the need for additional controllers and associated infrastructure.
- **Improved Site Takeover:** Aligns with Quick Switch functionality, allowing up to 16 doors per controller during migration scenarios

UI and Configuration Updates

- The Command Centre UI now allows configuration of up to 32 OSDP readers per C7000.
- A warning message will appear if more than 16 readers are assigned to a single RS485 port:
  - *"There are too many OSDP devices assigned to this bus."*

Hardware Integration

- Customers may use OSDP hubs to connect multiple readers, but the per-Controller port limit of 16 remains.

Example Use Case

A facility can now deploy 32 OSDP readers per Controller 7000, enabling centralized control of multiple entry points while maintaining fast and reliable access response.

5.9 Increase inter-controller comms from 60 to 100

Business value: Enhanced scalability and flexibility of Controller deployments to enable larger, more complex controller networks without compromising performance or manageability.

DESCRIPTION

Starting with Command Centre version 9.40, all variants of the Controller 7000 will support up to 100 concurrent inter-controller communication links. This change applies to Standard, Enhanced, and High Security models. The Controller 6000 remains capped at 60 links.

BENEFITS

This enhancement significantly boosts the scalability and flexibility of Controller deployments by allowing each C7000 to support up to 100 inter-controller communications, up from the previous limit of 60. This enables larger, more complex controller networks without compromising performance or manageability.

- **Greater Network Scalability:** Supports larger controller meshes for expansive sites.
- **Improved Redundancy and Coordination:** Enhances peer-to-peer messaging for alarms, inputs, and outputs.
- **Futureproofing:** Aligns with roadmap goals for high-density deployments and advanced controller features.

DETAILS

Compatibility Notes

- C7000 units running versions prior to 9.40 will retain the previous 60-link limit.
- No changes are made to C6000 controller capabilities

Example Use Case

A large campus with up to 100 C7000s can now fully interlink all C7000 controllers without needing to segment or compromise on peer communication, simplifying configuration and improving system responsiveness.

- Greater Network Scalability: Supports larger controller meshes for expansive sites.
- Improved Redundancy and Coordination: Enhances peer-to-peer messaging for alarms, inputs, and outputs.
- Futureproofing: Aligns with roadmap goals for high-density deployments and advanced controller features.

6 Minor Enhancements

6.1 Nedap ANPR Lumo and Nedap DESFire Boosters in Core

DESCRIPTION

Command Centre v9.40 includes in core enhancements to support the Nedap ANPR Lumo Cameras and Nedap Boosters for DESFire cards, eliminating the need for a separate CustCard DLL.

BENEFITS - NEDAP ANPR LUMO CAMERAS

Simplified setup: Operators can now enter license plates directly as text-format card numbers, eliminating the need for Universal Card Format (UCF) conversion

- **Native integration:** No need for a separate CustCard DLL, reducing complexity and maintenance overhead
- **Flexible configuration:** Supports direct Wiegand64 communication, enabling real-time access decisions based on plate recognition
- **Multi-region support:** Classifiers for New Zealand, Australia, and US plates ensure accurate recognition across geographies.

BENEFITS - NEDAP DESFIRE BOOSTERS

- **Secure vehicle access:** Enables MIFARE DESFire cards to be used with Nedap Boosters for high-assurance vehicle identification
- **Dual authentication:** Supports configurations where both vehicle and driver credentials are required for access, enhancing security
- **Streamlined configuration:** Uses a configuration card to program boosters,
- **No DLL required:** Like the ANPR Lumo, this feature is now part of the core system, reducing reliance on custom software.

6.2 Mobile Credentials support with SALTO wired Readers

DESCRIPTION

Command Centre v9.40 introduces support for 128-bit Wiegand data format, enabling mobile credentials to work seamlessly with wired SALTO readers and Gallagher controllers via the UBOX 4000 hardware. Command Centre now supports access and event tracking for mobile devices alongside traditional cards at SALTO wired readers setup as Gallagher Third party Wiegand readers. Note this functionality is only available in SALTO Native mode.

BENEFITS

- **Modern credential support:** Enables mobile devices to be used for access at SALTO wired readers via 128-bit Wiegand format
- **Seamless integration:** Works with Gallagher controllers and UBOX 4000 hardware, allowing mobile and card credentials to coexist
- **Enhanced security:** Native mode supports encrypted HTTPS communication with SALTO servers, improving data protection.

6.3 MorphoWave XP2 supported with Command Centre v9.40

DESCRIPTION

Command Centre v9.40 introduces support for the MorphoWave XP2, enabling seamless integration of IDEMIA's advanced contactless 3D fingerprint scanning technology for secure, high-throughput access control. Cardholders can be identified in less than one second with a simple wave of the hand. The MorphoWave XP2 supports up to 100,000 biometric templates and offers various authentication options including biometrics, card and PIN code credentials.

BENEFITS

- **High-throughput access:** Identifies cardholders in under one second with a simple wave of the hand.
- **Multi-factor authentication:** Supports biometrics, card, and PIN for layered security.
- **Scalability:** Handles up to 100,000 biometric templates, suitable for large-scale deployments.
- **Touchless experience:** Ideal for hygiene-sensitive environments and fast-moving entry points.

High quality T10 Security Torx Screwdriver for the installation and removal of T Series readers. Features palm pivot and hardened steel driver.

GALLAGHER Security

Information contained in this document is intended for general information only. While every effort has been taken to ensure accuracy as at the date of the document, there may be errors or inaccuracies and specific details may be subject to change without notice.
Copyright © Gallagher Group Limited 2025. All rights reserved.

Talk to us today

Join us on

security.gallagher.com

10/25