Command Centre v9.50

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 8
2.8 Command Centre Mobile Connect app compatibility 8
2.9 Command Centre Web browser compatibility 8
2.10 FIDO2 compatibility 8

3 Command Centre Features and Enhancements 9

3.1 AccessNow 9
3.2 Accessibility Adjustments: PIN Exemption 11
3.3 VisionPass SP Fingerscan Module 12
3.4 Reporting Dataset 13
3.5 Manual Access Event support in Time Report 15
3.6 Secure Controller Diagnostics - Retrieve controller logs 16

4 Readers & Controllers 17

4.1 Ethernet Bridging 17
4.2 Dual Ethernet Expansion 18

5 Minor Enhancements 19

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 v9.50 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 v9.50 may impact on the configuration of sites upgrading from earlier versions. Refer to the document '3E0068 Release Note Command Centre vEL9.50.XXXX (Upgrade Procedures).pdf' for further details.

Supported upgrade paths

- Command Centre v9.10 – Command Centre v9.50
- Command Centre v9.20 – Command Centre v9.50
- Command Centre v9.30 - Command Centre v9.50
- Command Centre v9.40 - Command Centre v9.50

CONTROLLER FIRMWARE COMPATIBILITY

Command Centre v9.50 supports the Controller 6000 and Controller 7000 firmware vCR9.50 . Command Centre v9.50 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 v9.50 versions once Command Centre has been upgraded. It is recommended to upgrade all controller firmware to the latest version as soon as possible.

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.

Important: Please read the below pre-upgrade information before upgrading to v9.50

PRE-UPGRADE VALIDATION TOOL V9.50

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 v9.50. 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 VCR9.50

Controllers running v8.20 or later (Linux) can be upgraded to v9.50 in less than two minutes. Controllers running v8.10.179 onwards (WinCE) can be migrated directly to v9.50 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 vEL9.50.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 Server 2025
- Windows Server 2022
- Windows Server 2019

COMMAND CENTRE WORKSTATION

- Windows 11 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 no longer supported under Microsoft's Fixed Lifecycle Policy. Microsoft has ceased 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.

Command Centre database
Microsoft SQL Server 2025/2025 Express
Microsoft SQL Server 2022/2022 Express
Microsoft SQL Server 2019/2019 Express

Note: SQL Server Express is the default database that is freely available for Command Centre. It is recommended that sites utilize the Microsoft SQL version that suits their present and future needs.

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 v9.50 from a previous version 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

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 130+
- Microsoft Edge version 130+
- Safari 18+

2.10 FIDO2 compatibility

FIDO2 logon requires Windows 10 version 1903 or later.

3 Command Centre Features and Enhancements

3.1 AccessNow

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.

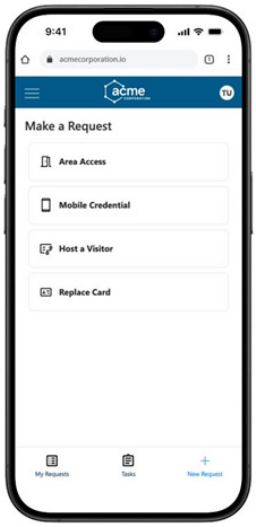
With its intuitive, no-code workflow builder, security teams can easily design and customise automation for every type of request they receive.

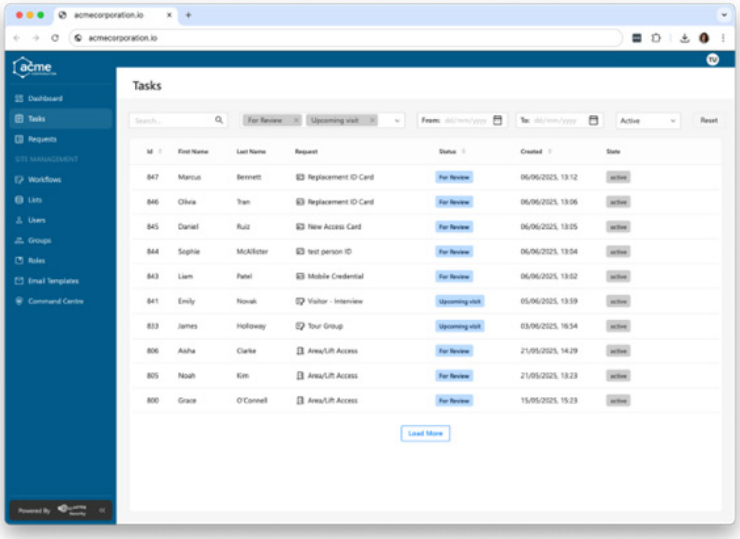
BENEFITS

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.

DETAILS:





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:

  - ACCESSNOW SMALL REQUEST PACK (1000) – Pack of 1,000 requests.
  - 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:

1. **Contact your Gallagher Business Development Manager** to initiate the request.
2. **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 Accessibility Adjustments: PIN Exemption

DESCRIPTION

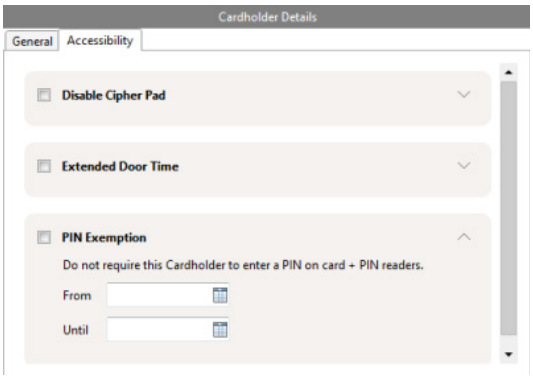
Adds a new accessibility option for cardholders, a PIN exemption. This allows a cardholder to be exempt from the requirement to input a PIN in areas that require card + PIN. The accessibility adjustments have been shifted to a new tab under cardholder details.

BUSINESS VALUE

Enables employers to adjust security practices to accommodate the accessibility needs of their staff.

DETAILS

A new accessibility option has been added to cardholders in Command Centre. It allows a cardholder to have an exemption to the requirement to put a PIN in areas that are secured with card + PIN. A tab has been added to cardholder details tile with the heading 'Accessibility' and the accessibility options have been shifted there.



Accessibility tab on cardholder details tile

A reporting option has been added to search for cardholders with particular accessibility options selected. PIN exemption has an option for from and until for a situation where someone has a temporary accessibility need.

PIN Exemption is configurable through Command Centre APIs.

Notes:

- No license is needed for this feature.
- Edit cardholder privilege is required for an operator to view.
- This replaces an existing feature that allowed cardholders to be exempt from PINs at an access group level.
- Accessibility options have been removed from the Command Centre configuration client.
- PIN Exemption also works with carparks, lifts, and lockers features.

3.3 VisionPass SP Fingerscan Module

DESCRIPTION

Command Centre v9.50 now offers support for the VisionPass SP Fingerscan Module. Functionality is limited to biometric face or fingerprint authentication exclusively. Card plus biometric access is only compatible with face templates stored on the card; fingerprint templates on card are not supported by VisionPass SP with Fingerscan Module.

BENEFIT

Operational Continuity in Real World Conditions

With the integration of facial recognition and fingerprint scanning as two complementary biometric methods, the VisionPass SP Fingerscan module provides dependable access control, maintaining effectiveness even if environmental, cultural, or operational factors affect one method.

Use Case 1 – Cultural and Regional Requirements

In regions such as the Middle East, where some women are required to wear face coverings, facial recognition may not always be appropriate or acceptable. The addition of a fingerprint reader provides an alternative biometric method, allowing individuals to gain access without compromising cultural traditions, while still maintaining strong identity assurance.

Use Case 2 – Challenging Environmental Conditions

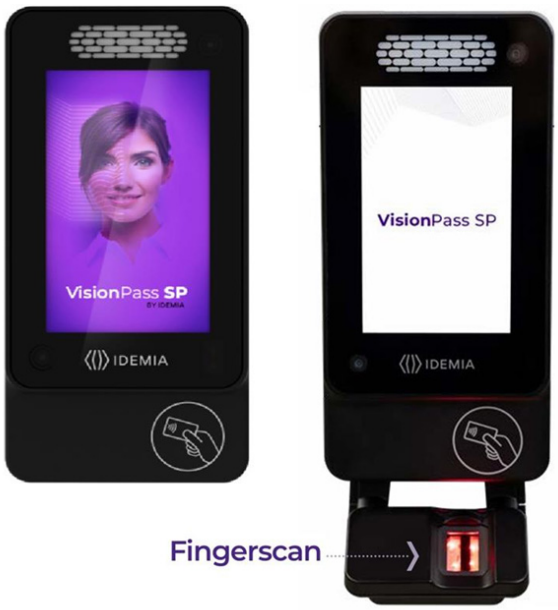
At vehicle entrances or perimeter access points, variable lighting conditions such as glare, or low light can affect facial recognition performance. In these scenarios, the fingerprint scanner offers a reliable secondary authentication method, ensuring consistent access for authorised users without reverting to cards or manual processes.

DETAILS

The VisionPass SP Fingerscan bridges the gap between fingerprint and facial recognition technologies, it integrates seamlessly with VisionPass SP, providing dual biometric modalities, enabling inclusive and efficient access control in any conditions. This adaptability and reliability make it an essential tool for modern, future-ready biometric systems.

Features include:

- High-quality fingerprint sensor designed for fast, accurate, and reliable biometric authentication
- Presentation Attack Detection
- Robust IP65-rated enclosure suitable for challenging environments
- Embedded secure communication to ensure data integrity
- Streamlined USB deployment for simplified integration



3.4 Reporting Dataset

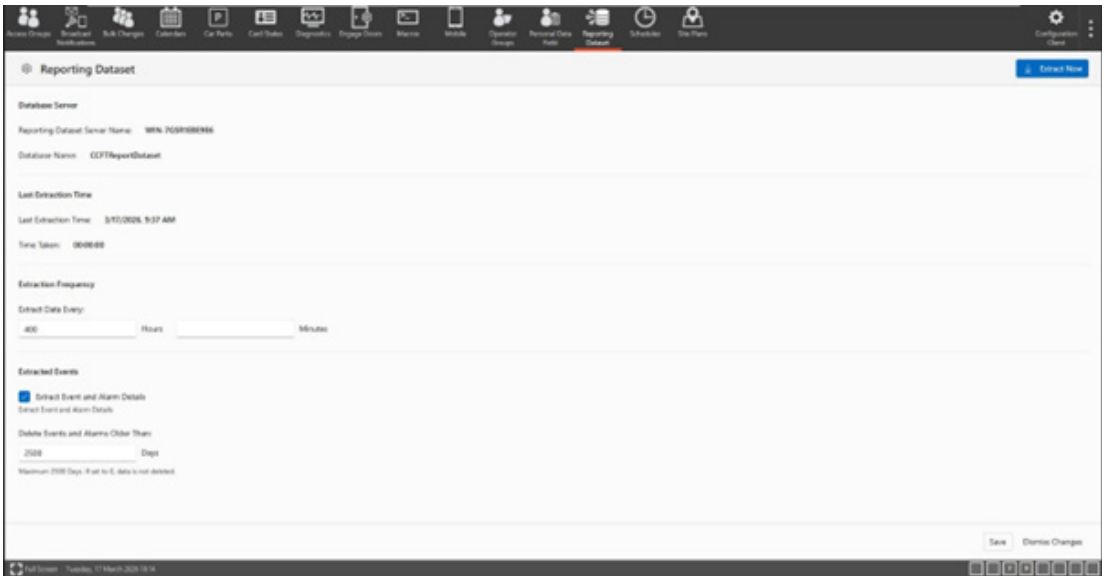
DESCRIPTION

A new Reporting Dataset feature provides a new database that runs along side Command Centre. This enables users to connect their Command Centre data to third-party analytics platforms such as Microsoft Power BI, Tableau, and Excel, allowing for advanced data visualization, trend analysis, and custom reporting.

BUSINESS VALUE

The new reporting dataset feature empowers users to extract and analyze access control data using third-party solutions, enabling deeper insights into security trends, operational patterns, and user behavior. This enhances decision-making, improves efficiency, and supports data-driven strategies across facilities and security teams.

DETAILS



PRIVILEGES

New Privilege for managing the Reporting Dataset Parameters (Manage Reporting Dataset Extractions)

LICENSING

A new license option that will enable the administration of the Reporting Dataset service.

[Features]

ReportingDataset=1

Note: Installed as a separate AppHost Module

3.5 Manual Access Event support in Time Report

DESCRIPTION

The Time Report now supports manual cardholder movement events including:

- Current and historical manual access events initiated from a Cardholder Viewer
- Tagboard manual movements
- Mobile Client manual movements

BUSINESS VALUE

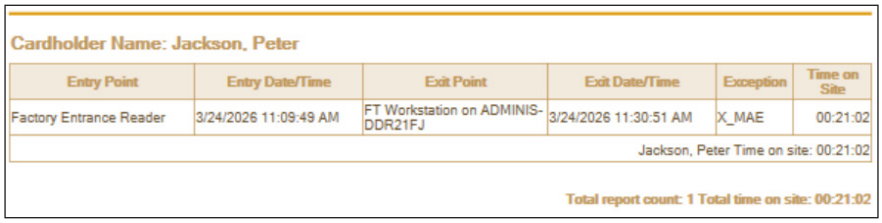
Manual access events retrospectively update cardholder movements to prevent skewed time-based data and zone location when cardholders manage to enter or exit site without using a credential (tailgating). This is particularly useful when movement data is used for safety, payroll, or contractor billing.

When cardholders tailgate entering or exiting a site, manually created historical movement events can now be optionally included in Time Reports to correct time-on-site data.

DETAILS

To include manual movements in Time Reports, an Exception filter must be added with the E_MAE (entry manual access events) and/or X_MAE (exit manual access events) exceptions included.

Entry and exit pairs (rows) in the time report with associated manual access events will be tagged with these exceptions where applicable



Cardholder Name: Jackson, Peter

Entry Point	Entry Date/Time	Exit Point	Exit Date/Time	Exception	Time on Site
Factory Entrance Reader	3/24/2026 11:09:49 AM	FT Workstation on ADMINIS-DDR21FJ	3/24/2026 11:30:51 AM	X_MAE	00:21:02
					Jackson, Peter Time on site: 00:21:02

Total report count: 1 Total time on site: 00:21:02

3.6 Secure Controller Diagnostics - Retrieve controller logs

DESCRIPTION

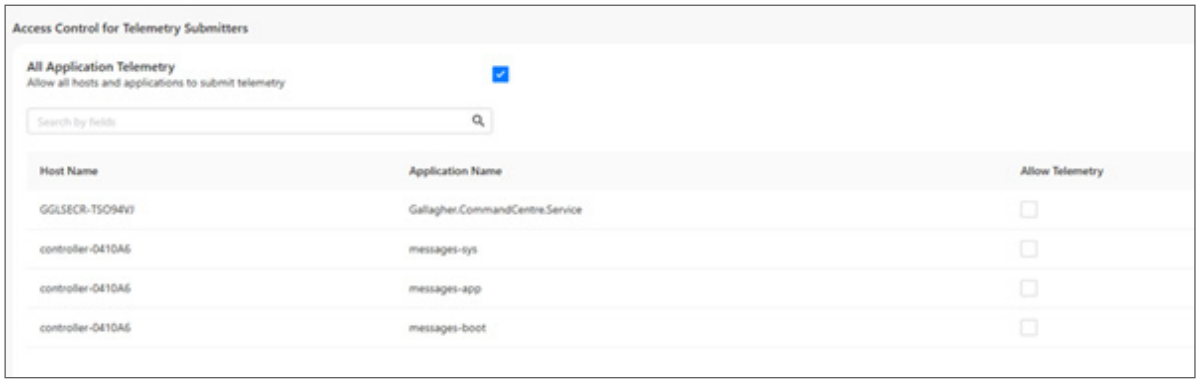
Secure Controller Diagnostics expands the capabilities of the Diagnostics Service to be able to collect controller logs.

BUSINESS VALUE

Adds a secure way to automatically retrieve controller logs without having to login individually to each controller.

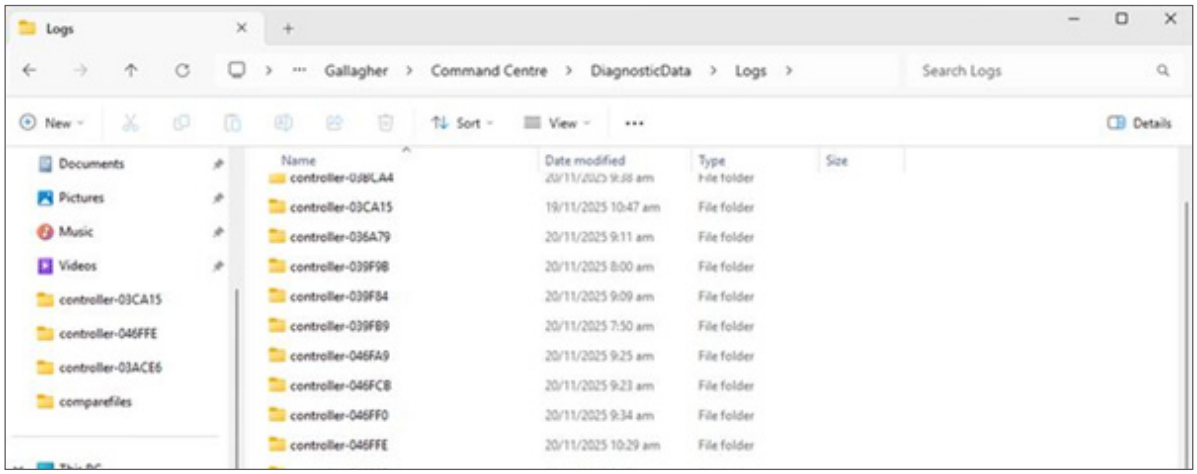
DETAILS

The image below shows the telemetry options for a Controller with the last 6 digits of the mac address. Selecting the check box will send those logs to the Diagnostics Service. Three controller logs are collected from connected controllers 'messages-app', 'messages-boot', and 'messages-sys'.



Diagnostics Service setup for devices / applications that can send data to the Diagnostics Service.

Files are saved to a designated location under the 'logs' directory, if the Diagnostic Service is setup to store telemetry. Each file will contain the logs that have been selected for the specific controller.



Stored Controller logs

New Alarm

Certificate checking has been implemented in the diagnostic service. A new alarm has been created in the event that a certificate is invalid. This allows an operator to check to see if someone is attempting to spoof the diagnostics being sent from a controller or application to the Diagnostics Service.

4 Readers & Controllers

4.1 Ethernet Bridging

DESCRIPTION

Allows the controller's second Ethernet interface to operate as a transparent network bridge, enabling up to four IP devices to connect through the controller without requiring an additional switch port or network cable.

BENEFIT

Ethernet Bridging reduces installation complexity and cost by allowing installers to connect additional IP devices - such as another controller or an IP camera - via the controller's secondary Ethernet port. This can eliminate the need to run additional Ethernet cabling back to a network switch, particularly in retrofit or constrained environments

DETAILS

When Ethernet Bridging is enabled:

- The controller operates as a Layer 2 transparent bridge between its primary and secondary Ethernet ports.
- All network traffic is forwarded without inspection, filtering or modification.
- The controller remains fully functional and accessible via its primary Ethernet interface.
- Bridging behaviour is independent of whether the controller is using static IP addressing or DHCP.

The bridge is not responsible for enforcing security or traffic control; those controls are expected to be implemented elsewhere in the network.

CONFIGURATION IN COMMAND CENTRE

Ethernet Bridging is configured directly in Command Centre:

- Navigate to Controller Properties → Network → Dual Ethernet
- Select "Ethernet Bridge" from the Operation Mode drop down

When upgrading to Command Centre v9.50:

- Existing Dual Ethernet configurations are retained and preserved
- "Ethernet Bridge" becomes an additional selectable operation mode for supported controllers

VISIBILITY & DIAGNOSTICS

When a controller is operating in bridged mode:

- The bridge status is displayed on the controller debug web pages
- The configuration is included in Command Centre site configuration reports

This provides clear visibility for commissioning, troubleshooting, and support.

SUPPORTED HARDWARE

- C7000 Enhanced Controller
- C7000 High Security Controller

SCOPE & LIMITATIONS

- Ethernet Bridging does not provide routing, firewalling, or traffic shaping
- Advanced network security controls remain the responsibility of the wider network design
- The feature is limited to dual Ethernet C7000 Enhanced and High Security controllers

4.2 Dual Ethernet Expansion

DESCRIPTION

Dual Ethernet Expansion improves clarity, reliability and supportability when deploying controllers into segmented or multi-NIC network environments, by introducing support for inter-controller communication behaviour and improved guidance for designing network connections.

BENEFITS

By defining supported communication paths and constraints, this expansion improves reliability, supportability, and design confidence for complex or segmented network deployments - without changing the fundamental hardware capabilities of Dual Ethernet controllers.

DETAILS

When Dual Ethernet is enabled:

- Controllers communicate with other controllers in the normal way
- The secondary Ethernet interface support for controller to controller connections is available when required
- Controller to server communication continues to operate over the configured network paths

When controllers are deployed across different subnets:

- A Layer 3 router or Layer 3 switch is required to route traffic appropriately
- Network design must ensure the primary interfaces are reachable for inter controller communication

Supported Configurations

- High Sec and Enhanced Controller 7000 variants
- Controller to server communication across segmented networks

5 Minor Enhancements

Remove Apple Account Binding

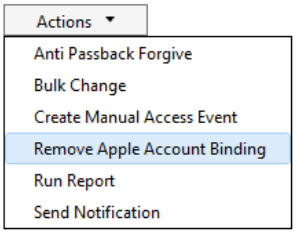
DESCRIPTION

The Apple Employee Badge solution employs strong account binding and a badge device transfer limit to prevent fraudulent use of Apple badges. In Command Centre v9.50, a privileged operator can remove a cardholder's binding and reset the badge transfer limit, enabling the cardholder to provision a new Apple badge with a fresh binding and transfer limit.

BENEFIT

When a cardholder receives the message "Credential Already Linked to Another iCloud Account" or "Device Migration Limit Exceeded" on their phone, a suitably privileged operator (after verifying the cardholder's identity) can remove the cardholder's binding and reset the transfer limit, enabling them to provision a new Apple badge.

This feature introduces the Cardholder Viewer Action "Remove Apple Account Binding" and the Operator Privilege "Remove Apple Account Binding".



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

04/26