



Gallagher Access Engineer Course - C892320



Introduction

Gallagher Access Engineer Certification provides attendees with the knowledge necessary to develop advanced security solutions within the Gallagher Command Centre. Differing levels of security are explored based on scenarios utilising key functionality with an emphasis on in-market flexibility.

Note: Certification is valid for a period of 2 years after which time re-certification is required to maintain certified status.



Goals

Upon completion of training attendees will have the skills necessary to implement the additional features available in Gallagher Command Centre.

- See **Modules** list for features

Attendees will understand the advanced functionality associated to the Gallagher Command Centre and how to configure the system, utilising these features when developing complex security solutions.



Prerequisites

Prerequisites:

- **Gallagher Access Technician Course** - Have successfully completed the Gallagher Access Technician Course
- **PC Skills** - Keyboard skills, an understanding of current Microsoft Operating Systems, create folders, save files, copy files and the Control Panel



Modules

Health Care Scenario

- Healthcare Scenario
 - System Divisions
 - Operators and Divisions
 - Inheritance of Division Privileges
 - Setting up System Divisions
- **Operator Groups and Divisions**
- **Macros**
 - Securing an Access Zone via (Lockdown)
 - Setting up the T20 Mimic Panel
 - Setting the LED flash sequence
- **Action Plans**
- **Alarm Instructions**
 - Creating a New Alarm Instruction
- **Insertion Tags**
 - Creating an Insertion Tag
 - Assigning Alarm Instructions
 - Viewing Alarm Instructions in Command Centre
- **Guard Tours for Gallagher Command Centre**
 - Configuring a Guard Tour
 - Guard Tours & the Event Response Tab
 - Guard Tours & the Status and Overrides Tab
 - Running a Guard Tour
 - Restarting a Guard Tour (if halted)
- **Site Plans**
 - Setting up Site Plans
 - Layering Site Plans
 - Adding Items to Site Plans
 - Using Graphics to Replace Icons
 - Adding a Macro to a Site Plan
 - Creating a New Icon Set
- **Command Centre Scenario**

Mining Scenario

- **Identity Analytics**
 - Configuring Competencies
 - Access Zone Competencies
 - Assigning Competencies
 - Configuring Cardholders
 - Adding a Competency to a Cardholder
- **Anti-passback**
 - Configuring Anti-passback
 - Anti-passback Forgive after Time
 - Anti-passback Forgive all Cardholders
 - Anti-passback Forgive a specific Cardholder
- **Event Notification Filters**
 - Email and Mobile PDF's
 - Enabling your Event Notifications
 - Creating a Notification Schedule
 - Assigning a Notification Schedule
 - Setting up the Email and SMS Server
- **Zone Counting**
 - Configuring Zone Counting Events
- **Command Centre Scenario**
 - Tag Board Tile

Education Scenario

- **Access Group Lineage**
 - Master Access Group
 - Assigning Lineage
- **First Card Unlock**
- **Personalised Actions**
 - Controlling Lockers
 - Configuring Locker Personalised Actions
 - Testing the Locker Scenario
 - Access Granted vs Access Taken Options
 - Using Macros in Personalised Actions

-
- **Enterprise Data Interface**
 - Operator Privileges
 - The Run as Operator
 - Creating the Run as Operator
 - The Source File
 - Enterprise Data Interface Folders
 - Create Local File Locations on the Server
 - Importing Images with EDI
 - Configuring Command Centre to Receive the Source Data
 - Create/Configure Personal Data Fields
 - Creating an EDI Interface
 - Setting the Mapping of Data between the Source File and Command Centre Data
 - Creating a Transformation Mapping
 - Adding a Card Transformation
 - Adding Access Group Transformations
 - Running EDI Manually
 - Error Messages and Log Files
 - **Command Centre Scenario**

Data Centre Scenario

- **Low Level Elevator Cars**
 - Creating the Elevator Controls
 - Access Zone Modes
 - Virtual Outputs
 - Inputs
 - Elevator Car
 - Configuring Elevator Floors
 - Advanced
 - Configure Access Group
 - Card Pin Codes
 - Reporting
- **Interlocking Doors**
 - Adding a New Interlock Group
- **Challenge**
 - Setting up Challenge

-
- Setting up the Access Group
 - **Logic Blocks**
 - Logic Block Rules
 - Introducing Logic Block Configurations
 - Controlling an Alarm Zone
 - Assigning Alarm Zone Privileges
 - How the Logic Works
 - **Contact ID**
 - Setting up the GG for the Server Room Alarm
 - Intruder Alarm Example
 - Panic Alarm Example
 - General Information
 - **Command Centre Scenario**

Evaluation
