QUANIKA (Enterprise) A&E Specification

May 08th, 2024

Document Control Information

Document Title: Quanika (Enterprise) A&E Specification

Revision History

Version	Date	Description
QU-EN-AE- 1009	10/09/2020	Revision 1
QU-EN-AE-1010	12/04/2021	Revision 2
QU-EN-AE-1011	17/06/2021	New Features
QU-EN-AE-1012	17/05/2022	Facial Recognition
QU-EN-AE-1013	08/05/2024	New Features

Table of Contents

Quanika Access Control System (QAC) Overview

Scalability

The QAC shall support small two-reader access systems up to medium size, multi-building, multi-site systems supporting up 128 number of doors and unlimited card holders using a single suite of software.

Available software modules shall include

1. Access Control Software Module.
2. Alarm Management & Reporting Software Module.
3. Interactive Graphical Floorplans Software Module.
4. Q-Vision Video Integration module.
5. Elevator Control.
6. Mustering Solution.
7. Visitor management System
8. Access and door controllers.
9. Data Exchange Service
10. Time & Attendance Reporting Software Module.
11. Mobile Identification and Verification Software Module.
12. Report Generation Software Module.
13. Area Configuration management
14. Data redundancy support
15. Database Integration support
16. Database Archiving
17. Alarm Management system
18. Cardholder Management
19. Cardholder template designer
20. Cardholder badge designer
21. Access levels and access level groups
22. Doors and Door groups
23. Statistics
24. Operator and operator role permissions.
25. Cardholder synchronization from Active directory
26. Dynamic Reporting
27. Schedule email reporting
28. Id badging
29. Data Import/Export
30. System partitioning
31. Digifort Camera Integration
32. Milestone Camera Integration
33. SIP (Voice Over Internet Protocol) Integration
34. STid Integration
35. HID Origo Integration

36. HID Digital id
37. Bulk cardholder enrollment
38. Input Zones
39. Alarm Routing
40. Facial Integration (Safr and Akuvox)
41. Traka key management
42. Manual control for doors, sensors, elevators
43. License Plate Number Integration
44. Sensor/Output Management
45. Mustering systems
46. Schedules application on doors, access levels and identification types
47. Live chat and Ticketing
48. Event receiver over TCP or Serial communication

System Requirements

The QAC software shall be designed as a fully integrated, full featured, Security Management System software package. The QAC software shall be fully compatible with x86 and x64 versions of all approved operating systems.

In order to run the Quanika Enterprise Software, following should be the minimum system requirements

1. Quad Core Processor or better (core Ix or XEON)
2. 16 GB ECC SD RAM minimum
3. 300 GB minimum disk drive
4. 10/1000 Ethernet NIC

The following are the supported operating systems of Quanika application

1. Windows 8 ,10 & 11
2. Windows Server 2019
3. Windows Server 2016
4. Windows Server 2016 R2
5. Windows Server 2014
6. Windows Server 2014 R2

The QAC software is fully compatible with the following SQL database engines:

1. SQL Server 2022 (Express, Standard, Enterprise (x86, x64)
2. SQL Server 2019 (Express, Standard, Enterprise (x86, x64)
3. SQL Server 2017 (Express, Standard, Enterprise (x86, x64)
4. SQL Server 2016 (Express, Standard, Enterprise (x86, x64)
5. SQL Server 2014 (Express, Standard, Enterprise (x86, x64)
6. SQL Server 2012 (Express, Standard, Enterprise (x86, x64)

System Overview

The QAC software shall be of an open architecture design. The QAC software shall be ODBC

compliant; supporting industry standard, off-the-shelf, relational databases. It is compatible with standard network communications, field controller hardware, and other standard- based systems and devices. It can be easily integrate/interface with 3rd-party software and hardware through the use of available SDK's and or API's.

The QAC is a true multi-user, multi-tasking operation software. The host server and client workstations include an operator interface supporting full system command & control functionality, database configuration and reporting capabilities. The functionality of the software is not limited in any way except by user authentication and individually defined operator permissions.

The QAC software dashboard screen provides the system monitoring and control functions including an alarm log window, a transaction log window, interactive graphical plans, system statistics window, cardholder picture, live camera video and other supporting functions.

The QAC access control software supports the creation and configuration of an unlimited number of schedules. Each schedule shall define specific day and time criteria applicable to various hardware & software time-controlled functions within the system, including cardholder access privileges at doors, scheduled override commands to system devices.

The QAC access control software supports Elevator control using I/O Peripheral devices. The elevator access for cardholders is manageable and can be configured through a dedicated interface.

The QAC access control software supports Mustering system. Using Mustering feature, multiple areas can be monitored. The statistics & reporting is available for operational and security staff.

The system functions and features are explained in detail below.

Dashboard

Alarm Monitoring

The QAC software provides full featured alarm monitoring and control of alarm, trouble, and off-normal conditions from various devices including card reader-controlled doors and any other type of alarm sensor connected to inputs on the system

The alarm log window provides real time alarms from controllers. The number of real time alarms in the list can be increased or decreased through a selection from dropdown list. Real time transaction logs can be extracted from the log list in the formats of csv, txt and pdf. The operator with the valid privileges can acknowledge or delete alarms. Alarm notes can be added to each alarm which can be used for reporting purpose in future. Alarm events are reported and listed in the alarm log in the order of priority and date/time and number of occurrences.

Transaction logs

The transaction logs are separately getting recorded and shown in the software. The number of real time transaction logs in the list can be increased or decreased through a selection from dropdown list. Real time transaction logs can be extracted from the log list in the formats of csv, txt and pdf.

Cardholder Picture

The cardholder picture window displays the picture of respective cardholder against every transaction. This can facilitate security staff identifying an individual without going into the details of transaction details.

Live Camera

Operators can select a camera of their choice to be viewed on dashboard all the time. The same live camera window can be used to show video related to transaction.

Plan Manager

The QAC support the interactive graphical plans and maps. The plans configuration shall allow for the linking of maps via navigation Icons, allowing the QAC user to move from map to map with single mouse click. There shall be no limit to the number of plans that can be used in the QAC. The plans allow for the assignment of interactive Icons for the following

1. Doors
2. Inputs (sensors).
3. Outputs.
4. Outputs Groups.
5. CCTV

The interactive Floor plans allow the system operators through Icons to perform functions like

1. Unlock doors,
2. Lock doors
3. Momentary Unlock Doors,
4. Lockdown doors
5. Lockdown Clear doors
6. Acknowledge alarms
7. Delete Alarms
8. Add Alarm Notes
9. View Camera
10. Switch On/Off Outputs
11. Access Intercom
12. Plan Navigation

The following options of the plan is configurable from the settings

1. Plan manager is a floating window and provide flexibility to set it up on a separate window.
2. Default plan can be selected through settings.
3. The time out settings that a plan will remain displayed after alarm is received and before returning to the default plan.

4. ‘Jump’ to the specific plan after alarm is received.
5. Set the icon size
6. Show the name and status of a point on a plan if the cursor is placed over the icon (tooltip).

Q-Vision Video Integrator

The Q-Vision is a Video Integration Interface built to have flexibility to integrate with any video management software like Milestone, Digifort etc. With this interface the QCS has got a powerful and integrated interface where security staff can relate alarms with video.
Q-vision communicate and extract the list of cameras from the video management systems and provide operators the following features

1. Create Views
2. Create Matrix
3. Playback recording videos
4. View Live videos
5. Transaction Search
6. PTZ Control
7. Presets
8. JPEG Snapshot of Live image
9. Download of Video Clip
10. Record video for specified time

The Q-Vision video application allows for the following Video display configurations:

1. 1 x 1 Camera
2. 1 x 2 Cameras
3. 1 x 3 Cameras
4. 2 x 2 Cameras
5. 2 x 3 Cameras
6. 3 x 3 Cameras
7. 4 x 2 Cameras
8. 4 x 3 Cameras
9. 5 x 3 Cameras
10. 6 x 3 Cameras
11. 6 x 4 Cameras
12. 6 x 5 Cameras
13. 7 x 5 Cameras
14. 8 x 4 Cameras
15. 8 x 5 Cameras
16. 6 x 8 Cameras
17. 1 + 3 Cameras
18. 1 + 5 Cameras

Elevator Control

Quanika software has an elevator module for AXIS Controller which utilize A9188 controller for this purpose. A9188 is a peripheral device which can be configured as a stand-alone module and can be used to function elevator system. Quanika Enterprise supports only two A9188 AXIS controllers together with A1601.

The AERO Controllers A1988, A1610, X1100, EP1501, EP1502, EP4502, LP1501, LP1502 and LP4502 has an elevator module

Elevator configuration consists of three parts:

1. Configuring the access levels of the users.
2. Configuring the access mode of the reader.
3. Configuring the physical nature of the elevator control relays

Access Controllers and Door Controllers

The QAC are integrated to Axis A1001 & A1601, A1610 and A9188 controllers. It communicates with the controllers via standard TCP/IP Ethernet via standard TCP/IP Ethernet. All Access controllers are fully intelligent and distributed processing controllers. The applicable system database and operating parameters are downloaded from the QAC host server to the access controllers and stored locally in its local memory. All access requests from card readers, local linkage parameters, and scheduled functions are processed locally at the access controller with no assistance required from the QAC host server.

If any loss of communication occurs between the System and the Controller, the controller will continue to validate local transaction decisions, and stores all events within its own internal database until communication is restored. Once communication is restored the stored events are uploaded to the database along with actual time stamp of the event occurrence.

The QAC support multiple card technologies, including 125Khz proximity, 13.56Mhz smart card technologies (iClass, Mifare, desfire etc.), Wiegand, magnetic strip, keypads, biometric devices, bar code, QR code. Data interface to the card readers shall support standard Wiegand Data1 / Data0, as well as Clock/Data protocols. It can store 100,000 cardholder and 100,000 Office line events in the local memory of the controller.

All operational parameters for the door controllers and the specific card readers are completely configurable.

QACS is also integrated with Aero controllers X1100, X100, X200, X300 and mercury controllers EP1501, EP1502, EP4502, LP1501, LP1502, LP4502. The components consist of two panel types: the System Control Processor (SCP) panel, also known as the Intelligent Controller, and the Serial Input/Output panels (SIO), also known as the Interface Modules. The SCP receives configuration for operational characteristics, monitors and controls devices connected to control boards based on configuration received from the host system. The SIO(s) are a class of devices that provide a direct interface to external field devices such as sensors and card readers.

Card Readers

Each card reader shall provide for the configuration of the following operational attributes:

1. Hard Anti-passback

2. Soft Anti-passback
3. Area Entering
4. Area Exiting
5. Assign Door Lock Output
6. Assign REX Input
7. Assign Door Sensor Input
8. Card Data Format
9. Pre-alarm Time
10. Fail safe/Fail secure
11. Elevator Reader
12. Door Held Open Delay Time
13. Extended Door Help Open Delay Time (for ADA operation)
14. Keypad Mode (keypad/PIN only, card & keypad/PIN, card or keypad/PIN)
15. Led Drive Mode
16. Lock Door on Close
17. Lock Door on Open
18. Rex Bypass (do not activate door lock on REX)
19. Schedule Door Unlock
20. Schedule Keypad Only Entry
21. Schedule Reader and Keypad Entry
22. Schedule Reader or Keypad Entry
23. Time and Attendance Logging
24. Unlock Time
25. Extended Unlock (for ADA operation)
26. Assign as an enrollment reader

ONVIF Profiles 'A' and 'C' compliance requirement

The growth in interoperability between access control and other devices is key to the end user 'fit for future' philosophy. Access controllers and field devices must be able to function on different software platforms; i.e. the controllers shall not be restricted to one manufacturer software. This is essential to afford end users with choice, both in immediate selection and to ensure the QCS remains fit for purpose over time, as demands and needs change. Access controllers shall demonstrate conformance with ONVIF Profiles A & C.

OSDP compliance

The controllers should be compatible with OSDP (Open Supervised Device Protocol) door readers. The QCS shall also be capable of both 125 KHz and 13.56 MHz Wiegand door reader technology, within a transition path from lower to higher frequency, the timing of which is dictated by the end user.

IP / Networked Controllers

The system shall be an IP based configuration with controllers connected via a dedicated network switch. Only IP controllers which are designed specifically for connection to company or security networks are acceptable.

PoE controller power / lock output

The controllers shall use PoE as the basis for operating power, together with lock output power, managed directly from the controller and configuration menu. Where additional power is required, the bid shall include power enclosures designed as suitable for user lock demand and power/battery back up in the event of a power outage and tested to perform with the nominated QCS controller.

Controller - operational overview

1. The Controllers should be configurable in a 'by the door' design; i.e. capable of location close to doors, thereby reducing the cabling to readers and door furniture (sensors, locks, buttons, etc.). Each controller shall have a housing fit for that purpose, with tamper sensing for cover and base removal. Controllers must offer a scalable growth path to enable the user to decide, on their timescale, if expansion of the system is required. Which is scalable and can be able to be adapted to a variety of applications. Each controller shall have, as standard, its own administration software for single controller installation. Set-up, alarms, events and a full reporting solution for all events and actions are to be included in the admin software.
2. Controllers should be able to operate without need for a permanently connected server or pc, where necessary and preferred. This is useful where a single controller or smaller installation can function without incurring additional costs of servers / pcs. UI software and configuration programs useful for the set up and commissioning / re-programming of controllers and
    a) Enhanced management of rules across several controllers are of course accepted for that
    b) Purpose.
3. Multiple controllers may be connected in a standalone network, to be administered by any pc, without the need for that pc or server to be connected during normal operational mode (out of configuration). Access to the controller(s) is achieved via a web enabled device and the device's IP address.

Door monitoring contacts

Door monitoring contacts shall be installed to each opening leaf of each door to be monitored to check the door status where this is not achievable through an access control lock or where

an access control lock shall not be installed.

Electric locks

All electronically controlled locks to be installed shall meet current building regulations. The type of lock shall take into account the nature, construction and use of the door, the volume of traffic and the level of security required. The Contractor shall confirm in their tender response which locks they propose for each door.

All locks that are fitted shall be of the type that allows monitoring of the lock by the system or a door contact must monitor each door leaf.

Any one and a half and double leaf doors shall have both leaves fitted with a locking device or the contractor shall obtain agreement from the client that the half leaf is to be normally secured shut using alternative mechanical locks.

All locking devices shall have a holding force of at least: 12 kN.

All locking devices shall adhere to the requirements of PAS 24:2012 requirements and will be tested as part of the full door set.

Fail safe/fail secure

All access control doors shall fail safe in the event of a fire alarm. Typically implemented to prevent the device from becoming unresponsive or causing any harm in case of any unexpected error or malfunctions.

Emergency break glass units (BGU)

Green emergency break glass units shall be installed adjacent to each access-controlled door to allow the door to be released in the case of an emergency.

The BGUs

1. Shall either have "EMERGENCY DOOR RELEASE" etched in white or a pictogram of a man exiting.
2. The style shall match that of the red fire BGUs.
3. Shall match the red fire BGUs in molding
4. Shall utilize resettable plastic elements.

Data Exchange Application (DXA)

The DXA is an interface between controller and the Database Server.

1. It has a two-way communication.
2. It keeps the controller up to date with the latest information by fetching updates from database server and at the same time fetching transactional data from controllers and update database server.
3. It monitors and report the real time status of the network devices.

4. It acts as a dashboard running as a Windows Service in the background and is independent from the normal QAC functions.
5. It provides an interface to upgrade the firmware
6. It provides an interface to initialize the controllers.

The DXA display a graphical device tree showing the live status of all devices connected to the QAC.

Schedules

The QCS is capable of creating and storing an unlimited number of schedules for use in the System.
A schedule is defined as specific time interval (start & stop time) on specific days of the week. Multiple time intervals can be applied to the same day of the week. The QCS provides daylight saving setup.
Schedules can be assigned to

1. Door Identification Type
2. Door Unlock
3. Access Levels
4. Outputs

Onetime Events

One-time event option can be used if you want to maintain a schedule for an event which is only going to happen once

1. Each One-time event is definable with a start and end date
   One-time events are stored in the controller and functionality is maintained in the event of disconnection with the Server.

Anti-Passback

The QAC has the ability for card readers to be configured with anti-passback. The QAC allows for hard anti-passback, soft anti-passback and timed anti-passback, on a per card reader basis. The anti-passback function must not be limited to readers connected to the same area controller, or readers connected to the same QAC communication server. A true global anti-passback system must be supported.
The QAC allows the creation of areas, with card readers assigned to specific areas for anti-passback control. The QAC supports an unlimited number of areas.
Each area is assignable with an alphanumeric name of up to 40 characters.
The System allows the card reader configuration of the following anti-passback functions:

1. Hard anti-passback
2. Soft anti-passback
3. Timed anti-passback
4. Global Anti-passback

Hard Anti-passback

When a card is read at a card reader configured with hard anti-passback, and the result is a valid access, the SMS updates the cardholder record with the area that the card reader is defined as "entering". If the cardholder requests access at the same card reader, or a card reader defined as entering the same area, the access request will be denied, and reported by the SMS as an invalid access – anti-passback. This event is reported to the system operator, and logged in the SMS transaction file.

Soft Anti-passback

When a card is read at a card reader configured with Soft anti---passback, and the result is a valid access, the SMS is updated the cardholder record with the area that the card reader is defined as "entering". If the cardholder requests access at the same card reader, or a card reader defined as entering the same area, the access request is granted, however the transaction is reported by the SMS as a valid access with an anti---passback error. This event will be reported to the system operator, and logged in the SMS transaction file.

Timed Anti-passback

Timed anti-passback shall be a function of a defined Area. The Area configuration shall support the configuration of an anti-passback Timer, which is set to a value in minutes from zero to nine hundred ninety-nine (0 to 999). A setting of zero (0) will disable the timed anti-passback function for that area. Any value higher than zero (0) will enable the timed anti-passback function for that area, and will prevent any cardholder using their card again for the duration of the timer setting. Once the time has elapsed the card can be used again at that reader.

Global Anti-passback

An area for which two or more readers are used to access the area, but are physically wired to different controllers. If any reader in that same area receives an ABP Violation, it will prevent that cardholder from entering through other doors in that area.

Area Management

In QCS area refers to group of doors that has restricted access. These areas can be designated based on security levels to define where individuals are allowed or restrict to enter, based on their authorization levels. By assigning different access rights one can easily manage and control the movement of individual within their premises for enhanced security.

Area Configuration for HID and mercury includes the following feature:

1. Mantrap/Airlocking
2. Maximum Occupancy for the number of users to access area
3. Occupancy up
4. Occupancy down

Operator Access and Permissions

The QAC shall support the definition of unlimited number of system operators. Operators shall be defined as administrators or general operators. Administrators shall automatically have access permission to all functions of the QAC software.

Each system operator shall be defined with a unique operator name and password. The operator password shall consist of up to 16 alphanumeric characters. A schedule shall be assigned to each operator to further define the times and days that each operator can have access to the QAC.

Each system operator shall be definable with specific access permissions on a per menu or function basis within the QAC software. Operator permissions can be specified as full permission, read-only, or no permission for each of the specific configuration, monitoring, and command functions, as well as specific reports within report generation.

Defined operators shall have the option for an expiration date, causing that operator to be restricted from QAC access when expired.

Access Levels

The cardholder database shall support the use of access levels for defining what doors/portals the cardholder is authorized to enter. Each access level shall be defined as a list of card reader controlled doors/portals, along with an assigned schedule to designate when the cardholder is authorized to access that door.

Each access level shall be defined with an alphanumeric text name for easy recognition.

The cardholder record shall allow the assignment of multiple access levels to the same cardholder.

Rules Management

The QAC shall support the ability for an event or input to be linked to an event or output. The linked event could cause any of the following linked dependencies

1. Door Momentary
2. Door Unlock
3. Door Lock
4. Door Group Momentary
5. Door Group Unlock
6. Door Group Lock
7. Door Lockdown
8. Door Lockdown Clear
9. Door Group locked down
10. Door Group release
11. Output Momentary
12. Output On
13. Notifications
14. Record Video of 5 seconds for any camera in Q-vision
15. Move Camera to Preset Location
16. Show Live Streaming

17. Take a snapshot from specified camera

The QAC shall allow for the ability to alter event system event messages as either a Global setting or on an individual input.

Cardholders Management

Managing your card holders' data effectively is one of the fundamental tasks you perform in the application. Cardholder management module allows to register a new card holder and manages the existing card holders' data as well. Physical cards are assigned to the users along with their specific details.

Card holders and access levels

1. You can add a new access level by specifying details
2. Existing access levels can be accessed through access level tab in card holder details panel
3. Elevator access levels can be created by adding a name for the access level, schedule and multiple floors for the associated elevator. Existing access levels can also be modified as per the user requirement.

Adding cardholder details

To add a card holder, specify Card number in decimal format, raw card data in lower case hexadecimal, 4-digit pin and a facility code.

Following information is required:

1. Appropriate reader
2. Validity period [specifying the valid from and valid to dates and time]
3. Status

Enable anti pass back override mechanism if required.
Enable ADA for disabled cardholder if required
Enable AD override mechanism if required
Enable Facial enroll card to enroll the cardholder on Safr or Akuvox
Save card info for the specified cardholder

Database Backup Module

Database recovery and backup are help in case of accidental loss of information. Database module is used for backup and restore of the application data.
Backup: You need to specify a destination where you want the backup file to be created.

Report Generation Software Module

The QAC shall include a full featured Report Generation Utility to display or print and create database information Reports.
The Report Utility should contain the following functionality:

1. Parameter select functions
2. Search between two date/time stamps
3. Search on event time
4. Export to Excel (XLSX)
5. Export to PDF (PDF)
6. Export to Word (DOCX)

Custom report designer contains following features:

1. Conditional formatting based on logical operators
2. Aggregate functions for returning the single output
3. Sorting in Results
4. Search between two date/time stamps
5. Export to Excel (XLSX)
6. Export to PDF (PDF)
7. Export to Word (DOCX)

Schedule Report Generation Module

The QAC include a full featured Report Generation Utility based on schedule. With different time ranges scheduler reports will be sent to the assigned operator for the reliable tracking
It should contain the following functionality:

1. Type of schedule with schedule time
2. Selection of report to be send
3. Operator or custom email selection
4. Export to CSV
5. Export to PDF

Multilingual Support

QAC shall support multiple languages. The default language shall be user-definable through the system desktop. The software shall support all the RTL and LTR languages. User shall be able to install the language pack by downloading the sample translation file and uploading it with custom translation.

Partitioning

This feature allows user to divide their access control systems into separate partitions. It is useful for managing different areas, door groups, access level groups, camera server and plan

within a building, allowing for more granular control over who has access to specific partition

Alarm Routing

This feature allows you to handle alarms. It is useful for detecting the alarms coming from different workstations in order to alert the appropriate person, system or resource that the alarm is triggered. The alarm escalation becomes easy like if alarm is not being acknowledged within a certain time frame in such case alarm escalate to another workstation in hierarchy and if it is not getting acknowledge from even the last workstation, the system will send email to the operator for completing the routing interval.

Workstation

This module supports the indication of the connected workstations with the red and green statuses respectively. Connected workstation will be indicated as green status and red status will be for disconnected workstation.

Synchronizer Utility

QAC shall support the process of retrieving the existing configuration / cardholders of Controllers at the time of installation if required. Following configurations can be restored

1. Doors
2. Cardholders
3. Readers Configuration
4. Doors Configuration
5. Access Levels
6. REX Configuration
7. Door Monitors Configuration

Third Party Integration Software (optional)

Event Receiver

QAC shall provide Event Receiver for third party systems.
The received events shall be able to have following.

- Display as events
- Display as alarms
- Integration with Graphical interface
- Enable / Disable

Communication

Event Receiver shall allow to have two types of communication

- Serial
- TCP/IP

Following customizations can be made within the module to extract events

- Event Matches can be defined for multiple type of events.
- Date and Time for Event can be extracted.
- Location of Event can be programmed.
- Event Details can be extracted.

Event Receiver can be used for integrating with external, 3rd Party systems such as fire alarm systems, intrusion detection systems and building management systems

ID Badge Design

QAC shall provide utilities for the design and layout of the ID badge format to be printed on the badge.
The Badge design utility shall allow for single or dual sided badge designs.
Data from the fields of the cardholder record as well images, custom labels, backgrounds shall be available to the part of badge design.
The Badge design shall allow different color backgrounds on the badge. Colors and fonts of text can be customized with this utility.

Badge Printing

QAC shall support the printing of cardholder badges, in conjunction with the photo ID and badge design process.

Badge printers and software shall support single-side or double-side printing. Printing allows of single as well as selected cardholders badges too.

Badging Utility

Badging Utility provides operator to create templates for cardholders with customization facility to design the input form with custom new fields or existing field. User shall be able to place the fields as desired within the grid.
This Utility is useful for segregation, classification of cardholders where additional information is required from cardholders like visitors or contractors.

Data Import /Export

QAC shall provide a data import /export utility that allows users to automatically import data fields from other databases after mapping the columns of both databases. Import / Export utility shall also allow data to be exported data to be delimited files (CSV) or other external database.

Segregate Database Structure

QAC shall support segregate database structure. Databases can be allocated in a distributed

system. Central database synchronization with remote databases. In case of offline environments each remote database can function independently and sync with the central database once network connectivity resumes.

Repository Management

All resources like images, icons and any other format of files can be locally stored and utilized from the local repository. Resources can be removed, added using this Utility.

Database Archiving

This capability will allow for the archiving of data by certain period of time customizable by operator. Database archiving will automatic and will place the data in separate partition and can be accessed specifically if require.

GDPR Support

This feature will support GDPR based on categorization of users. Records for the selected types of cardholders can be deleted after set interval of time automatically through scheduler. Time interval and no of days can be set with this feature.

Grekkom Integration

Quanika Enterprise is integrated with Grekkom Temperature analytics in vision to analyze the temperatures of cardholder.

Site Information Report

All specifications related to access controls can now be viewed through Site Information Report which will give quick information for the site like total doors, total cardholders, total controllers and other related information to site.

Data Exchange Redundancy

This capability will create a backup support for data exchange server with the help of one primary and secondary server. In case of failure of Primary server, Secondary server will be automatically switched and will provide support.

Cardholder Templates

This feature will provide the capability for user to create custom input templates for cardholders. Custom fields can be created for extraction of extra information other than default fields. This feature can be handful for different type of cardholders like contractors and visitors.

Integration with Axis Audio Controllers

The following Axis Audio Controllers can be integrated with Quanika Application.

- C1310-E
- C1004-E
- C1410
- C2005
- C1411

This integration will provide following features.

1. Add Media to Audio Controllers.
2. Media can be played / stopped on Audio Controllers
3. Media can be recorded with Audio Controllers
4. Audio controllers can be mapped on visual plan with Quanika Plan Manager
5. Specific rules on play /stop as trigger point can be applied.

Statistics

This feature will provide the user capability to create custom counters. There are four types of events for which counters can be created for specific doors as listed below.

1. Occupancy
2. Valid Access
3. Denied Access
4. Door Forced

Occupancy Counter shows the number of persons inside specific area with option to set customized time limit.

Mustering Support

Quanika Enterprise provides mustering solutions which mainly works with Areas. It provides an interactive interface for monitoring mustered areas and give useful information to security personnel for quick actions in an emergency situation.

The following features it should have:

1. AREAS should be programmed
2. Printing of mustering report with time ranges
3. Export to PDF with time ranges

AXIS License Plate Verifier Integration

This integration will provide following features

1. Vehicle License plate numbers cane be registered for cardholders.
2. Dedicated Background service to support push event option in AXIS LPN Verifier

application

3. Support for AXIS Cameras P1445-LE-3 & P1377

HTTPS

SSL (HTTPS) protocol for communication with controllers for enhanced security.

Facial Recognition Integration

SAFR

Quanika Access control system provides integration with SAFR (3.5.1.136) facial recognition system

This integration provides following features.

8. Face Registration
9. Access based on valid facial recognition
10. Access level assignment

SIP (Voice over Internet Protocol) Integration

Quanika Access control system provides SIP integration for calling over internet.

This integration provides the following feature:

1. Calling stations can be programmed
2. Door mapping with calling stations
3. Cameras integrated with door to show the view

STID Integration

User can access and manage STid range of access control solutions such as RFID readers and controllers. It allows user to remotely control and monitor access to secure areas in providing flexibility and convenience. From the STid mobile application one can easily manage user permissions and access rights making it simple to update access levels and credentials if needed.

This integration provides following feature:

1. Cardholder Registration on STid via QCS
2. Cardholder enrollment in mobile application

HID Origo Integration

HID Origo simplified the management of access control system and centrally manage the access control devices, credentials, and application as well as streamline the process of issuing and revoking access rights and gain insights into access control activities and enhance security

measures. The mobile app allows users to remotely manage and monitor their access control devices, credentials, and applications from their smartphones or tablets on a single go.
This integration provides the following features:

1. Cardholder registration on HID portal.
2. Cardholder enrollment in mobile application

Active Directory

QCS is also integrated with Active directory to maintain set of services to authenticate and authorize all users and computers in a domain network by automate service and makes the information easy for administrator and users to find and use.
It provides the following features:
Single logon for access to multiple resources
Managing of unlimited Groups.
Managing Active directory users within or outside the Organizational Units.
Excluding the users of specified Organizational units
Assigning Additional Attributes to Cardholders
Deletion Approval of Active Directory users from Quanika Application.

Web Application

Quanika enterprise software now features a website version as well.

Interactive Dashboard

Dashboard contains real time counters, events and alarms.

Cardholders

This feature allows to manage the cardholders that concludes

1. Access levels assignment
2. Card assignment
3. Modification of existing cardholders

Access Levels

This feature allows user to manage access levels, create new access levels and modify existing access levels.

Visual Rule Builder

This interactive feature allows user to create rules / dependencies using simple visual tool.

Report Designer

This web-based features can help create and design multiple reports with tons of features like custom filters, custom design.

ID Badging

This capability allow user to create custom templates for cardholders with custom fields / placeholders like visitors, contractors.

HTTPS & HTTP

Both communication protocols are supported. For HTTPS valid SSL certificate is required.

Physical Access Control System

ONVIF Profiles 'A' and 'C' compliance requirement

The growth in interoperability between access control and other devices is key to the end user 'fit for future' philosophy. Access controllers and field devices must be able to function on different software platforms; i.e. the controllers shall not be restricted to one manufacturer software. This is essential to afford end users with choice, both in immediate selection and to ensure the QAC remains fit for purpose over time, as demands and needs change. Access controllers shall demonstrate conformance with ONVIF Profiles A & C.

OSDP compliance

The controllers should be compatible with OSDP (Open Supervised Device Protocol) door readers. The QAC shall also be capable of both 125 KHz and 13.56 MHz Wiegand door reader technology, within a transition path from lower to higher frequency, the timing of which is dictated by the end user.

IP / Networked Controllers

The system shall be an IP based configuration with controllers connected via a dedicated network switch. Only IP controllers which are designed specifically for connection to company or security networks are acceptable.

PoE controller power / lock output

The controllers shall use PoE as the basis for operating power, together with lock output power, managed directly from the controller and configuration menu. Where additional power is required, the bid shall include power enclosures designed as suitable for user lock demand and power/battery back up in the event of a power outage and tested to perform with the nominated QAC controller.

Controller - operational overview

4. The Controllers should be configurable in a 'by the door' design; i.e. capable of location close to doors, thereby reducing the cabling to readers and door furniture (sensors, locks, buttons, etc.). Each controller shall have a housing fit for that purpose, with tamper sensing for cover and base removal. Controllers must offer a scalable growth path to enable the user to decide, on their timescale, if expansion of the system is required. Which is scalable and can be able to be adapted to a variety of applications. Each controller shall have, as standard, its own administration software for single controller installation. Set-up, alarms, events and a full reporting solution for all events and actions are to be included in the admin software.
5. Controllers should be able to operate without need for a permanently connected server or pc, where necessary and preferred. This is useful where a single controller or smaller installation can function without incurring additional costs of servers / pcs. UI software and configuration programs useful for the set up and commissioning / re-programming of controllers and
    c) Enhanced management of rules across several controllers are of course accepted for that
    d) Purpose.

    Multiple controllers may be connected in a standalone network, to be administered by any pc, without the need for that pc or server to be connected during normal operational mode (out of configuration). Access to the controller(s) is achieved via a web enabled device and the device's IP address.

Door monitoring contacts

Door monitoring contacts shall be installed to each opening leaf of each door to be monitored to check the door status where this is not achievable through an access control lock or where an access control lock shall not be installed.

Electric locks

All electronically controlled locks to be installed shall meet current building regulations. The type of lock shall take into account the nature, construction and use of the door, the volume of traffic and the level of security required. The Contractor shall confirm in their tender response which locks they propose for each door.

All locks that are fitted shall be of the type that allows monitoring of the lock by the system or a door contact must monitor each door leaf.

Any one and a half and double leaf doors shall have both leaves fitted with a locking device or the contractor shall obtain agreement from the client that the half leaf is to be normally secured shut using alternative mechanical locks.

All locking devices shall have a holding force of at least: 12 kN.

All locking devices shall adhere to the requirements of PAS 24:2012 requirements and will be tested as part of the full door set.

Fail safe/fail secure

All access control doors shall fail safe in the event of a fire alarm.

Emergency break glass units (BGU)

Green emergency break glass units shall be installed adjacent to each access-controlled door to allow the door to be released in the case of an emergency.

The BGUs:

Shall either have "EMERGENCY DOOR RELEASE" etched in white or a pictogram of a man exiting.

The style shall match that of the red fire BGUs.

Shall match the red fire BGUs in molding

Shall utilize resettable plastic elements.

General Controller Specification Consideration

1. Safety
2. IEC/EN/UL 62368-1
3. Environment
4. IEC/EN 60529 IP20, UL2043 Plenum rated, NEMA 250 Type 1, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27

Warranty

The controller unit shall be backed by a minimum of three years' manufacturer warranty. The manufacturer shall provide the option of extended warranty for the unit. The optional extended warranty shall be available for a total warranty period of maximum five years.

Sustainability

1. The specified unit shall be manufactured in accordance with the environmental standards as defined in ISO 14001.
2. The specified unit shall be compliant with the EU directives 2011/65/EU (RoHS) and 2012/19/EU (WEEE).
3. The specified unit shall be compliant with the EU regulation 1907/2006 (REACH).
4. The specified unit shall be PVC-free.
5. The manufacturer shall have signed and support the UN Global Compact initiative as defined by United Nations https://www.unglobalcompact.org/
6. The manufacturer and its sustainability strategy and policy, shall be based on the ten principles outlined by UN Global Compact, relating to;" human rights, labor, environment and anticorruption".

Quality Assurance

1. The manufacturer shall go through documented physical testing to ensure the products' complete functionality for the complete specified operative environments in a worst-case scenario.
2. The specified unit shall be manufactured in accordance with ISO9001.