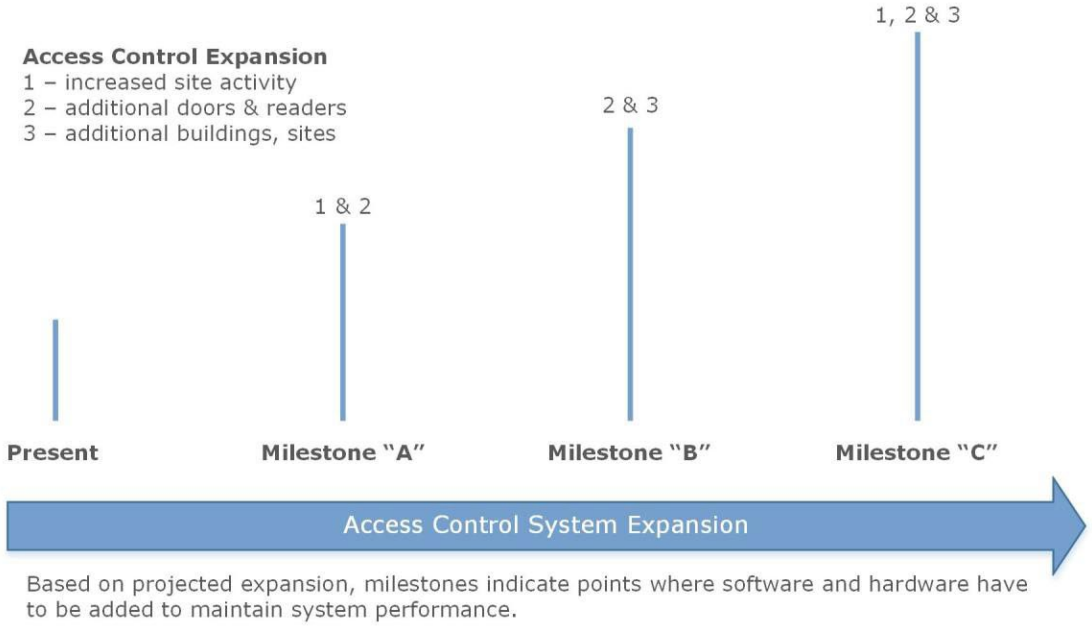
dormakaba

Keyscan Aurora System Architecture

Contents

Purpose

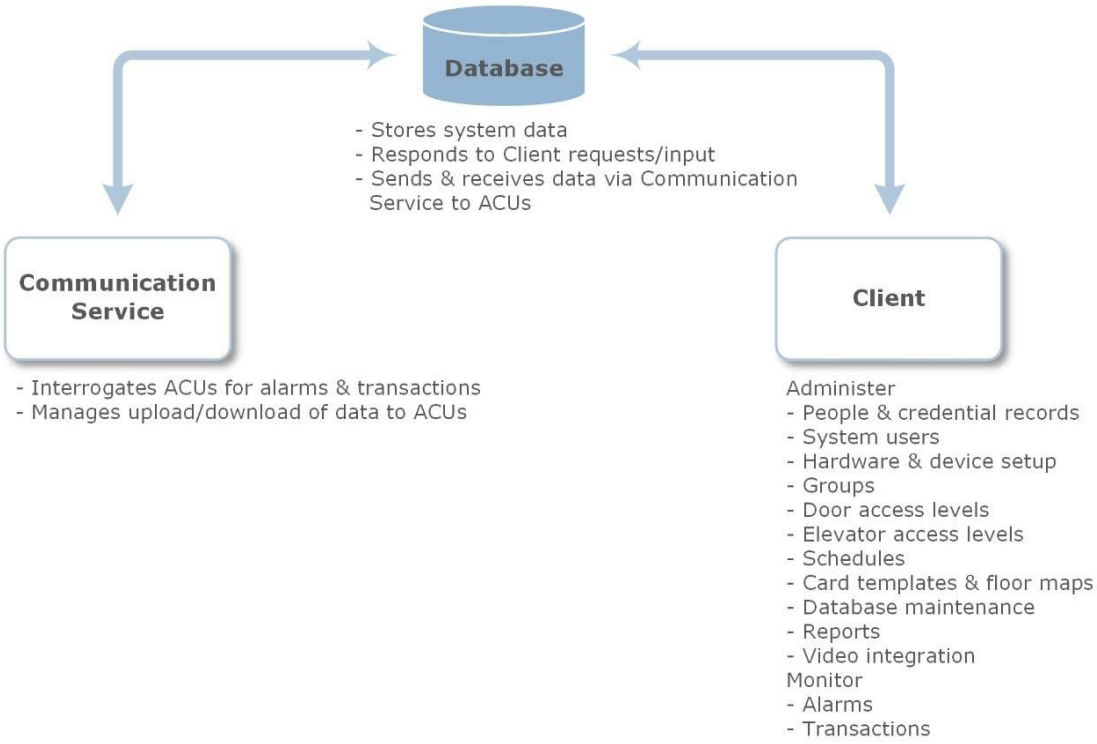
Keyscan access control systems and Aurora software are built on the underlying premise of a flexible and scalable platform accommodating continuous expansion. Systems can be as basic as one computer connected to one access control unit regulating a few doors in a solitary building to highly developed systems consisting of multiple access control units regulating hundreds of doors in numerous buildings located in different geographic regions on a network of servers. In many cases, access control systems are not static entities but are continually evolving and expanding in conjunction with corporate or organizational growth. Hence, this paper provides a template for growing an access control system so that a standardized architecture is consistently maintained for better overall manageability and performance. This paper also reviews Keyscan software modules and their function within the access control system, software/hardware configurations indicating expansion milestones, factors that influence system performance, Keyscan encrypted data transmission format, and database considerations.



Background on Keyscan Software

Keyscan Aurora Access Control Management software has a modular format so that the access control system can be tailored to an infinite variety of configurations – from one computer to multiple servers in multiple locations – and retain the same high-level of operational efficiency with the access control units. The Aurora Access Control Management software consists of the following three primary modules:

- Client software
- Database – SQL Server 2017 Express
- Communication Service



Client

The client module, which is used to administer and monitor the access control system, can be installed on one or multiple servers contingent on the license agreement. The Aurora basic license includes operating two concurrent clients. Additional client licenses can be purchased separately for increasing the number of system user stations on the access control network. Clients can function from either within the same site/building or remote sites/buildings provided they have a connection to the system's database engine.

Communication Service

The communication service directs the system's data flow. It interrogates the access control units for alarms and transactions, and it transmits client workstation user input data and task requests to the access control units. The communication service is not governed by any license restrictions and is configured to run as a Window's service.

dormakaba Canada Inc. also offers a reverse network (RN) communication service designed for centrally managed access control, such that it may be employed with Internet, intranet or WAN connections. Centrally managed access control may also be referred to as “software as a service”. The RN communication service is an optional application and requires the purchase of a license available in one of three formats: one, five or ten network connections.

SQL Server 2017 Express

Keyscan Aurora uses SQL Server 2017 Express as its dedicated database engine for storing all system records. SQL Server 2017 Express has a 10 gigabyte limit and is included in the Aurora basic license.

The database engine can only be installed on one server and all other Keyscan software modules must have a path to the database for the system to function.

Aurora Agent Service

The Aurora Agent Service manages database backups, reports and notifications. The agent must be installed on the same server on which the SQL Server 2017 Express database was installed. The agent operates as a Windows service and must be running to perform its designated tasks.

Aurora Optional Software Modules

dormakaba Canada Inc., in keeping with its modular software concept, offers additional specialized modules for augmenting system functionality. These modules can all be integrated with Aurora to derive additional benefits from the access control system.

Video Management Software Integration

- offers integration with Keyscan-compatible NVR systems

Aurora Web-Client Module

- offers remote access control management from any location that has Internet access

Intrusion Panel Integration

- integrates DSC Power Series and MAXSYS intrusion panels
- monitors and controls the intrusion system from within Aurora's dedicated "status widgets" screens

Active Directory Integration

- uses the domain or local Windows login and password for Aurora software access

Software Development Kit

- allows software developers to write customized applications that interact with a Keyscan access control system
- has a set of exposed software functions to control a range of Aurora's commands and operations

Reverse Network Communication

- designed for managed access control or software as a service application
- uses a corporate intranet or Internet connection between a host and remote locations

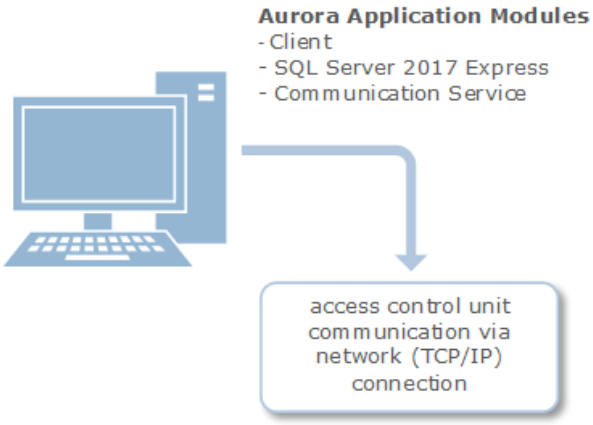
Computer Hardware Configurations

Keyscan Aurora Access Control Management software may be configured for operation on a single computer or on multiple severs offering a flexible and scalable delivery platform using a LAN/WAN (TCP/IP) infrastructure to communicate with the access control units. LAN/WAN communication presents almost limitless possibilities for enterprises to structure the access control system and integrate multiple buildings, local or distant, into one access control entity with central and remote management. The following sections review a rudimentary single computer installation and more evolved multiple server installations.

Single Computer Configuration

All Aurora modules, client, SQL Server 2017 Express, and communication service can be installed on one computer. This type of configuration is better suited to an environment with a low number of access control units/readers, a small credential holder population and a low volume of site transactions. A single computer configuration may be the most cost efficient, as it relates to computer hardware, but it must be weighed against system performance, future system growth, and end-user expectations.

Figure 1 – Single Computer Installation

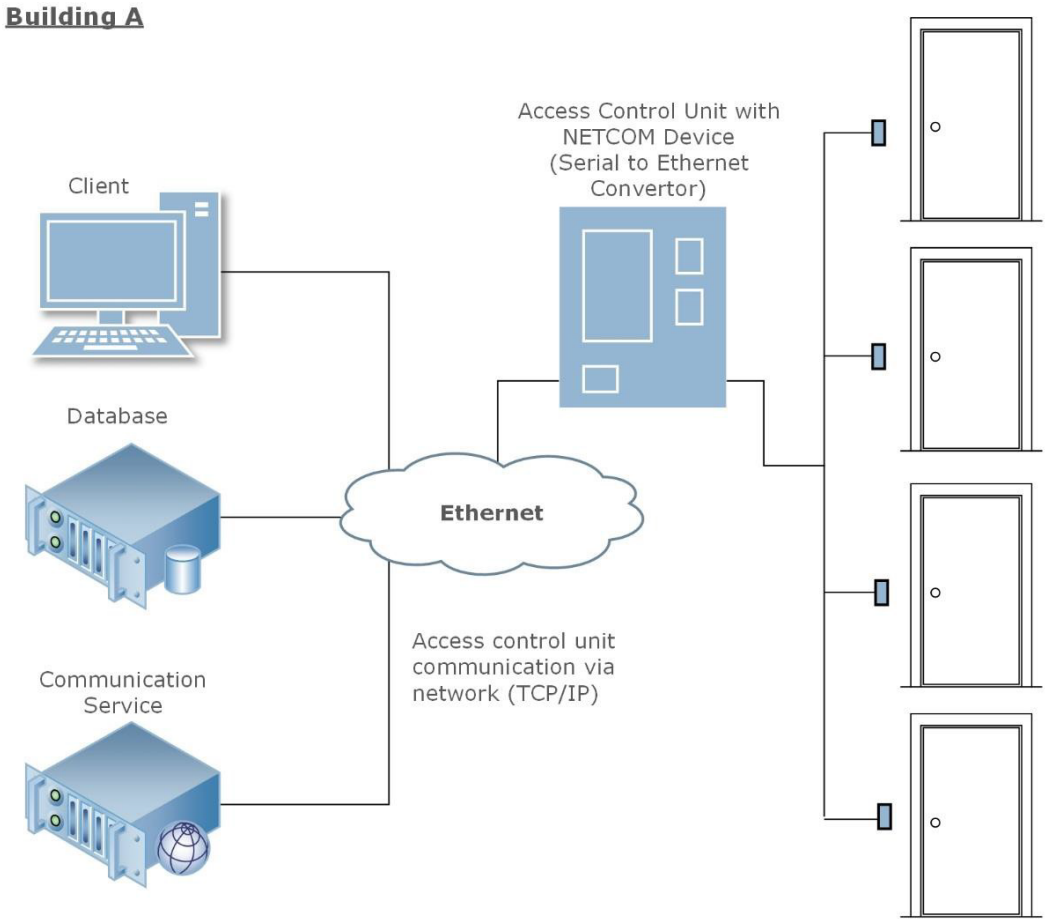


We recommend when the resources of a single computer configuration, if initially used to run all the Aurora modules, no longer meets system performance or customer expectations, the first step would be to transfer the database to a separate server. You may also have to add a server for the communication service.

Multiple Server Configurations

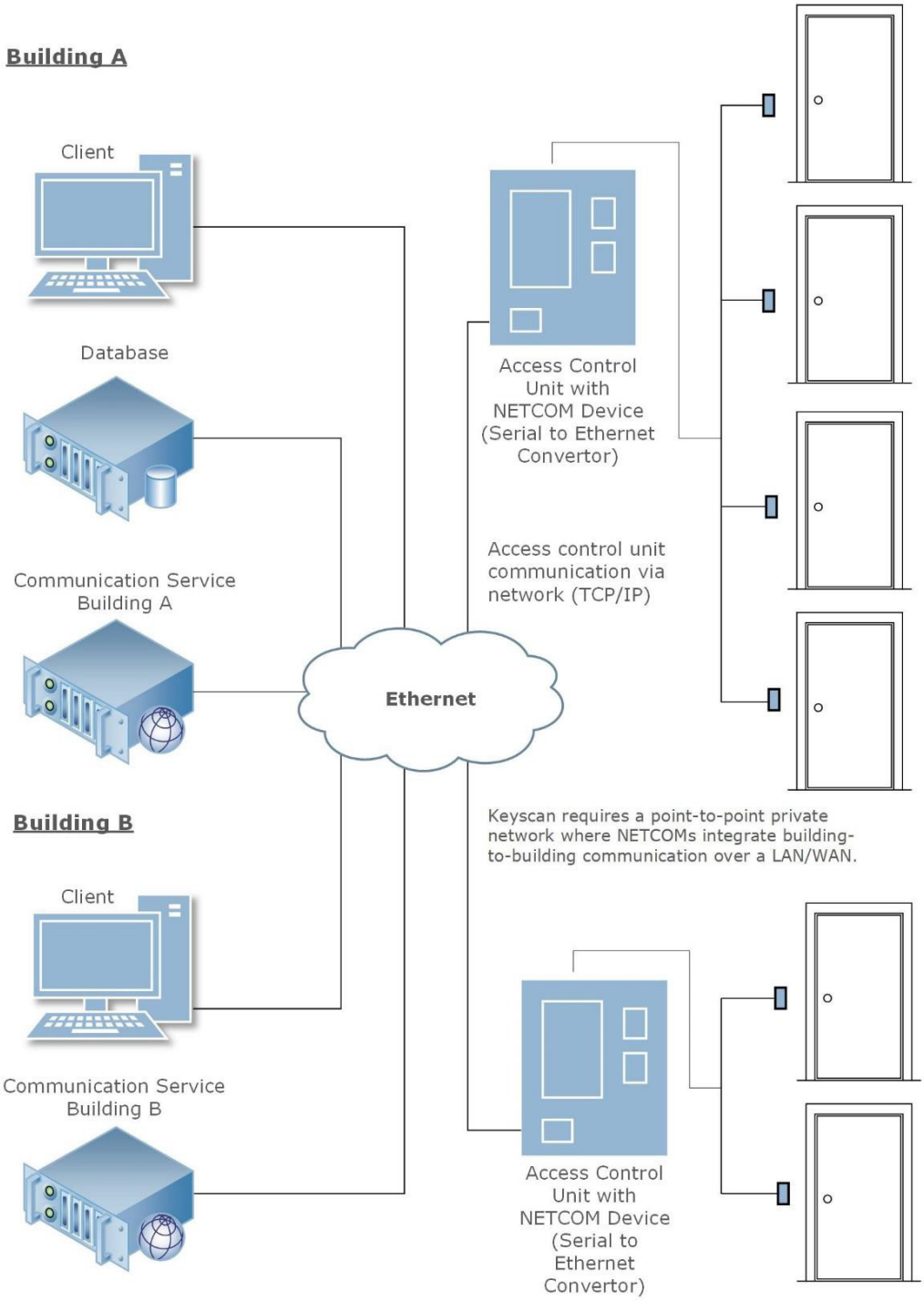
Our recommended configuration is to employ a dedicated workstation for the client, and dedicated servers for the communication service and the SQL Server 2017 Express database engine on a LAN/WAN (TCP/IP). The diagram below shows a basic configuration with dedicated servers and workstation, which in comparison to the single computer setup on the previous page, offers better system performance. Networks are also highly flexible and adaptive to future system expansion.

Figure 2 – Multiple Server Configuration



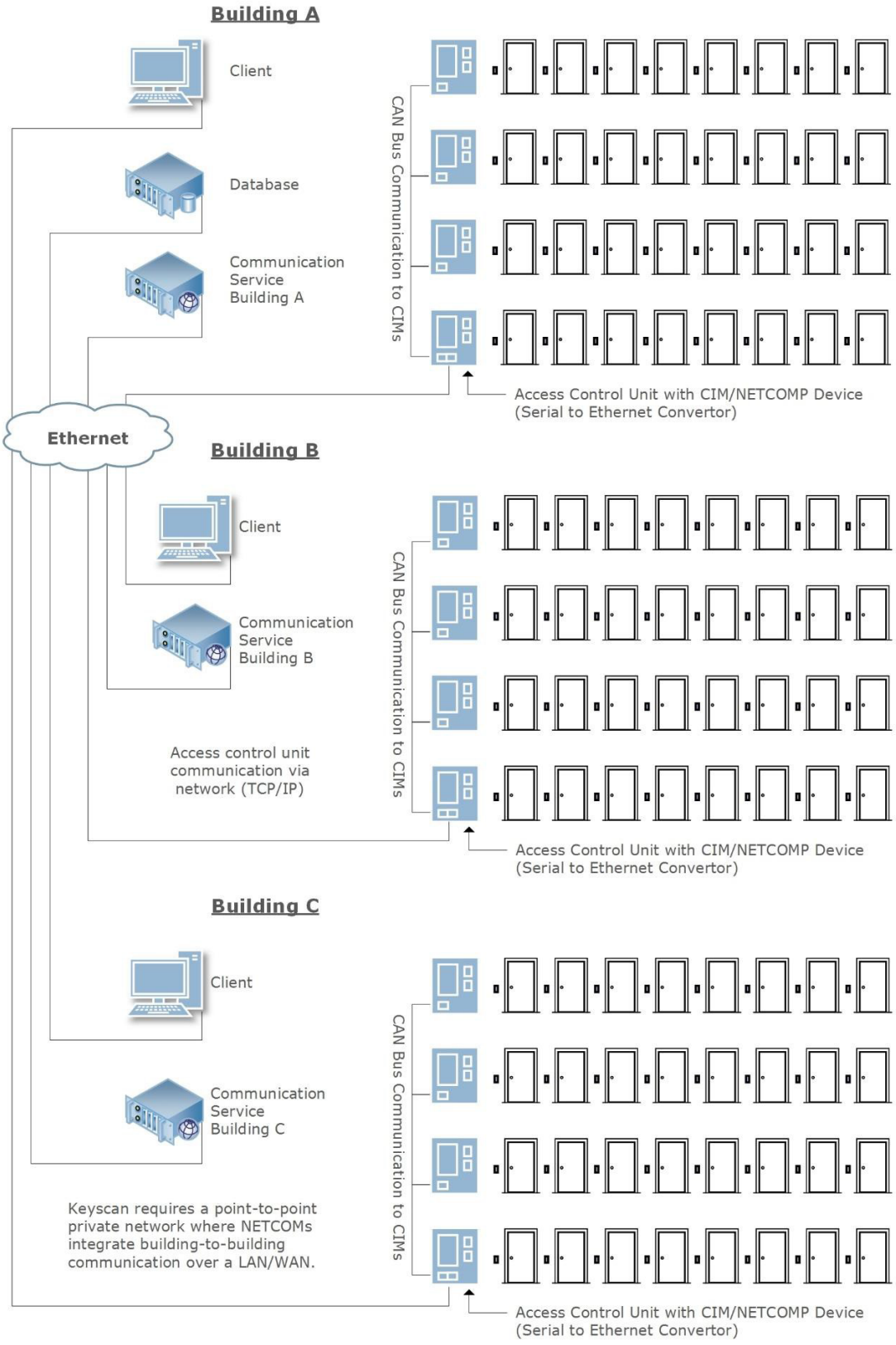
In the following example, the multiple server configuration has been expanded to incorporate another building into the access control system via a LAN/WAN connection. One client workstation has been added for a system administrator in the second building and a server running the communication service. Depending on the authority levels assigned, the administrator could have full to nominal control over one or both sites.

Figure 3 – Multiple Servers with a Second Building Added



In the last example of a multiple server configuration, a third building has been integrated with a communication service running on a dedicated server and a client workstation installed for building oversight. Both are connected on the network with a path to the database in building "A". Also, buildings "A" and "B" have undergone an expansion with more access control units added accommodating more doors and readers and a much larger credential holder population.

Figure 4 – Multiple Servers with a Third Building Added



Data Encryption

dormakaba Canada Inc. employs an AES Rijndael (NIST approved) encryption algorithm for its optional NETCOM6P product.

Encryption converts readable data into scrambled characters. On the other end, decryption converts this back to a readable form. An algorithm performs the encryption and requires a key. The key is a set of numbers that is protected. The key can be 128 bits, 192 bits, or 256 bits to minimize the possibility of an attacker figuring out the key. When both ends have the same encryption algorithm and the same key, secure communication can occur.

dormakaba Canada Inc. employs a Cipher Feedback 128 bit (CFB128) mode for encrypting data on TCP sockets. In this mode, the first TCP packet payload sent must contain the initialization vector. This packet is sent only by the active peer calling connect on the socket. Since this is a connection-oriented protocol, we only need to send encrypted data bytes in successive packets. Also note that dormakaba Canada Inc. employs CFB128 bit mode, which implies the encryption function is only called once every 128 encrypted bits (or 16 bytes).

ACU Interrogation Rates

The communication service issues an interrogation broadcast requesting transactions from all access control units. Using a multi-threaded communication protocol, the communication service interrogates all network connections simultaneously for faster and robust data transfers resulting in more efficient system communication. Factors that affect communication performance are the number of network connections, the number of access control units on each network-connected communication bus, the volume of site transactions, alarm reporting, and front-end activity at the clients such as uploading credential holder information or manual unlocking/locking of doors.

The communication service interrogation rates are listed below to give a time perspective on alarm and activity reporting. Communication rates may vary as they are also affected by the volume of network traffic and connectivity issues.

- LAN/WAN – 12 panels/1 second
- Serial – 12 panels/1 second

Bandwidth

Interrogating one access control unit via a NETCOM2 at the default time of 1000 milliseconds will produce the following network traffic. This does not include any transactions that may be produced by the access control unit during this time.

- Total Sent – 92,815 bytes per hour
- Total Received – 63,800 bytes per hour.

Interrogation and retrieval of transactions from 1 access control unit, with a full transaction buffer via a NETCOM2 at the default polling time of 1000 milliseconds, will produce the following network traffic:

- Total Sent – 218,670 bytes per hour
- Total Received – 1,620,170 bytes per hour

Keyscan latency ceiling is 200 milliseconds maximum, round trip.

Influences on System Performance

System performance is governed by any and all of the following circumstances:

- physical connections within the system – the number of connections and the types of connections influence system performance
- the number of readers and access control units per network connection – the ratio may affect performance and manageability
- end-user expectations – how critical is the timing for reporting alarm events and site transactions

We recognize that system performance is subjective and contingent on what end-users expect from the system and how critical alarm and activity reporting are. Obviously, this can only be determined by the end-user.

Recommended Communication Service to Reader/Access Control Unit Ratio

We recommend the following ratio for best system performance and system manageability:

- 1 communication service/communication server per every 600 readers or 75 access control units (+/- 5 access control units or +/- 20 readers – exceeding this limit may cause degradation to system performance)

This ratio is intended as a general rule of thumb but has been found to be the most optimum configuration.

Communication Service & Communication Servers

Aurora supports running multiple communication services; however, each communication service must be installed on a separate communication server. You cannot install and operate 2 or more Aurora communication services on the same server.

Database Considerations

Aurora currently ships with SQL Server 2017 Express as its dedicated internal database engine. As reviewed earlier SQL Server 2017 Express has a ten gigabyte maximum. To-date dormakaba Canada Inc. has found that with proper database management the ten gigabyte limit has been sufficient to handle even enterprise scale data storage. The following table compares SQL Express and the two variants of SQL 64-bit.

	SQL Server 2017 Express (64-bit)	**SQL Server 2017 – Standard (64-bit)**	**SQL Server 2017 – Enterprise (64-bit)**
Database Limit	10 GB	524PB	524PB
Number of CPUs	Limited to lesser of 1 socket or 4 cores	Limited to lesser of 4 sockets or 16 cores	Limited by OS maximum
RAM	1 GB	64 GB	Limited by OS maximum
Keyscan License	n/a	Requires Aurora SQL license	Requires Aurora SQL license

SQL Server 64-bit License Options

Refer to the Microsoft SQL Server 2017 Licensing Guide available at microsoft.com for more details.

Assessing When to Upgrade to SQL 64-bit

When do you consider purchasing and installing Microsoft SQL Server 64-bit? You should consider purchasing and installing Microsoft SQL Server 64-bit, Standard or Enterprise, when the following conditions are true:

- Retain an amount of active history larger than the limits imposed by SQL 2017 Express of 10GB
- Anticipate active history will exceed 10 million transactions
- Take advantage of the increased RAM capabilities of full SQL Server 64-bit
- Take advantage of the multi-processor capabilities of full SQL Server 64-bit

Required Resources for SQL 64-bit Upgrade

- Must have IT resources on staff or third party contracted IT resources to maintain and manage SQL Server 64-bit and related hardware, software, and backups
- Must purchase and license Microsoft SQL Server 64-bit from an independent reseller
- Must purchase a compatible operating system (Windows Server 2012 64-bit Standard, Windows Server 2012 R2 64-bit Standard, Windows Server 2016 64-bit Standard, Windows Server 2019 Standard 64-bit) and licenses, including Microsoft client licenses
- Must provide hardware to support increased database size and database backups
    - Purchase all necessary hardware
    - Purchase all necessary software for the hardware

- This should include removable media to handle database backups and operating system backups
- This should include off site storage facilities for backups

Recommended Server Specifications

The selection of computer hardware is another critical element that affects system performance. The following outlines Keyscan recommended requirements for maximum system efficiency and performance with the client, communication service, and database installed on separate servers.

Server Specifications

Recommended Minimum Requirements

	Aurora Client Workstation†	Aurora Database Server	Aurora Communication Server	Aurora Web Server
Processor	Intel Core i7 – 4770 3.4 GHz with 4 cores	Intel Xeon E5 – 2420, 1.90GHz, 15MB Cache with 6 cores*	Intel Xeon E5 – 2403, 1.80GHz, 10MB Cache with 4 cores*	Intel Xeon E5 – 2403, 1.80GHz, 10MB Cache with 4 cores*
RAM	16GB RAM 1600MHz DDR3 NON-ECC	16GB RAM 1333MHz, RDIMM	8GB RAM 1333MHz, RDIMM	16GB RAM 1333MHz
Hard Drive	500GB 7.2K RPM SATA	2 x 1TB 7.2K RPM SATA RAID 1 Configuration	500GB 7.2K RPM SATA	500GB 7.2K RPM SATA
Network Adaptor Card	Ethernet Port - 1GB Network Card	Ethernet Port – Dual Port 1GB Network Card	Ethernet Port – Dual Port 1GB Network Card	Ethernet Port – Dual Port 1GB Network Card
Ports	USB 2.0 Ports	USB 2.0 Ports	USB 2.0 Ports	USB 2.0 Ports
Peripherals	AMD RADEON HD 8490 1GB Dual Monitor or AMD RADEON HD8570 1GB Dual Monitor System compatible with 1024x768 or higher resolution— single or dual monitor Keyboard & Mouse	Integrated HD Graphics Card Keyboard & Mouse	Integrated HD Graphics Card Keyboard & Mouse	Integrated HD Graphics Card Keyboard & Mouse
Protective Devices	UPS Backup (recommended)	Dual, Hot-Plug, Redundant Power Supply UPS Backup (recommended)	UPS Backup (recommended)	UPS Backup (recommended)

Operating Systems	Windows Server 2022 Standard 64-bit Windows Server 2019 Standard 64-bit Windows Server 2016 Standard Windows Server 2012 64-bit Datacenter, Standard, Essentials & Foundation Windows Server 2008 R2 64- bit Datacenter, Enterprise, Standard & Foundation Windows 11 Enterprise & Professional 64-bit Windows 10 Professional Windows 8 Professional 64-bit Windows 7 SP1 64-bit Ultimate, Enterprise & Professional	Windows Server 2022 Standard 64-bit Windows Server 2019 Standard 64-bit Windows Server 2019 Standard 64-bit Windows Server 2016 Standard Windows Server 2012 64-bit Datacenter, Standard, Essentials & Foundation Windows Server 2012 R2 64-bit Standard	Windows Server 2022 Standard 64-bit Windows Server 2019 Standard 64-bit Windows Server 2016 Standard Windows Server 2012 64-bit Datacenter, Standard, Essentials & Foundation Windows Server 2008 R2 64-bit Datacenter, Enterprise, Standard & Foundation	Windows Server 2022 Standard 64-bit Windows Server 2019 Standard 64-bit Windows Server 2016 Standard Windows Server 2012 64-bit Windows Server 2008 R2 64-bit Windows 11 Enterprise & Professional 64-bit Windows 10 Professional Windows 8 Professional Windows 7 SP1 Professional, Enterprise and Ultimate

† Aurora Client not recommended for virtualization
* When virtualized, please ensure that you allocate the matching number of cores as shown above

Virtual Machine Server	• Keyscan Aurora supports virtual machine topology, providing that all licensed and required Keyscan software applications are allocated sufficient server resources for proper system performance and that the VM software / server is supported by qualified IT personnel • For best results in virtual machine, dedicate hardware use on the network card and serial or USB port • Virtual machine topology does not always provide optimal system performance

Specifications in this document are subject to change without notice.

Summary

In conclusion, a Keyscan system can be continually expanded to incorporate almost a limitless number of buildings or locations provided the necessary communication infrastructure exists.

dormakaba Canada Inc. strongly advocates the use of the 75 access control units or 600 readers per communication service rule of thumb for maximum system efficiency. This grouping of hardware should be assigned to a single Aurora Communication Server or Servers based on the required hardware groupings. However, it is advised that the Aurora Database Server and the Aurora Communication Server should be on two separate servers. Also, whenever expansion occurs, this standard template provides a model for maintaining a relatively consistent architecture that ultimately leads to better system management and performance.

When assigning a communication service to interrogate designated access control units, consideration should be given to their geographic locations and the expected volume of transactions. Where the access control system is installed in multiple buildings that span different geographic areas, a communication service should be assigned to access control units that are in the same regions or time zones, where possible. Also the distribution of access control units if assigned to multiple communication services should reflect a balanced volume of transactions for better system efficiencies.

The 75 access control units/600 readers guideline is a general rule of thumb, and, in some cases, these limits may have to be stretched because of extenuating circumstances.

dormakaba Canada Inc.
901 Burns St., E.
Whitby, Ontario
Canada L1N0E6
T: 888-539-7226
eadorders.ca@dormakaba.com

www.dormakaba.us