



RBH
ACCESS

Axiom_VTM

Enterprise Security Management System



Building Security Worldwide

Our Corporate Vision

Drawing on decades of experience in the Electronic Access Control industry, RBH's founders insisted

that **Innovation,**
Quality,
Integrity,

and **Value** be the cornerstones of the company and its products – and that the advantages resulting from dedication to these principles flow to its dealers and customers. Meticulous attention to details goes hand in hand with our broad strategic vision.

Since 1995 RBH Access Technology has been known for quality and innovative design.

Product design and manufacturing takes place at our Brampton, Ontario facility in Canada. Sales, distribution and support centers around the world provide services tailored to local customer's needs as we market our products through an international network of security dealers and systems integrators. Selective dealer recruitment and comprehensive training ensures the highest customer satisfaction.

RBH Axiom systems have been installed in over 100 countries, on five continents and in multiple languages. Our company's growth is currently several times the industry average – bearing testimony to the acuity of its vision.

We continue to invest in research and development to provide innovative and effective products that address the ever-growing market demands for open, stable, scalable and integrated security management systems. We will continue to complement our exceptional products with first-rate support and competitive pricing to the ultimate satisfaction of our dealers and their customers.

Enterprise Security Management System

AxiomV™

Complete security management solution

Bringing together different aspects of security management can be challenging. AxiomV stands up to the challenge by combining Access Control and Alarm Monitoring with Video, Building management automation, Asset tracking, Guard tour and Visitor management, and many more important security functions into an elegant and versatile security management solution.

Scalable and extensible system platform

Harnessing the power of the Microsoft SQL Server™ and powerful MS .NET™ framework, AxiomV is positioned on the cutting edge of modern security technology. Adding new applications and solutions is easy due to the flexibility of the underlying software and hardware platform.

Sophisticated and Competitive

Solid architecture and a highly customizable, flexible user interface provides powerful tools for Enterprise Security management. Robust and highly sophisticated hardware implements a variety of flexible solutions at a firmware level. Designed and manufactured "in house", AxiomV offers unmatched longevity and will ensure a long life span for a security investment. AxiomV provides a sophisticated yet affordable solution for systems of all sizes.

Staying future proof, while constantly improving our products is, in our opinion, a true path in satisfying our clients demands without sacrificing our position at the cutting edge of security technology.

Today, our controllers and field panels installed over 15 years ago work with our latest software.

System Architecture

Advanced, Flexible Infrastructure

AxiomV is designed to provide a scalable security management solution that takes advantage of the Microsoft native and well supported technologies for the Windows platform. "NET" framework, fully integrated into Windows 7, Windows 8 and Windows Server family of products allows for secure communications and feature scalability.

Modular Server Components

Individual server components responsible for Client/Server interaction, communications with field hardware, messaging and many others are as native Windows Services that launch automatically and remain operational even if an operator logs off from Windows. All functionality will remain available even in the event of unattended re-boot of a single or multiple host PCs.

Easily Scalable Platform

Free database engine (SQL Express Edition) and a fully featured Microsoft SQL Server allow for a wide range of system sizes, capabilities and configurations. From a single PC, that contains a client and all of the server components, to a widely distributed system with multiple communications servers and various redundancy features AxiomV is infinitely flexible, expandable and easily maintained.



Advanced system architecture allows AxiomV to grow from a small office to an enterprise-wide security management system spanning multiple time zones and languages.

Optimized for system performance

To eliminate common bottlenecks, our engineers had worked with our largest clients to maximize the throughput of our data, messaging and communication server components. Processing a staggering number of events every second, AxiomV delivers a responsive yet comprehensively detailed experience to users and integration partners.

Active Directory Integration

Concurrently multi-lingual UI

On-line, context sensitive help

Intuitive and Powerful User Interface

Interactive Status Display

See live status of all controllers, devices, access points, apartments/suites, alarm points, outputs, etc. From unlocking a door to upgrading firmware on the fly, every control function can be accessed here. Right-click access to live video or last ten recorded events for seamless CCTV integration. Quick reporting and easy access to complete configuration make our interactive status screen an invaluable tool in AxiomV's management. Certain operators can be denied access to this feature, it can also be quickly turned off to make more of the screen's real estate available. In conjunction with the module selector it provides a powerful tool for control of an extremely large system.



Event Viewer

More than just a running list of occurring events, the Event Viewer offers all of the control, CCTV and configuration functionality through a convenient right click. Go right into editing of Cardholder's record by right-clicking on the card number, look at live video or video of an event, grant access on the door in which access was just denied, edit email notifications and re-configure alarm points at the first sign of trouble.

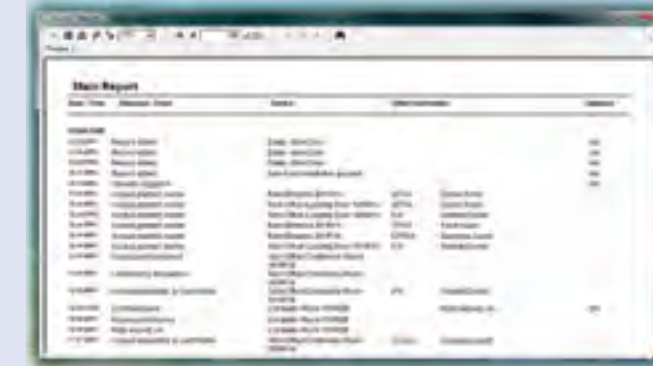
No more looking, writing down and going into other sections of software – direct access to all features is where the convenience and power of AxiomV truly shines.



Reports

Powerful report generating capability is built into AxiomV. Database and history reports allow for thousands of variations, conditions, layouts and sorting. Provided functionality allows printing, export, email of reports, CCTV event playback as well as report export into many popular file formats.

Create and save custom reports, schedule automatic generation of routine reports.



Alarm Monitor - AxiomV allows scheduled designation of any event for persistent display and acknowledgement by the operator. Display priority can be set, event's age and action instructions displayed. Specify a schedule during which a guard would be required to type in or select a pre-programmed comment before clearing the event.

Interactive Mustering - displays the current location of cardholders, area occupancy counts and lists can be easily accessed. Quickly set or reset anti-pass for areas and cardholders. Configure the automatic printing of the **Evacuation Reports**

Access Point Activity

Greeting someone by name or verifying that an authorized person is using a card are just a few aspects of this feature. The video verification screen can be assigned to monitor specific doors and display cardholder's live and on-file picture, basic information and 5 additional fields as access is attempted. Granting Access and locking/unlocking of the displayed door(s) is accomplished through on-screen controls. Quick cardholder lookup simplifies staff training.



Dynamic Interactive Maps

Control all system devices and view live status from a dynamic map with just the click of a mouse. The easy "drag and drop" interface allows you to create your own maps or import bitmaps and AutoCAD drawings. Position and re-size icons for every controller, door, input and output, cameras and shortcuts to other maps. Complete with manual or automatic display on alarm, mapping is enhanced by direct and full access to all control and configuration functionality, integration with live and event video for each device. Display 3rd party alarm zones and other control functionality on our Interactive Map with our PC-100 modules.



Alarm Monitoring

An extremely large number of unique alarm points can be monitored by an AxiomV system. Each point can be fully configured for type of annunciation, priority, customizable action messages, ASCII output, CCTV trigger and executable link. Live graphic maps and color coded alarm handling instructions guide operators in efficient response to each alarm.

Central Station reporting

Via IP or a fully supervised dialer, AxiomV will forward alarm messages to the Central Station in industry standard SIA format.

Accessible from anywhere...

Access to all control and configuration functionality, integration with live and event video is available from Event Viewer, Live Status Display and our Dynamic Interactive Maps on all Client workstations.

Photo ID Badging

Our Photo ID module provides an easy to use and powerful tool for creating high quality, dual sided personalized credentials. Multiple images can be stored for each cardholder. They can be printed on a card along with barcodes, signatures, fingerprints, static text and every data field of Cardholder's record.

Intuitive, built-in card template designer allows for import of images and backgrounds, positioning and custom configuration of cardholder's images, text and data fields. Multiple templates can be created to differentiate employees, departments, etc. Magnetic stripe, Proximity, and Smart Card encoding is available with appropriate hardware. Utilizing standard MS Windows interfaces allows use of any WIA compatible video sources for image capture, Signature capture pads and Card printers from various manufacturers.



- Dual-sided Cards
- Multiple Templates
- USB, WIA-based cameras
- Windows Printer support

Biometric Integration

Multiple brands of biometric readers are transparently integrated with AxiomV. For example: Enroll fingerprints within Cardholder Management screen on any workstation and they will be automatically transmitted to appropriate fingerprint readers: no 3rd party programs, no double data entry.

A variety of biometric technologies are supported: fingerprint, iris, palm etc. Using a combination of TCP/IP and Wiegand connections allows to integrate virtually any upcoming or established biometric technology.



- Fully integrated
- Multiple Technologies
- USB enrollment readers
- TCP/IP and Wiegand

Cardholder Administration

AxiomV's Cardholder database can be setup for a single or multiple credential (car tag, card, fingerprint, etc.) to accommodate different reader technologies and management techniques. Each credential can have a 1 to 5-digit PIN associated with it which can be used independently, in parallel or with a card, depending on access point's configuration.

Variable behavior - Credentials can be designated as Normal, Visitor, Supervisor and Contractor to specify the type of behavior they will exhibit. For example: requiring an escort, overriding anti-passback and a number of other functions.

Status - Flaggering of lost, stolen and suspended cards. Scheduled activation/de-activation - Date and time can be set to activate a card immediately or in the future (pre-mailing, contractor access, etc.). De-activation date and time will de-activate the card even if the PC is down, not communicating with field panels.



Extended Unlock - To comply with ADA requirements, designated handicapped cardholders will enjoy longer unlock times when they use access points controlled by AxiomV.

Access Permissions

A wide selection of methods for flexible assignment of access permissions is available:

A conventional **"Access Level"** designates access to particular doors during particular times and days, and once created can be assigned to large numbers of cardholders. A change in it will affect all cardholders assigned to it.

A flexible way to reduce the number of required "Access Levels" is our **"Special Access"** option allowing you to create a custom list of schedules and doors in addition to or instead of the "base" access level.

"Multiple Access Levels" allow you to "build" a custom set of permissions from modular "access level" components working doors in addition to or instead of the "base" access level for each cardholder.

Card Trace

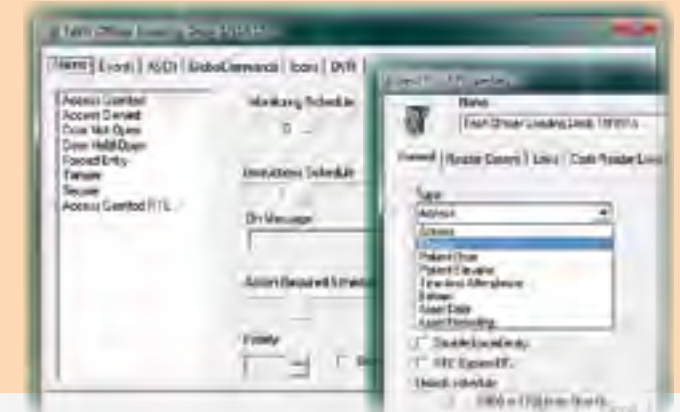
To help organizations deal with suspicious activity, certain cards can be marked for tracing triggering special notifications and automation sequences when used on doors with enabled tracing function.

Additional Features

Limited Use - Individual cards can be assigned a balance of up to 254 uses from which certain doors will deduct uses. As usage balance gets to zero, card will stop working. Certain cards can be exempt from these deductions.

Vacation - To prevent unauthorized use of cards while employee is on vacation without changing their access level, status and other settings, two temporary suspension periods can be configured for each cardholder.

Stealth - Helping Security Managers supervise and audit their staff, AxiomV allows making use of a credential invisible to system operators on a scheduled basis. Stealthy inspection will not be seen on operator's screen but will be recorded in the database for future reporting.



CodeLinks

AxiomV provides an ability to execute an automation sequence when a particular card or PIN is used on a particular reader. This feature serves our customers especially well in situations when a single reader controls a large number of field hardware (locks, alarm zones, etc.). Public storage, manufacturing facilities are just a few of many useful and unique applications of this feature.

Cardholder User Interface Features

Card Management - Card and cardholder data can be easily copied and duplicated streamlining management operations and reducing operator training required.

Search - Cardholders and their card can be easily found via built in quick card number search and powerful "Search" function, allowing use of every field of cardholder's record along with Boolean operators for truly complex searches.

Custom Fields - functionality of the Cardholder Management screen can be further extended by adding additional information tabs with custom database fields and layouts. Text, number, date custom fields will be added to all search functions and report configurations.

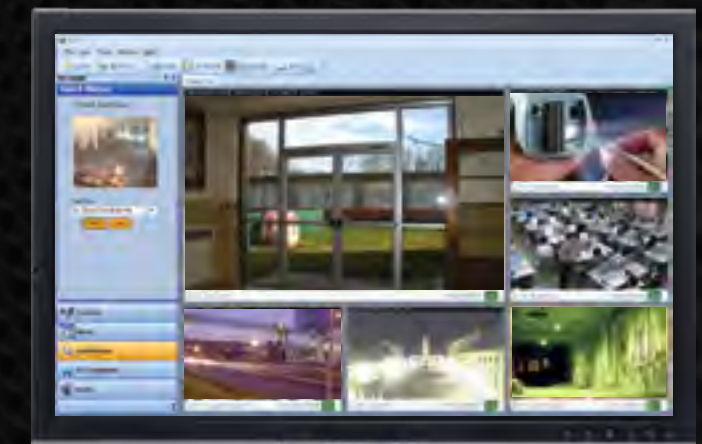
CCTV Module



Capabilities of AxiomV's sophisticated Access Control and Security Management Systems is extended through an open architecture interface with a wide range of Digital Video Recorders (DVRs) and RBH and 3rd party Network Video Recorders (NVRs).

Supporting multiple DVRs from different manufacturers on the same system simultaneously provides enhanced flexibility and freedom of choice of manufacturer.

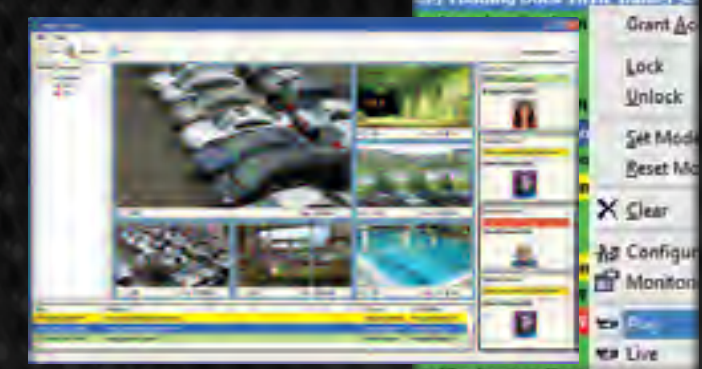
By simplifying video search and allowing Access Point control directly from the live video screen, AxiomV provides a wide range of user -friendly features.



- History event viewing
- Live video on screen
- TCP/IP connections
- Report integration
- Pre, post event viewing
- Supports multiple makes
- Control PTZ on-screen
- Call/Shot assignment

Over the Internet or office LAN, the system user has direct system-wide access to live video, event viewing, historical event based video search, and video export functionality. Custom tailored assignments link individual Access and Monitoring Points to specific cameras across multiple DVRs, providing an ability to set pre- and post-alarm viewing preferences and PTZ shots.

Our system provides direct access to DVR features from the System Status screen, Event Log display, Interactive Maps, and History Report module.



AxiomLinks™

Automation sequences that can change status, settings and values of all control points (readers/doors, inputs, outputs and differential counters) or devices anywhere in the system.

Any system event of any control point can trigger the execution of these links. It can also be scheduled for a specific date-time, daily, weekly or monthly automatic execution with or without Holiday exception.

AxiomLinks can also be executed when a specific card is used on a specific reader or when a designated "Action Code" was entered on a keypad following an "Access Granted" event.

All of the SQL, AxiomV Server and Client components can be installed on the same PC, or span multiple PCs for better scalability and load balancing on the **AxiomV Enterprise Edition**

AxiomV Enterprise Edition can be configured for "Hot Stand-by" with an Automatic "Fail-over"

When Primary Server fails, "Stand-by" server will be activated automatically, providing complete functionality of the failed one

Large Multi-site Systems

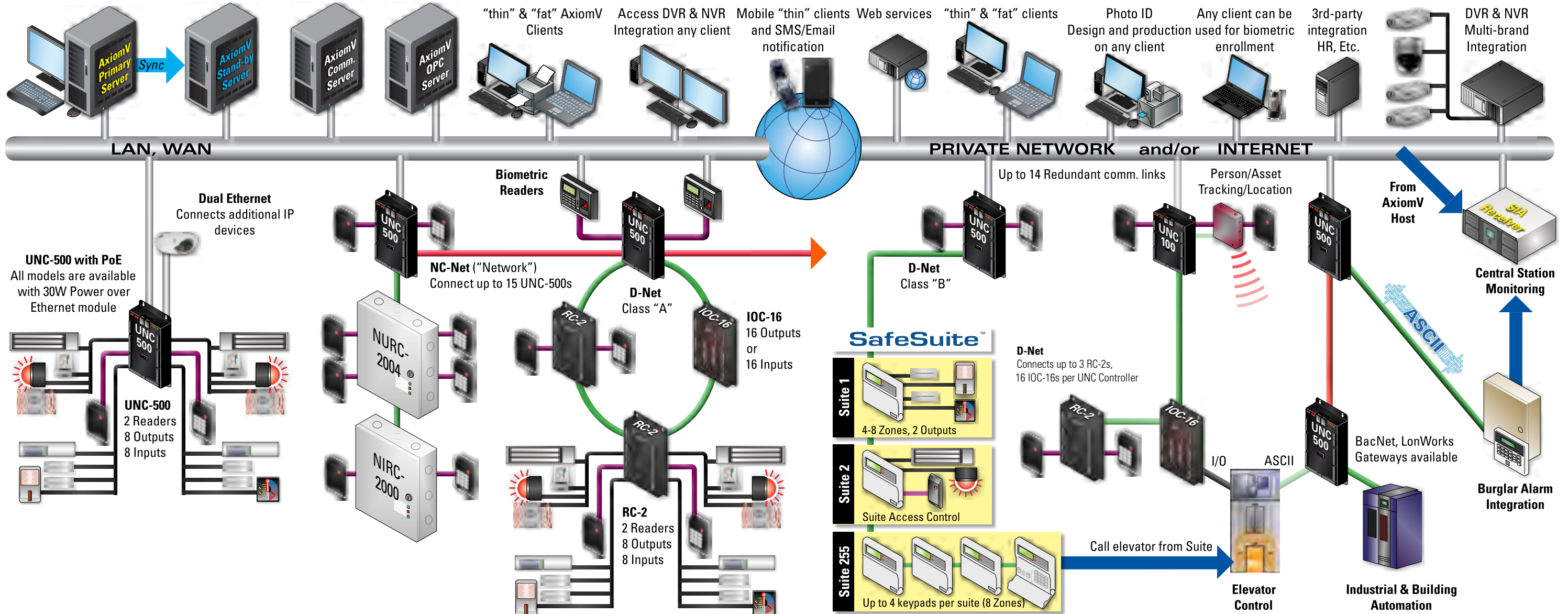
The advanced architecture of the AxiomV allows for multiple hardwired and/or IP Network connections between our Communication Servers and field hardware (NCs, RCs, etc.). Each connection ("Network" as we call it) can include up to 240 Doors ("Access Points" as we call them) and up to 4,800 hard-wired or virtual (see PC-100-3xx) Input/Output points, with all functionality available even when communication with the Server is interrupted.

Time offset on individual sites ("Networks") for geographically distributed systems.

Multi-tenant and Locally Managed Sites

Role based, Operator-centric improvement upon "Database Segregation". Groups and/or Individual AxiomV Operators can be restricted to a part of the wider system. This will preclude them from interfering with or monitoring of the parts of the System outside of their assigned scope. These restrictions get setup on a profile policy basis:

- **Hardware** – permission assignment down to individual doors and alarm points
- **Access Levels** – Access Permission/Schedule, to exclude ones outside of Operators scope
- **Cards and Cardholders** – as assigned to Operator on "Company(s)" designation
- **Control and Reporting** – only for assigned cards, doors and other security hardware



Access Control

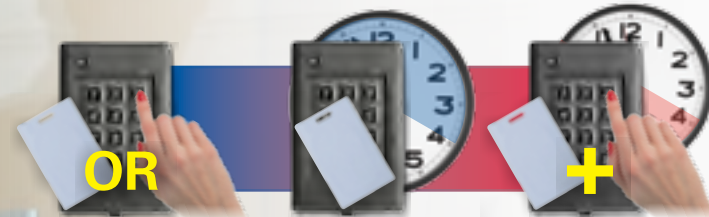


Advanced Access Control Technology

Multiple Reader Technologies - Reader of any technology can be used via our standard Wiegand interface. Proximity (traditional, iClass or MIFARE), Mag-stripe, Bar-code, Biometric to name just a few.

Multiple Card Formats - Up to 5 different card formats can be used simultaneously on the same Access Point (Reader/Door). This feature allows easy site consolidation and smooth transition between new and legacy cards.

Reader/Keypad operation - Card reader and an 8-bit Wiegand keypad (integrated into the reader or installed side-by-side) parallel card or PIN use. Both reader and keypad can be individually enabled by schedule or system command to provide "Card+PIN", "Card Only" or "PIN Only" operation. Unique user defined PINs 1 to 5 digits long are available to each cardholder.



Man-trap, Air-lock, Sally-port - any way you call it, our controller logic can handle them with up to 120 doors each, enabled by schedule or command without any additional wiring or hardware.

Two-stage Door Held Open operation - (programmable warning and alarm) with reader sounder annunciation and external event trigger.

Door unlocking/re-locking - automatic by schedule with "First Person" delay feature, card multi-swipe as well as by an automation or manual command.

Elevator Control

Restricting access to particular floors on schedule, locking down elevators or making them accessible without restriction are part and parcel of our true elevator control. From a reader installed inside of the elevator cab a cardholder can enable all of the buttons to allowed floors, and after floor selection button press to disable activated buttons preventing piggy-back access to other floors. Multiple cardholders can make their selections during the trip.

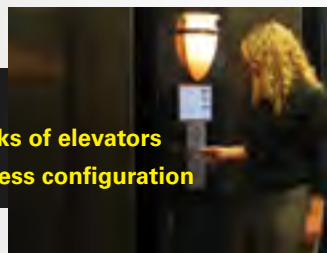
AxiomV can communicate with elevator controller via programmable ASCII or input/output interface. Architecture employed makes it easy to add visitor access functionality to existing systems. Permissions are easily configured in "Access Level" screen.



Visitor Management - quick check-in, check out with many great features

- Issue cards and track their use
- Check-in items and issue receipt
- Create and print Photo IDs

- Up to 256 floors per cab
- Control individual or banks of elevators
- Floor-groups for easy access configuration



Advanced Access Control Features

Multi-swipe Functionality - Control your access points without access to AxiomV software. Particular cardholders can be authorized on door-per-door basis to be able to Lock or Unlock doors with a **double swipe** of a card (fingerprint or PIN use). **Four-swipe** will allow turning on and off of the High Security Mode.

2-Swipe Locks/Unlocks Door

4-Swipe Door's Hi-Security On/Off



Two-man rule enabled on schedule for each door, or cardholder based "Visitor-Supervisor" or "Escort required" linking.

Anti-Passback functionality provides controlled sequence of card use with a fully featured multi-area layout, anti-tailgating, schedule enabled "Hard Enforcement" and area status reset. Anti-passback can operate locally, without a PC within a network of 120-240 doors, or Globally, system-wide with information routing through the PC. Door opening can be configured to trigger card's current area change. Live area status monitoring and timed anti-passback features are provided.

Man-trap, Air-lock, Sally-port - any way you call it, our controller logic can handle them with up to 120 doors each, enabled by schedule or command without any additional wiring or hardware.

CodeTracing - When you cannot restrict access, but need to take measures when a marked cardholders pass through designated doors, variety of functions can be triggered to record or prevent pilfering or to activate specialized automation sequences.

High Security Mode can interactively elevate access privilege requirement: an additional privilege designation on top of the assigned access levels. This mode can be enabled and disabled on schedule, by an automation link, card multi-swipe or manual command.



- Multi-level threat response
- Automatic or manual activation
- Easy to configure

Auto Void - Dealing with a large, and especially high-turnover workforce can be challenging. AxiomV is capable of automatically disabling cards not used in a specified number of days. There is an ability to except certain cards from being affected by this feature: so your outside sales force would be able to use their cards regardless of how often they visit the office.

Much, much more - There are many more aspects of the Access Control operation that can be automatically or manually triggered or adjusted to ensure that doors operate exactly as customers require.

Additional Features

Automated Card Import - Configuration wizard makes it easy to configure an automatic on-going synchronization with third party personnel, resident and other management systems. Cardholders and cards can be added, updated and deleted automatically. SQL Server, MS Access databases, text files can be accessed on scheduled basis, contained changes implemented and downloaded to field controllers immediately. Source text files can be automatically deleted upon successful import.

Universal Copy Wizard - Programming and re-configuring hundreds or thousands of doors, tens of thousands of inputs and outputs, hundreds of thousands of cardholders does not have to be a tedious process. Our Universal Copy Wizard makes it possible to copy selected fields from a source record to especially selected destination records for every type data and many other configuration settings available in the system.

- Intuitive Access Levels with Elevator permissions
- Cardholder Reader Access for effective "task team" access permissions in addition to Access Levels
- Areas for mustering and anti-passback with triggered muster report printout and scheduled clearing.
- Intuitive hardware configuration tree
- Device groups for multiple item control
- Holidays - multiple days, two types
- Flexible sixteen period Schedules
- Adjustable toolbars and user interface



Automatic Backup - Keeping data safe will ensure painless recovery in case of hardware failure and other oops moments. Our integrated wizard will help you to specify where you would like to store your backup (local or removable drive, network volume, etc.), what data and when it is backed up. Multiple copies of backup can be kept, with oldest versions automatically deleted to preserve space. Backup can also be triggered manually to make a system snapshot before any major changes are implemented.

Message ports - Custom configured ASCII messages including static text and event data can be transmitted via serial, TCP/IP and email messaging ports. Every event of every hardware point and additional trigger events can initiate transmission through an appropriate port on a scheduled basis: during the day data may be sent to email, while after hours to a mobile phone. This feature makes it possible to integrate with virtually any piece of software and hardware capable of ASCII or email communication

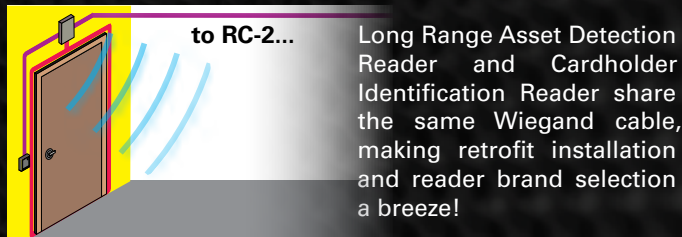


Asset Tracking



To prevent theft of your organization's assets or to keep track of their current location, our Integrated Asset Tracking system is designed to help stop persons leaving with valuables they are not authorized to remove from the premises or move them to another part of your facility. AxiomV will link individual assets with their owners and with pictures of both the protected valuables and their assigned owners.

Asset Tracking system operates by detecting the tag attached to an asset and requiring the use of a card or another security credential to authorize the removal of this item from the premises. If owner and asset do not match, system can notify authorities of an attempted action and if needed to lock down doors to prevent an unauthorized asset movement.



- Real-time operation, works with PC down
- Live location status, owner and asset image display
- Easy to retrofit - multiple reader brands supported

Asset Tracking function can be easily added to any access point controlled by the AxiomV Security Management System without the need for an additional panels and controllers. Full video integration is available for an additional visual verification as well as to easily assessable record of the events.

Asset/Person Location

Easily locate and track movement of mobile assets or persons within the facility without door control stations

- Interactive location screen with signal indicator
- Roaming asset tracking capability
- Email notification and other integration features

Interactive Guard Tour

In a small or a large facility there is no substitute for personal inspection of the access points and secured areas. To verify a door's operation, presence of people in the area, or various other issues that can be out of normal order, a patrolling security officer is needed to make sure that these inspections are performed on time and in proper order.



- Real-time operation
- Live progress display
- Uses existing readers at access points
- Start tours manually or by schedules

Access Points can be arranged in a sequence to be visited by a security guard. This GuardTour can be started manually or automatically on a schedule and will specify the times at which points on this tour must be visited.

As with all things in real life there are reasonable delays, and our programmable Grace Periods were designed to account for them. However if a guard was late beyond reason or had arrived too early, possibly taking a shortcut deviating from prescribed route, an alarm will be displayed and recorded.

For example "Routine Tour" will start at 10 PM at the Security Office, the guard must make it to the Main Door 10 minutes into the tour, Rear Door in 25, Loading Dock in 40 and so on.

AxiomLinks™ Integration - Programmable automation sequences and commands can be automatically executed when the guard arrives to a station early, late or on-time.

Guard Tour Status Screen - Displays if the tour has started, and if so when, as well as which guard has reached which access points and when.

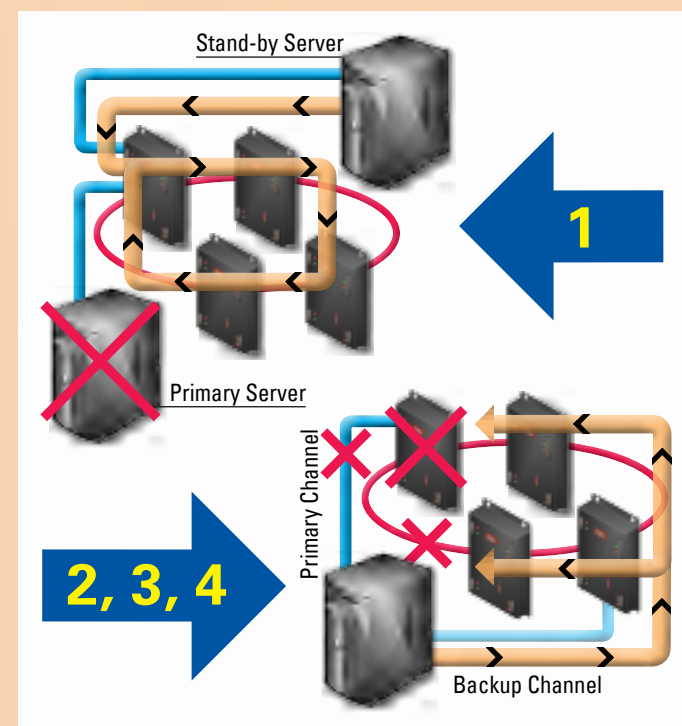
CCTV Integration - Live video from a camera associated with an access point can be displayed when a guard reaches it while the tour is in progress. This allows for visual verification and recording.

Guard Groups - For added flexibility, multiple guards can be assigned to a Guard Group to conduct tours together or separately. Any guard belonging to this group can advance the tour by presenting their ID.

High Availability

High Availability Communications via 4 layers of redundancy, is available in the Enterprise Edition of the AxiomV™ Security Management System

- Multi-Channel Connectivity, Threat Aware Hardware
- Distributive Processing, Redundant wiring
- Synchronized Hot Stand-By with automatic Fail Over



AxiomV™ Enterprise Edition is built on multi-server architecture, where discreet servers are implemented across the corporate network with "Hot stand-by" and automatic "Fail-over" features. In case of one of the communication and/or data servers going off line, there is a fully synchronized, up-to date stand-by server ready to take over.

Each Communications Server handles multiple networks of UNC controllers via a wide variety of communication technologies. Each one of those NC networks can have multiple connections to a Comm. Server. Our unique architecture allows these backup channels to connect to both "Master" and "Slave" NCs constituting a network. This way, not only the loss of a communication channel is sustainable, but also a failure of one or more of the Network Controllers. "Slave" controller will assume the role of a "Master" as the backup communications channel activates.

D-NET connects devices such as RC-2 Reader Controllers IOC-16 Input/Output controllers to the UNC controller. 38.4 Kbps, RS-485 circuit runs on a "Class A" bi-directional communication loop of twisted, shielded copper pair. UNC controller, 4-8 of the RC-2s and 16 IOC-16 controllers act as boosters and repeaters, combining the 3,000' distances between individual devices into a 15,000' loop. Due to it's bi-directional nature, D-NET can sustain cable sabotage and a failure of a device.

C-NET connects up to 15 UNC controllers to each other creating a network of NCs. 2.5 Mbps, ARCNET packet based, supervised and self-adjustable C-NET runs on a "Class A" bi-directional communication loop of twisted, shielded copper pair. Each UNC controller acts as a booster and a repeater, combining 2,000' distances between individual NCs into a 12,000' loop. Due to it's bi-directional nature, C-NET can sustain a C-NET cable sabotage and a failure of a UNC controller.

SafeSuite™

AxiomV's Complete Security System for Condominium and Hotel Suites

Elegant keypads serve as a burglar alarm and access control system, message center and building automation gateway. Operated locally, monitored and controlled from a management office SafeSuite takes advantage of AxiomV's existing infrastructure to deliver a cost effective and user friendly solution for integrated residential security.

Complete audit logs and live status display provide dynamic and secure platform for hotel operation and property management companies, while enriching guest's and resident's experience.



- Options:
- Individual suite offsite monitoring, Revenue generation
 - Suite notification of family members entering the building via parking or entrance door
 - Wireless (pet motion detectors etc.)

Readers Supported	1 (any technology, Wiegand interface)
Programmable Inputs	4 (8 per Suite); 8 - Special order LED keypad
Programmable Outputs	2 (voltage outputs, 8 optional)
Communications	RS-485; TCP/IP, 38.4 Kb/s, Supervised; 255 Suites/UNC
Power	50 mA (200 mA max) @ 12 VDC
Dimensions	6.625"W x 4.5"H x 1.25"D (15.9 x 11.4 x 3.2 cm)

AxiomV™ Hardware

Our controllers and devices share a common design approach in being **Flexible, Flash upgradable, providing Visual diagnostic LEDs, and Removable connectors, packaged into a rugged case.**

UNC-100 Network Controller

The RBH-UNC-100 series is a welcome addition to the new generation of powerful and reliable AxiomV hardware. The single door native TCP/IP controller comes equipped with onboard battery backup charger and accommodates up to 16 individual IOC-16 input/output controllers or 254-SafeSuite keypads. The unit is expandable to 7 doors using 3 additional RC-2 or NIRC/NURC controllers. The UNC-100 also features a 32-bit processor with encryption and expanded memory. The UNC-100-132 model comes equipped with IEEE 802.3at compliant PoE capability, further increasing the UNC series' award winning efficiency.



RBH-UNC-100-xx2

UNC-500 Network Controller



RBH-UNC-500-xx2
UNC-500 Controller in a Metal shell



RBH-UNC-RACK-01
Rack mount enclosure fits up to 2 UNC-500-xx5 controllers

Next generation 32-bit processor with hardware encryption and expanded memory, drastically increases the system capacity in doors, cards and history event log while opening exciting opportunities of new functionality.

Certain UNC-500 controller models come equipped with PoE capability. Augmented with onboard battery backup with the ability to bolster power output when necessary.

19" rack mount for IT style configurations or wall mount for more traditional installations, UNC-500 delivers a lot of features in an attractive package. Wall mount unit fits into existing enclosures and if ordered with metal protective shell can be mounted directly on back boards or inside of 3rd party cabinets. Compact rack mount foot print efficiently utilizes rack space to provide 2 or 4-door packages in a slim and functional design.

1U rack mount enclosures come with a variety of available trim options: easy wiring with modular connectors on the back or 1/2-3/4" knockouts for secure cable management. Fixed mount or pull out rails make this a versatile solution for a number of requirements.

RC-2 2-Door Reader Controller



RC-2 is designed to provide reader, input and output connections for two Access Points (Doors), controlled by a UNC controller via secure and redundant D-Net link.

The RC-2 is one of the most rugged and reliable reader controllers on the market, with a multitude of built-in features found only in high-end custom designed systems.

Variety of reader technologies supported via Wiegand interface (MIFARE, iClass, RFID, Barcode, Mag Stripe, Fingerprint, Iris, Etc.)

Concurrent support of up to 5 card formats per reader with 5-12 digit card numbers, multiple supervised power supplies, programmable I/O and full set of other features make RC-2 stand out in today's crowded marketplace.

IOC-16 Input Output Controller



IOC-16 is designed to provide a large number of inputs and outputs for monitoring and control by UNC controllers, up to 16 IOCs can be connected to each NC.

Flexible design allows installer to select between fully programmable supervised input or programmable Form C dry relay output for each of 16 available points.

Perfect for Elevator control, monitoring large number of inputs and controlling outputs especially with our "Virtual Door" logic, while providing lightning-fast response.

Readers Supported	2 with up to 5 concurrent card formats each	None
Audio/Visual Controls	Red and Green reader LED, audible controls	
Reader Supervision	On-board reader tamper monitoring	
Cable Requirement	Shielded, stranded 6 or 8 conductor, 20 - 22 AWG; Max 500 ft (150 m) @ 20 AWG)	
Programmable Inputs	8 - with status LEDs	Up to 16 (field selectable) with status LED
Circuit Types	N.O. or N.C with no supervision, single EOL or dual EOL supervision (1K EOL)	
Dedicated Inputs	1 - Fire Alarm input with Status LED; 1 - Cabinet Temper Input	
Cable Requirement	2 conductor, 20-22 AWG; Max 1000 ft (300 m)	
Programmable Outputs	8 (4 relays + 4 voltage outputs) with status LEDs	Up to 16 relays (field selectable) with status LEDs
Relays	Form C relays, SPDT, 2 A @ 30 VDC, dry contacts; Fail Safe/Secure programmable	
Voltage outputs	Open collector electronic drivers, (12 VDC @ 100 mA MAX)	
Communications	D-NET (Bi-Directional; Class A; RS-485; 38,4 Kb/s)	
Circuit Type	Ring (short or open circuit protection), 2 x D-Net ports / Panel (fully supervised) with status LEDs	
Cable Requirement	Shielded, twisted pair, 20 - 22 AWG; 3,000 ft (900 m) between devices, 15,000 ft (4,550 m) total	
Power : Current Draw	400 mA max (controller)	500 mA max (controller with all relays energized)
Reader Power Output	1 A @ 5 or 12 VDC Fused; Supervised with LED	None
Auxiliary Power Output	1 A @ 12 VDC; Fused; Digitally Supervised with LED status indicator	
AC Power Requirements	16.5 VAC 40VA transformer; 3A Fused with Low/High Status LEDs; Run LED	
Battery Charging Circuit	13.8 VDC; 3A Fused with Status LED; Digital dynamic load test; Deep discharge protection	
Back-up Battery	12 VDC, 7 AH lead acid or gel cell rechargeable battery	
Lock Power Circuit	RC-2 Only: Input 16-18 VAC 40-80VA transformer; Output 12-24 VDC, 3A Fused with Status LED	
Dimensions	9.75" H x 6.875" W x 3.25" D (25 x 18 x 10 cm)	
Operating environment	Temperature: 0 to 70°C (35 - 150°F); Humidity: 20 to 80% RH (non-condensing)	

Processor / Memory	32-bit Processor / 2MB	32-bit Processor / 2MB. 4MB up to 8 MB
Memory Capacity: Cards	50,000	50,000 - 300,000 (Dependent on model)
Event Log	30,000	30,000 - 100,000 (Dependent on model)
Communications	Built in TCP/IP, RS-485	
Ports / Circuit Type	1 RS-485 programmable (Supports OSDP, Etc.)	1 or 3 (Dependent on model) RS-485 programmable (Supports OSDP, Wireless Locks, Etc.)
Cable Requirement	Shielded, twisted pair, 20 - 22 AWG; 4,000 ft (1,200 m) total	
Doors / I/O / Other	7 (1-onboard) / 308 (4 onboard) / 254 SafeSuite KPs	8 (2-onboard) / 320 (16 onboard) / 254 SafeSuite KPs
On board Reader Ports	2 Wiegand ports with up to 5 concurrent card formats* (UNC-100 is Single door read IN & read OUT only)	
Audio/Visual Controls	Red and Green reader LED, audible controls	
Cable Requirement	Shielded, stranded, 6 or 8 conductor, 20 - 22 AWG; Max 500 ft (150 m) @ 20 AWG)	
Programmable Inputs	4 + Cabinet Temper Input	8 + Cabinet Temper Input
Circuit Types	Four State Monitoring	
Programmable Outputs	4 (2 relays + 2 open collector outputs 100mA)	8 (4 relays + 4 open collector outputs 100mA)
Relays	Form C relays, SPDT, 5 A @30 VDC, dry contacts; Fail Safe/Secure programmable	
Power : Current Draw	1.5 A @ 12VDC (backup battery charger requires 13.8 - 15VDC)	
Circuit Protection	Thermal - Power In, Power Out, Reader Power	
PoE (optional)	IEEE 802.3at compliant : 25.5W; Other : 30W	
Auxiliary Voltage Outputs	12-14 VDC @ 500 mA	
Dimensions	PCB 6" H x 5.3" W x 1.5" D Shell 7.75" H x 5.5" W x 1.5" D	PCB 8" H x 5.3" W x 1.5" D Shell 9.75" H x 5.5" W x 1.5" D Rack 1.75" H x 19" W x 15" D
Operating environment	Temperature: 0 to 70°C (32 - 158°F); Humidity: 20 to 85% RH (non-condensing)	



Listings/certifications are product specific

Our dedication to quality and innovation clearly shows in our innovative and reliable hardware products.

In combination with AxiomV's universal, field configurable **software ASCII interface and OPC Server**, our award winning **PC-100 Hardware ASCII Gateway** makes our product offering even more relevant in the building management, security and industrial control markets.



Interfacing with a wide variety of 3rd party building management, security and industrial control equipment can be challenging and costly. Our PC-100 hardware ASCII gateway is designed make this integration much easier and less expensive than conventional input/output means.

PC-100 Universal ASCII Gateway

Axiom V™ Edition Comparison

Edition	PROFESSIONAL EDITION	ENTERPRISE EDITION
Data Storage	MS SQL Express Edition 2008	MS SQL Server 2005, 2008
Automated SQL Server Installation	Yes	No
Access Points Supported	256	512, 1024, 2048 ... Unlimited
Networks per Comm. Server	49	256
Clients (Included)	5 (5)	Unlimited* (10)
Server components on multiple PCs	No	Yes
Dynamic Mapping	Yes	Yes
Hot Stand-by	No	Yes*
Automatic "Fail-over"	No	Yes*
Load Management	No	Yes*
Active Directory Interface	No	Yes*
O.P.C. interface	No	Yes*
High Availability communications	Yes*	Yes*
Data Import/ Export Wizard	Yes*	Yes*
Interactive Guard Tour	Yes*	Yes*
Asset Management	Yes*	Yes*
Asset Tracking	Yes*	Yes*
Asset/Person Location	Yes*	Yes*
Badging PhotoID and Design	Yes*	Yes*
OSDP Support	Yes*	Yes*
VMS / DVR / NVR Integration Module	Yes*	Yes*
Custom Report Designer	No	Yes*
Automatic Report Generation	Yes*	Yes*
Visitor Management	Yes*	Yes*
Integrated Biometric Fingerprint Enrollment	Yes*	Yes*
Integrated Biometric Iris Enrollment	Yes*	Yes*
Integrated Biometric Palm Enrollment	Yes*	Yes*
Palm Scanner Integration	Yes*	Yes*
Wireless Lockset Integration	Yes*	Yes*

* Available Option

The advertisement features a central graphic with the text "Axiom V™ Reader Technologies" in a large, stylized font. Surrounding this central text are several images of access control devices, including keypad readers, proximity readers, and biometric scanners. The logos for "HID iCLASS", "MIFARE", "LEGIC", "AWID", and "PROXIMITY" are displayed around the central text. At the bottom right, the "RBH ACCESS" logo is shown, which consists of a globe icon and the text "RBH ACCESS".

www.RBH-Access.com