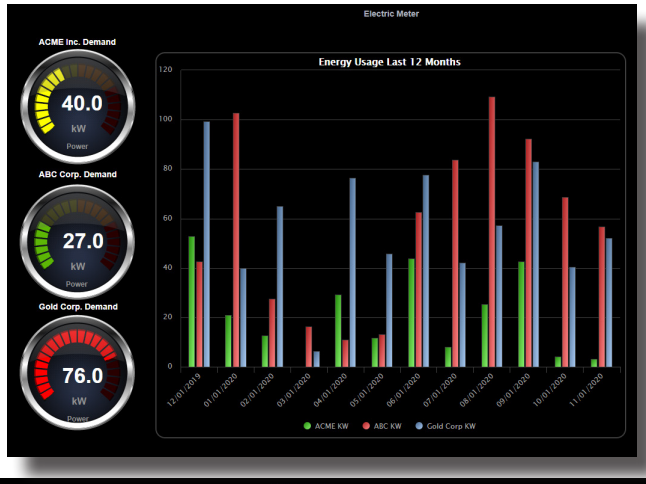
i-Vu® Building Automation System
i-Vu 8.0 Pro

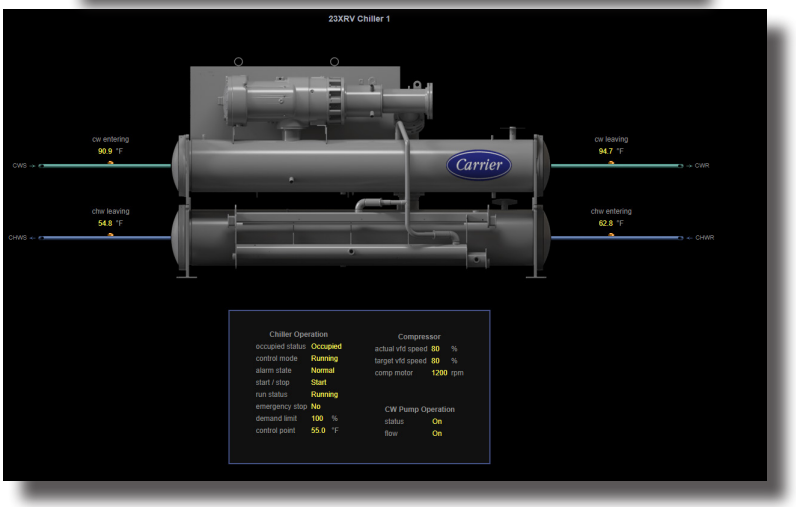
Manage your facility 24/7, 365 days a year with the powerful i-Vu web user interface that allows you to:

- Manage the HVAC equipment in your building from anywhere in the world using a standard web browser
- View and control the equipment in your building with a variety of PCs, tablets, and mobile devices
- Graphically configure and view schedules, setpoints, trends, alarms, and reports
- Integrate, monitor, and control other building systems such as lighting and meters using standard protocols

Features

- Powerful, comprehensive building management with intuitive point-and-click graphical access
- Dynamic, scalable vector floor plan graphics dynamically resize to monitor resolution and convey a quick understanding of building conditions
- Customizable graphics, schedules, trends, reports, and alarms
- Powerful reporting engine supports pre-built and customizable reports (available in Pro 750, Unlimited & Life Sciences)
- Plug and play connectivity with both factory and field-installed i-Vu®/CCN controllers
- Built-in ACxelerate™ VAV Auto-Commissioning tool
- Haystack-compatible semantic tagging automatically assigns standard reference names to equipment data
- BACnet/SC ready to support secure BAS infrastructures once BACnet/SC hardware is also available (future)
- Ready to support IPv6 once IPv6 Router is also available (future)
- Unlimited simultaneous users
- Easily integrates to third-party building systems and software using BACnet, Modbus® and LonWorks® protocols
- Multiple versions available to fit any size building or campus





i-Vu® Building Automation System
i-Vu 8.0 Pro

Client Requirements

Mobile Devices	Smart phones Android™, iOS Tablets: Android, iOS, Surface™	
Browsers	**A computer with this operating system**	**Supports these web browsers**
	Windows	Google™ Chrome™ v84.0 or later Microsoft® Edge v84 or later Mozilla® Firefox® v79.0 or later
	Mac OS	Safari® v11 or later
	(Apple Mac only)	Google Chrome v84.0 or later Mozilla Firefox v79.0 or later
	Linux	Google Chrome v84.0 or later Mozilla Firefox v79.0 or later

Server Requirements (Server sold separetely)

Specs	Quad core processor, 4G RAM, 100Mbps or higher LAN communications Supports PCs running Windows and Apple (Mac) PCs running Mac OS X	
OS	The following operating systems in 64-bit versions: Windows 10 Professional and Enterprise Windows Server 2019 Windows Server 2016 Windows Server 2012 R2	Windows 8 Professional and Enterprise
Database	The i-Vu Pro® v8.0 system supports the following and database engines are sold separately: Apache Derby (default database engine-included with purchase) SQL Server® Express 2019, 2017, 2016 SQL Server 2019, 2017, 2016 Oracle 12c MySQL 5.7.2 and 8.0 PostgreSQL 9.4 through 12	
Security	Supports TLS (Transport Layer Security) v1.3 with 256 bit encryption between client and i-Vu server Bacnet Secure Connect (BACnet/SC) secure, encrypted datalink layer	
Supports	Unlimited simultaneous users Communication to field controllers via BACnet (TCP/IP)	
Languages	International English, Brazilian Portuguese, Dutch, Finnish, French, French Canadian, German, Italian, Japanese, Korean, Norwegian, Russian, Simplified Chinese, Swedish, Thai, Traditional Chinese, Vietnamese	
BACnet	Advanced Operator Workstation (B-AWS) supporting BACnet Revision 19	
Part Numbers	CIV-OPNPR5 CIV-OPNPR32 CIV-OPNPR CIV-OPNPRUL	i-Vu 8.0 Pro-5 i-Vu 8.0 Pro-32 i-Vu 8.0 Pro-750 i-Vu 8.0 Pro Unlimited	5 Controllers Maximum 32 Controllers Maximum 750 Controllers Maximum, can create custom reports Unlimited Controllers, can create custom reports

For more information, contact your local Carrier Controls Expert.
Controls Expert Locator:
www.carrier.com/controls-experts

Carrier

i-Vu® Building Automation System
i-Vu for Life Sciences

i-Vu for Life Sciences provides the tools, reports and insights necessary to manage critical environments in your facility to maintain regulatory compliance. The intuitive web interface allows you to:

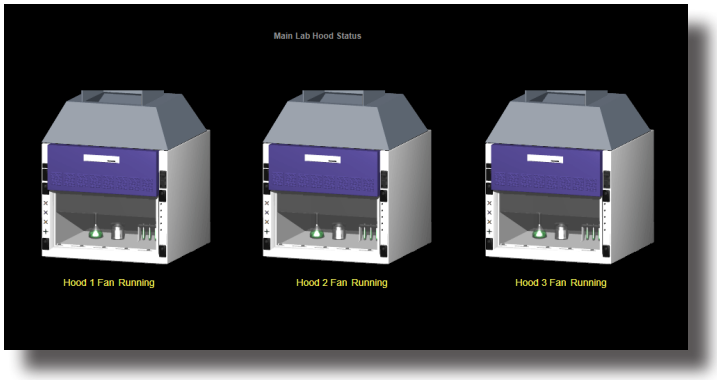
- Manage all HVAC equipment in your building while connected securely to the i-Vu Pro server using a standard web browser
- Maintain system integrity by recording all changes to equipment setpoints and configurations with authorized password protection
- Graphically configure and view schedules, setpoints, trends, alarms, and reports
- Integrate, monitor, and control sub-systems and devices using industry standard protocols
- Generate records compliant with FDA 21 CFR Part 11 requirements

i Vu

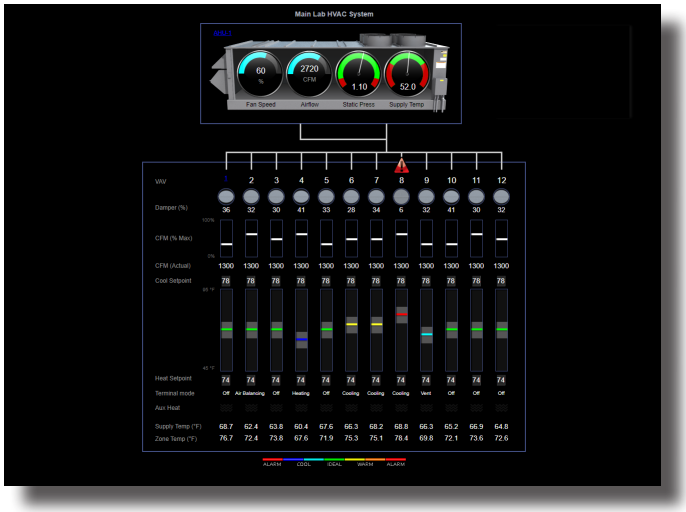
LIFE SCIENCES

Features

- Powerful reporting engine with pre-configured, digitally signed and approved compliance reports
- Flexible operator management with predefined and custom user levels
- Secure login management with LDAP/Active Directory
- Critical alarm acknowledgment requires operator signature and comment
- Dynamic, scalable vector floor plan graphics resize to monitor resolution to convey a quick understanding of building conditions
- Customizable graphics, schedules, trends, reports, and alarms
- Support for unlimited number of controllers
- Haystack-compatible semantic tagging automatically assigns standard reference names to equipment data
- BACnet/SC Ready to support secure BAS infrastructures once BACnet/SC hardware is also available (future)
- IPv6 Ready to support IPv6 once IPv6 Router is also available (future)
- Easily integrates to third-party building systems and software using BACnet, Modbus® and LonWorks® protocols



Lab Hood Status Screen



Lab HVAC System Screen

i-Vu® Building Automation System
i-Vu for Life Sciences

Client Requirements

Mobile Devices	Smart phones: Android™, iOS Tablets: Android, iOS, Surface™

Browsers	**A computer with this operating system**	**Supports these web browsers**
	Windows	Google™ Chrome™ v84.0 or later Microsoft® Edge v84 or later Mozilla® Firefox® v79.0 or later
	Mac OS	Safari® v11 or later
	(Apple Mac only)	Google Chrome v84.0 or later Mozilla Firefox v79.0 or later
	Linux	Google Chrome v84.0 or later Mozilla Firefox v79.0 or later

Server Requirements (Server sold separately)

Specs	Quad core processor, 4G RAM, 100Mbps or higher LAN communications Supports PCs running Windows and Apple (Mac) PCs running Mac OS X
OS	The following operating systems in 64-bit versions: Windows 10 Professional and Enterprise Windows 8 Professional and Enterprise Windows Server 2019 Windows Server 2016 Windows Server 2012 R2
Database	The i-Vu Pro® v8.0 system supports the following and database engines are sold separately: Apache Derby (default database engine-included with purchase) SQL Server® Express 2019, 2017, 2016 SQL Server 2019, 2017, 2016 Oracle 12c MySQL 5.7.2 and 8.0 PostgreSQL 9.4 through 12
Security	Supports TLS (Transport Layer Security) v1.3 with 256 bit encryption between client and i-Vu server BACnet Secure Connect (BACnet/SC) secure, encrypted datalink layer
Supports	Unlimited simultaneous users Communication to field controllers via BACnet (TCP/IP)
Languages	International English, Brazilian Portuguese, Dutch, Finnish, French, French Canadian, German, Italian, Japanese, Korean, Norwegian, Russian, Simplified Chinese, Swedish, Thai, Traditional Chinese, Vietnamese
BACnet	Advanced Operator Workstation (B-AWS) supporting BACnet Revision 19
Part Numbers	CIV-OPNPRLS i-Vu 8.0 Pro-Life Sciences Unlimited Controllers

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System
i-Vu Cloud

Part# CIV-OPNPRC

The Carrier I-Vu Cloud solutions bring deployment flexibility to customers while helping them scale for growth and reduce their support burden. Powered by the technology, security, and infrastructure of Amazon Web Services (AWS), I-Vu Cloud provides a predictable cost of ownership. It includes cloud-hosting, server maintenance, I-Vu site reliability monitoring, database redundancy and backups, and software upgrades eliminating the need for customers to install, configure, and manage a building automation server in the building. In addition, there is no costly IT infrastructure to maintain, and IT compliance directives for the server - including reliability, security, and uptime – are managed by Carrier.

Always Patched

Always Secure

Always Backed up

Always Authenticated

Key Features and Benefits

The I-Vu Cloud system provides local to global indoor environmental quality control and energy management, all with the peace-of-mind knowing that I-Vu Cloud uses BACnet Secure Connect to encrypt network communications and keep the building automation networks secure. I-Vu Cloud includes all the features of the I-Vu system plus:

- BACnet Secure Connect (BACnet/SC), the ASHRAE Standard secure, encrypted datalink layer designed to meet the requirements and constraints of modern IP infrastructures

Provided by AWS:

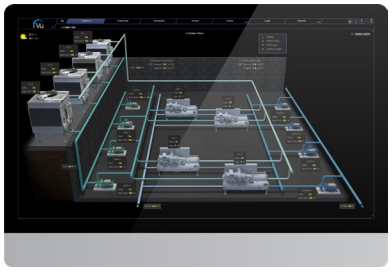
- Assured Server Uptime
- Triple datacenter redundancy
- Daily database backups
- GuardDuty threat detection service

- Internet Protocol Versions IPv6 and IPv4 are supported
- Pair with i-Vu Add-ons to add more capability and value to your i-Vu system. Here are some example add-ons that are compatible:
  - IntelliPro™: i-Vu Health Monitoring and Asset Analytics
  - Hourly Weather
  - Automated Demand Response
  - BACnet® Scheduling Interface
  - Microsoft® Exchange Scheduling
  - Trend Export

i-Vu Building Automation System
i-Vu Cloud

SPECIFICATIONS

CLIENT REQUIREMENTS		
Mobile Devices:	Smart Phones	Android™, iOS
	Tablets	Android, iOS, Surface™
Computers:	**Computer operating system**	**Supports these web brows**
	Windows	Google™ Chrome™ v84 or later Microsoft® Edge v84 or later Mozilla® Firefox® v79 or later
	Mac OS X (Apple Mac only)	Safari® v11 or later Google Chrome v84 or later Mozilla Firefox v79 or later
	Linux	Google Chrome v84 or later Mozilla Firefox v79 or later
COMMUNICATION		
BACnet:	BACnet Secure Connect (BACnet/SC) secure, encrypted datalink layer BACnet Protocol Revision 19 Compliant BACnet Advanced Operator Workstation (B-AWS)	
Languages:	International English, Brazilian Portuguese, French, French Canadian, German, Italian, Japanese, Korean, Russian, Simplified Chinese, Swedish, Thai, Traditional Chinese, Vietnamese, Dutch, Norwegian, Finnish	
I-Vu SECURITY		
Security:	BACnet Secure Connect (BACnet/SC) secure, encrypted datalink layer	
	Supports TLS (Transport Layer Security) v1.3 with 256 bit encryption between client and I-Vu server	
AWS CLOUD SECURITY		
Comprehensive Security and Compliance Controls AWS regularly achieves third-party validation for thousands of global compliance requirements that are continually monitored to help you meet security and compliance standards. AWS supports PCI-DSS, HIPAA / HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping satisfy compliance requirements for virtually every regulatory agency around the globe. For the latest AWS security standards visit: https://aws.amazon.com/security		



PRODUCT VERSIONS

SKU	Description
CIV-OPNPRC	I-Vu CLOUD
CIV-OPNPRCUG	Used when upgrading I-Vu to I-Vu CLOUD

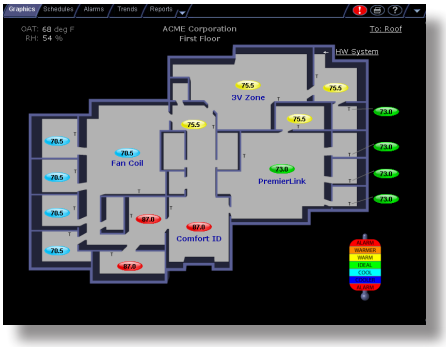
COMPATIBLE ADD-ONS AND ACCESSORIES

SKU	Description
ADD-SCH_EXCH	Microsoft® Exchange Scheduling add-on
ADD-OG-IAM	Lenel OnGuard – Integrated Alarm Management add-on
ADD-FDD	Fault Detection and Diagnostics Reporting & Dashboards add-on
ADD-HR-WTHR	Hourly Weather Forecast add-on

For more information, contact
your local Carrier Controls Expert.
Controls Expert Locator:
www.carrier.com/controls-experts

Carrier

i-Vu® Building Automation System
i-Vu Alarming

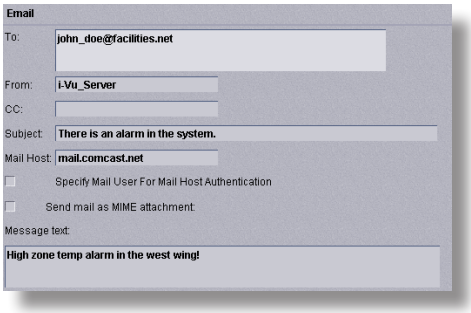


i Vu

Alarm Actions

i-Vu is easily configured to perform alarm actions that can notify personnel of an alarm or record information about an alarm in your Carrier system:

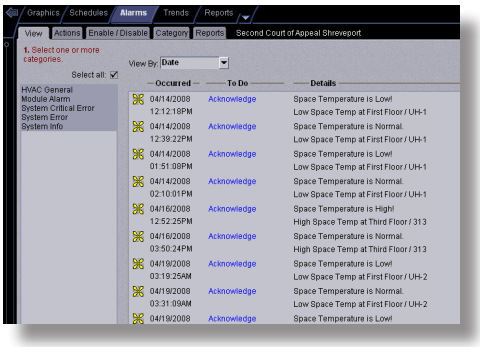
- Send an e-mail
- Print
- Play an audio file
- Pop-up a message on a client PC



System-Wide Alarms Button

A system-wide alarms button is always present and changes color based on severity of alarms in your Carrier system:

- Red - critical alarms need to be acknowledged
- Yellow - non-critical alarms need to be acknowledged
- Black - no alarms need to be acknowledged

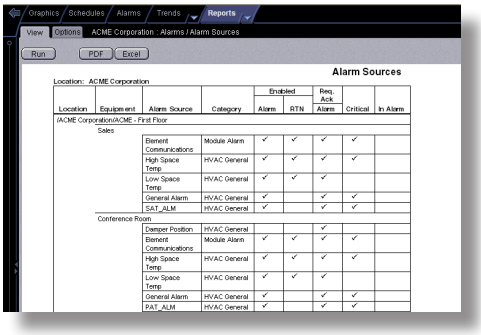


Intuitive Alarm Viewer

i-Vu's powerful alarming capabilities allow you to see alarm events in your entire Carrier system from a single screen.

Alarms are easily sorted by date, type, or incident, allowing you to respond quickly to critical alarms while filtering out nuisance alarms.

- View, acknowledge, print, or delete alarms with ease
- Search for specific alarms based on time and date



Reports

- Alarms - view alarms that are currently in the system
- Alarm Sources - view all points that are configured to alarm
- Alarm Actions - view the configured actions for each alarm

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

 Cat. No. 11-808-374-01 Rev. 10/20

Carrier

i-Vu® Building Automation System
i-Vu Scheduling

Area Scheduling

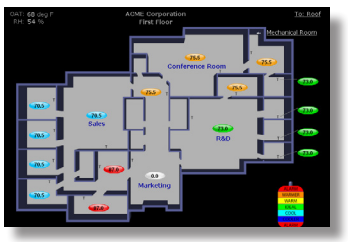
Scheduling your Carrier system is a breeze with i-Vu's intuitive scheduling interface. Simply point and click in i-Vu's navigation tree to enter schedules at the building, area, or zone level:

- Schedules added at the building level affect all equipment in the building
- Schedules added at an area level affect all pieces of equipment in that area.
- Schedules added at a zone level affects only the equipment in that zone.
- Define schedule groups for even greater flexibility. When you apply a schedule to a schedule group, the schedule affects all pieces of equipment in that group.

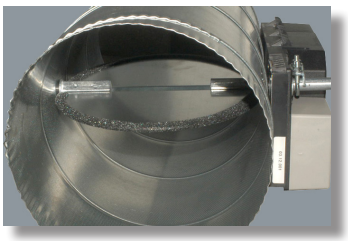
Viewing Schedules

Point and click in the navigation tree, and i-Vu allows you to view the relevant schedules at that level and below. The effective schedules (occupied or unoccupied), and priority schedules (Normal, Holiday, and Override), are all color-coded for easy viewing on one screen. View schedules for the current week, or rewind/fast forward to see past or future schedules.

Conserve Energy



Area Scheduling



Effective Control

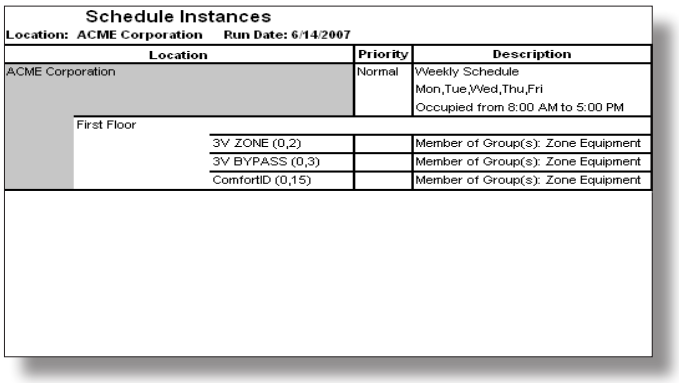
i-Vu® Building Automation System
i-Vu Scheduling

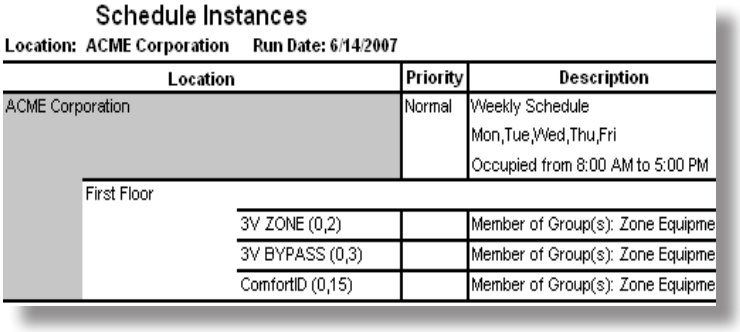
Creating Schedules

It's simple to add customized schedules to keep occupants comfortable and equipment running efficiently. First select the priority for the schedule that you wish to add (Normal is low priority; Holiday is medium; Override is high). Then select the schedule type that meets your needs:

- Weekly - every week on the specified days
- Date - on a single, specified date added
- Date Range - between two specified dates
- Date List - on multiple, specified dates
- Wildcard - according to a repeating pattern
- Continuous - continuously between specified times on two separate dates
- Dated Weekly - weekly between a start date and an end date
- Date List - on multiple, specified dates

Then simply drag the start and stop times on the schedule graph to complete the schedule. Once schedules are in the system, they can be easily edited by dragging the start and stop times to change them. You can also delete or print schedules with the click of a button, directly from the same screen.





Reports

For added flexibility, i-Vu also supports schedule reports. These reports may be viewed within i-Vu, or they may be exported to .pdf or Excel for easy viewing.

- Schedule Instances - shows detailed information as to locations, priorities, and other schedule details such as start/stop times, days of week, etc. This report can help you discover newly added and conflicting schedules.
- Effective Schedules - View all equipment that may be scheduled and the net result of all schedules in effect for a selected time and date.

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System
BACnet Scheduling Interface Add-on

Part Number: ADD-SCH_BACNET

The BACnet Scheduling Interface add-on allows third-party event management software to write BACnet schedules to the i-Vu building automation system. These schedules can then be used to tell mechanical equipment when to run in the building.

Often times building operators may use operations management software to maintain a single calendar of events for a facility. This add-on provides them with a seamless integration to the building automation system so that they can manage comfort conditions and/or lighting systems in the building during scheduled events. When BACnet schedules are written through this add-on, building operators are also able to manage the schedules using the i-Vu user interface.

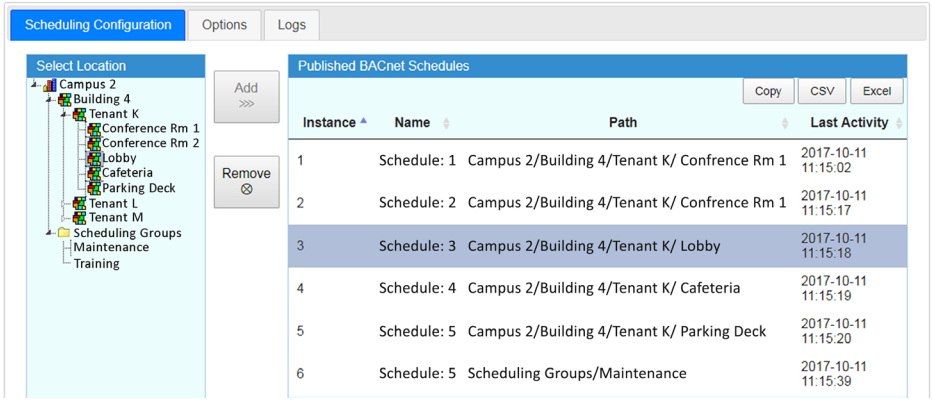
Application Features

Allows the i-Vu building automation system to be scheduled via third-party BACnet software such as:

- SchoolDude® - Operations Management Software
- Events2HVAC™ - Event Automation Software
- Hospitality Scheduling Software

Requirements

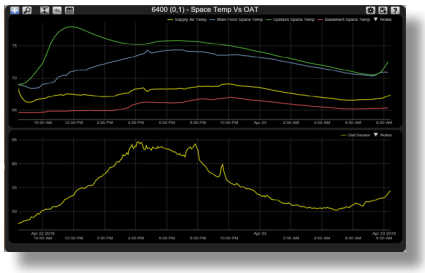
- i-Vu Pro 6.5 or later user interface with latest cumulative update
- Software is configured with at least one active BACnet IP connection
- Licensed BACnet Scheduling Interface Add-on
- Third-party BACnet software must meet BACnet protocol revision v4 or later, including clients that support the K.3 BIBBs: SCHED-A, SCHED-AVM-A, SCHED-VM-A.



For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System
i-Vu Trends and Reports



Multiple Trend Samples

Automatic Trends and Powerful Reports

i-Vu's automatic trending capabilities mean that a history of your equipment's operation is being saved without any special setup. Trends can be easily modified to sample at different time intervals or on change of value instead.

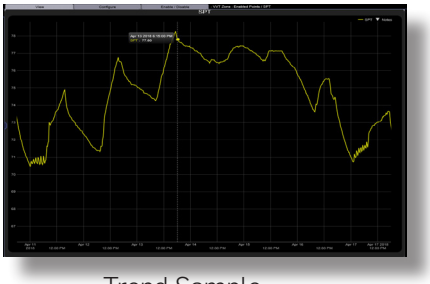
Turn trend data into interactive, graphical reports using i-Vu's reporting capabilities. Reports can be scheduled to run automatically, sent to e-mail recipients and stored in multiple file formats.

i-Vu Trends

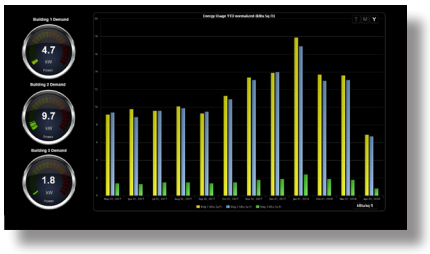
Viewing trends is effortless with i-Vu. Simply point and click to a piece of equipment in the navigation tree, and you will be presented with a comprehensive list of trend points that are already enabled. Pick any point to view the trend graph. While viewing the trend graph, there are many tools at your disposal:

- Use arrow keys to pan the trend graph in different directions.
- Draw a rectangle around a specific area to zoom-in on that data.
- Use the Page Down key to zoom-out on specific trend data.
- Enter a specific start date to jump to the trend graph for that date.
- Show point markers for each data point in the graph.
- Copy the trend graph data that is being displayed on the screen and paste it into Excel.

You can also graph multiple trend points simultaneously to help monitor and troubleshoot your system. A comparison trend graph can display up to four graphs on the same page.



Trend Sample

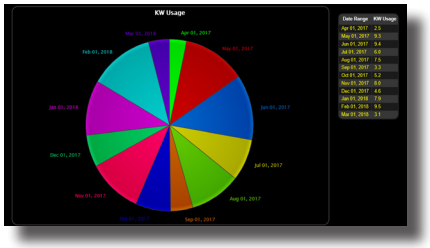


Reports -Bar Chart

i-Vu Reports

The i-Vu system includes standard reports that provide insight on equipment status and users of the system. Security, alarms, schedules, equipment and commissioning reports can be viewed and printed. i-Vu Plus and Pro systems also include custom reporting capabilities. Reports can be created, edited, viewed, and scheduled using the Report Manager tool. Easily create reports for energy usage, system status, historical data, and much more. The Report Manager also supports Java math functions to perform calculations on column data, allowing for easy creation of reports based on calculated data. Some examples include:

- BTU calculations from flow and delta temperature measurements
- Normalized energy usage
- Aggregate consumption
- Min/Max/Average values



Reports -Pie Chart

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

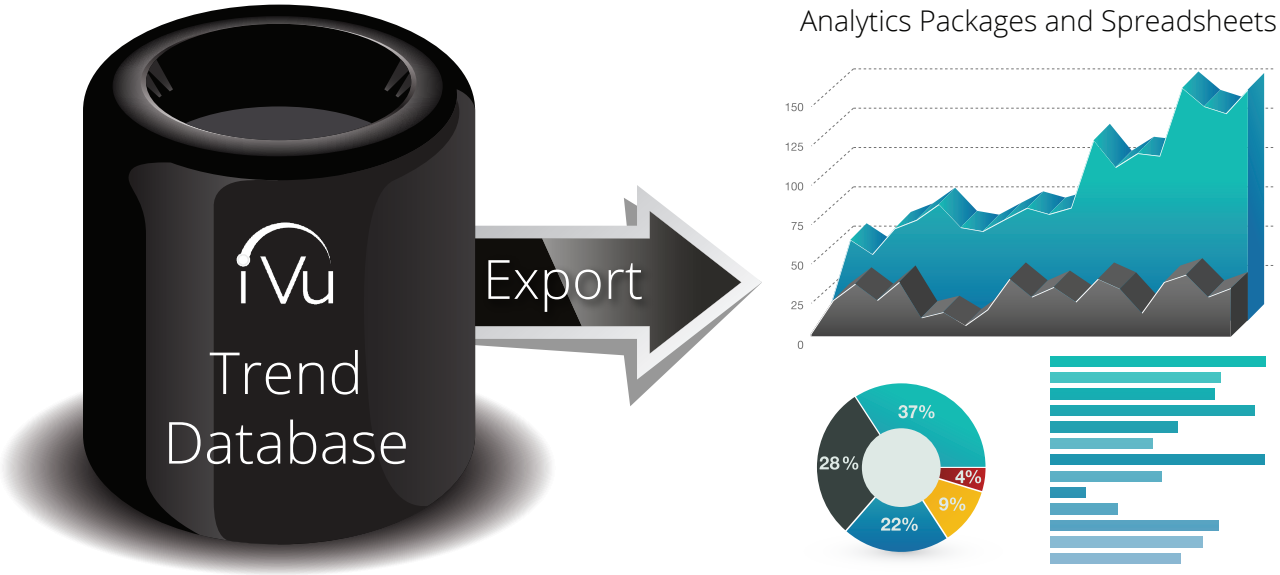
i-Vu® Building Automation System
Trend Export Add-on

Part Number: ADD-TRNDEXP

Carrier® i-Vu® add-ons extend the capability of the i-Vu building automation system. The Trend Export add-on allows you to specify, manage, and export trend data from the i-Vu building automation system so that it can be analyzed externally using third party analytics packages or tools. Trend data can be exported on-demand or at scheduled intervals. This provides building operators with a simple and powerful way to view their important building data inside their visualization tool of choice.

Application Features

- Common .CSV or database export format for the trend data ensures ease of use outside of the i-Vu building automation system
- Daily, hourly, and on-demand export options
- Up to two years of trend data can be exported
- Trend data can be grouped and scheduled for added flexibility
- Reoccurring trend exports only include new historical data received since the last export
- Trend source geographic information included with export



Requires: i-Vu Pro User Interface

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System
Hourly Weather Add-on

Part Number: ADD-HR-WTHR

Carrier® i-Vu® add-ons extend the capability of the i-Vu building automation system.

The hourly forecasting add-on extends the capability of the existing weather add-on (version 2.5 or higher) using data from the AccuWeather.com® weather service. Once licensed, the hourly forecasting capability is enabled in the weather add-on allowing i-Vu to execute intelligent control strategies based on hourly weather forecast data for the next five days. These predictive control strategies can help building operators maximize occupant comfort and energy efficiency indoors, while also optimizing the use of water in irrigation systems outdoors.

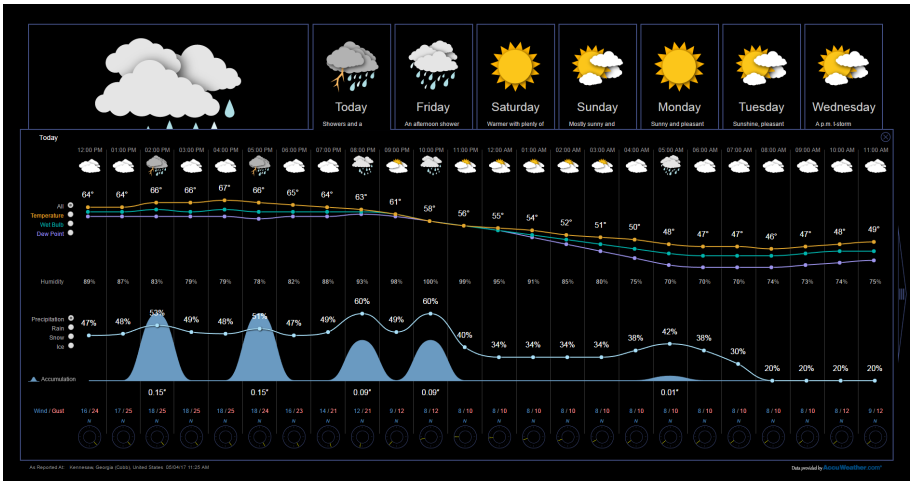
Application Features

- Full 5-day, hourly forecast: Temperature | Dewpoint | Web bulb | Humidity
- Hourly precipitation forecast: Rain | Snow | Ice
- Wind conditions forecast: Direction | Speed | Gust speed

Requirements

- i-Vu Pro User Interface with latest cumulative patch

Includes control program and i-Vu system graphic for easy deployment.



For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System
Micosoft® Exchange Scheduling

Part Number: ADD-SCH_EXCH

The Microsoft® Exchange Scheduling add-on integrates Microsoft Outlook® room reservations with Carrier's i-Vu® building automation system.

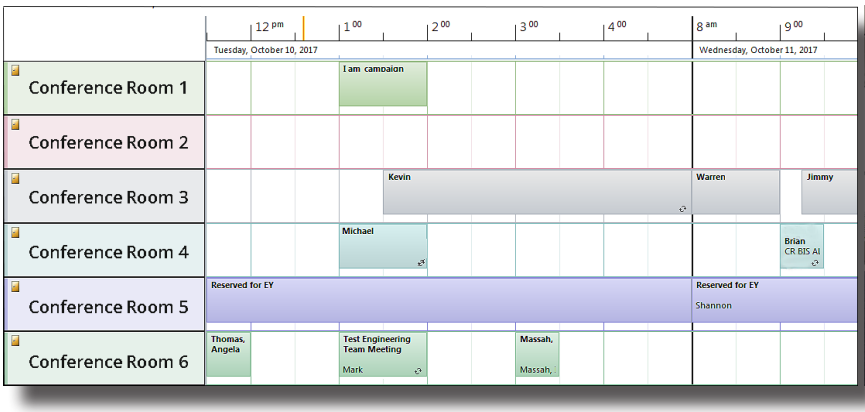
The Microsoft Exchange scheduling add-on uses Microsoft Exchange Web Services (EWS), to read Outlook room reservations from the Microsoft Exchange server. As Outlook room reservations are read from the Exchange server, they are written to the i-Vu building automation system. They are then used to operate heating, cooling, and lighting systems in the room based on the desired schedule, promoting optimized comfort for occupants and energy savings for building managers.

Application Features

- Allows the building automation system to be scheduled using Microsoft Outlook
- Keeps occupants comfortable by turning on HVAC and lighting systems when rooms are in use
- Promotes energy savings by keeping room temperatures within a specified range during occupied and unoccupied periods

Requirements

- Requires i-Vu Pro 6.5 or later user interface with latest cumulative update
- Licensed Microsoft Exchange Scheduling add-on
- Microsoft Exchange 2010 or later with a service mailbox
- Exchange Web Services (EWS) must be enabled on the Microsoft Exchange Server
- Microsoft Outlook client with room scheduling access



 Cat. No. 11-808-649-01 Rev. 10/20

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

Carrier

i-Vu® Building Automation System
i-Vu Tenant Billing

i-Vu

i-Vu's Tenant Billing application provides building owners and managers with a convenient mechanism for tracking and billing tenants for their after-hours energy consumption in the i-Vu Building Automation system. This after-hours energy consumption is based on override events that can be initiated by the tenant inside of their controlled space. If a tenant wishes to extend their normal business hours or decides to enter the building during a normally unoccupied period, then they can simply press the override button on their space sensor to turn on the HVAC and/or lighting system. Each override event is then captured by the Tenant Billing application, allowing the building owner to invoice the tenant for their energy usage during that time period.

As a result, after-hours energy costs are easily tracked and distributed to the tenants in your facility. And best of all, you can view tenant activity or invoices at any time from anywhere in the world using a standard web browser.

Easy Owner Configuration

It's simple to create a customized invoice template for your tenants. Simply add your company's return address and logo to the invoice, along with a billing contact name and any special billing instructions. Configure email settings for all tenant invoices from a single screen.

Easy Tenant Setup

It's easy to manage all of the tenants in your Carrier system. Add, edit, or delete tenants with the touch of a button. Customize the way that each tenant is billed. Define allowances, exemptions, billing rates, minimum billing time, and minimum override increments for each tenant. Associate tenants with their specific area(s) of the building easily with the click of a button.

Invoicing Options

Invoices can be scheduled to run monthly for each tenant or they can be created manually on an as-needed basis. You can choose to bill tenants based on the previous calendar month or you can define custom start and end dates. When creating invoices manually, the user has the option to view invoices using Excel (.xls format), or Adobe Reader (.pdf format). Once the invoice is displayed, the user can choose to save it for future reference. When invoices are scheduled to run automatically, only a .pdf invoice is generated. The invoices are then automatically e-mailed to the specified tenants.

Detailed Invoices

Detailed invoices are a standard part of the package. All invoices include an invoice date, number, billing period, due date, and the amount due. All override events are outlined in a detailed summary section of the invoice. Each event includes a date, begin time, duration, and billed amount. Then a sub-total is calculated for all events along with the total due.

System Requirements

i-Vu Plus or i-Vu Pro

TLO

Timed Local Override

Override Events Recorded

i-Vu® Building Automation System
i-Vu Tenant Billing

Invoicing Options

Invoices can be scheduled to run monthly for each tenant or they can be created manually on an as-needed basis. You can choose to bill tenants based on the previous calendar month or you can define custom start and end dates. When creating invoices manually, the user has the option to view invoices using Excel (.xls format), or Adobe Reader (.pdf format). Once the invoice is displayed, the user can choose to save it for future reference. When invoices are scheduled to run automatically, only a .pdf invoice is generated. The invoices are then automatically e-mailed to the specified tenants.

Detailed Invoices

Detailed invoices are a standard part of the package. All invoices include an invoice date, number, billing period, due date, and the amount due. All override events are outlined in a detailed summary section of the invoice. Each event includes a date, begin time, duration, and billed amount. Then a sub-total is calculated for all events along with the total due.

System Requirements

i-Vu Plus or i-Vu Pro

 Cat. No. 11-808-384-01 Rev. 10/20

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System
LDAP/Active Directory Add-on

Part Number: ADD-LDAP

The LDAP/Active Directory® add-on for the i-Vu® building automation system is an authentication provider that allows you to log in to the building automation system using LDAP (Lightweight Directory Access Protocol) or AD (Active Directory) credentials.

This add-on uses the building automation system operator login name to find the user's LDAP entry and discover their LDAP login name from the entry. The exact configuration is determined by the authentication type chosen, but all implement a Search Base where the LDAP add-on will search to find users. The values set in the Search Filters determine how that search is performed.

Once the LDAP add-on has been set up, user credentials within i-Vu are managed through the network security. The add-on also supports a mixed mode where assigned local operators are managed through the i-Vu system.

Application Features

- i-Vu user credentials can be managed via the same process as other network credentials
- The LDAP/AD add-on supports two LDAP authentication methods:
  - Simple with Transport Layer Security (TLS)
  - Digest-MD5 with or without TLS
- Supports host certificate discovery

Requirements

- Requires i-Vu Pro 6.5 or later user interface with latest cumulative update
- Licensed LDAP Add-on
- System administration capabilities for LDAP or Active Directory configuration host certificate discovery

For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System

Automated Demand Response Add-on

Part Number: ADD-OADR2

Carrier's Automated Demand Response (OpenADR®) add-on is a software application that allows a utility supplier to automatically and securely communicate with Carrier's i-Vu® building automation system.

The OpenADR add-on listens for demand response signals from the utility company. These signals are passed to i-Vu controllers, where demand-reduction strategies are applied to the connected HVAC equipment. When participating in automated demand response programs, customers may receive reduced utility rates or utility rebates[1].

[1] Cost reductions are dependent on proper implementation of demand response strategy. Availability of rebates depends on your utility provider. Please contact your utility provider for more information.

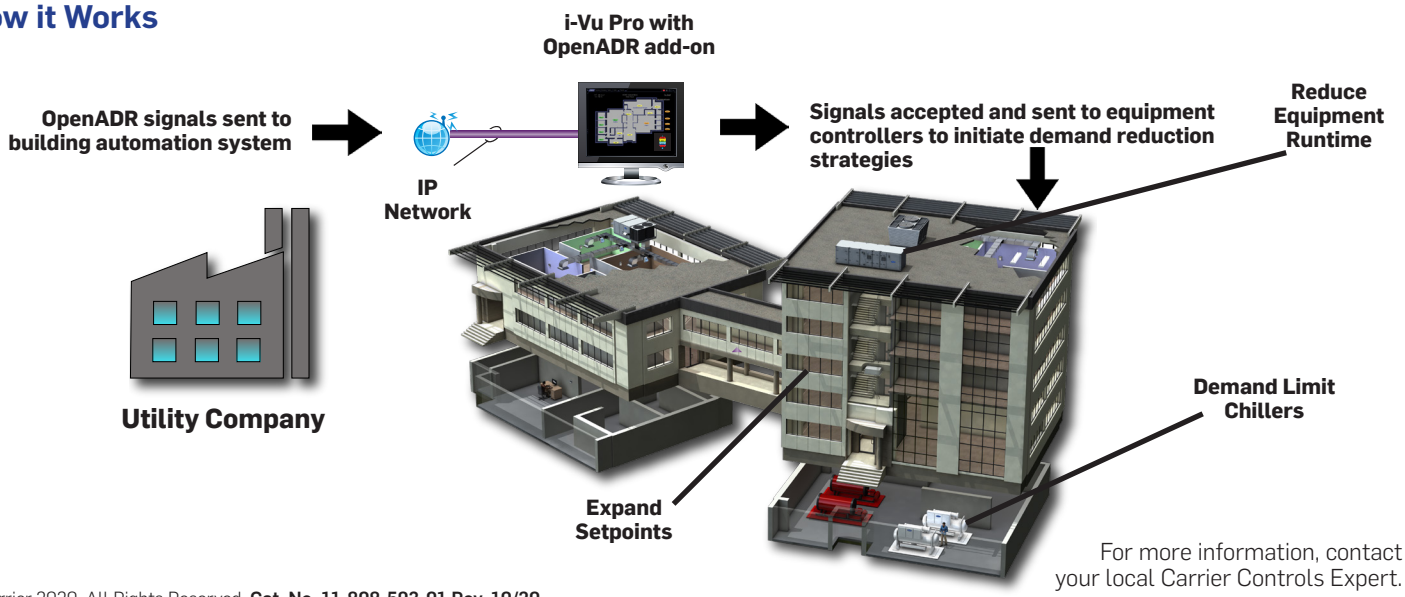
Application Features

- Provides a standardized connection to utility providers that participate in OpenADR®
- Mitigates the cost associated with Critical Peak Pricing (CPP) events
- Earn incentives for participation, depending on utility company
- Plug and play - demand level response is built into all Carrier i-Vu® factory programmed controllers

Compatibility

- Requires i-Vu Pro user interface
- Meets OpenADR profile 2.0a+b. Simple signal profile 2.0a+b application is available in EquipmentBuilder library; other signal types are supported using custom Snap applications.
- OpenADR certified

How it Works



For more information, contact your local Carrier Controls Expert.

Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System
Door Status Integration

Part Number: ADD-DOOR_STATUS-17-01

The Door Status Integration 17-01 allows you to monitor and respond to door-related events from a Honeywell® system by creating points that can be viewed on a graphic in the i-Vu system.

Application Features

- Visualize door status on i-Vu floorplan graphics
- Monitor these door events:
  - Door Normal
  - Door Forced Open
  - Door Ajar
  - Door Trouble
  - Door Locked

Requirements

- ADD-DOOR_STATUS-17-01
- i-Vu Pro version 7.0 (minimum*)
- Honeywell WIN-PAK® with API v4.7 (minimum*)
- Internet Information Server (IIS) v5.1 (minimum*)
- .NET Framework v4.5 (minimum*)

*Contact your Carrier representative to determine if subsequent releases of this product are compatible with the Door Status Integration add-on

Example of a door status visualization:
Green | Yellow | Red dots indicating status on floorplan.

For more information, contact your local Carrier Controls Expert.
Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System

OnGuard® Integration Add-on

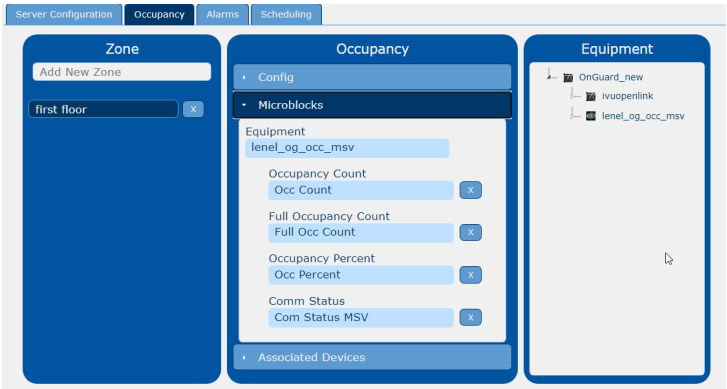
Data Connector (Part# ADD-OG-DIP)

The OnGuard integration consists of a collection of add-ons that allow the i-Vu building automation system and an OnGuard security system to work together. The OnGuard integration solution consists of three add-ons that you can purchase based on your integration needs.

It starts with the Data Connector add-on, which provides the basic communication connection that is needed to transfer data to and from the OnGuard system. With this add-on only, occupancy data can be read into i-Vu through control programs that can then be displayed on i-Vu graphics pages. The Data Connector is a required component for the other two add-ons that are supported.

The Advanced Occupancy Scheduling add-on predicts and schedules occupancy based on past occupancy data that comes from the OnGuard system to promote optimized energy usage and occupant comfort.

The Integrated Alarm Management add-on enables the exchange of alarms between the i-Vu system and the OnGuard system.



Key Features and Benefits

- Read occupancy data provided by the OnGuard system
- Configure OnGuard connector settings
- Display occupancy data visually on i-Vu graphics pages

Data Connector add-on required for

- Advanced Occupancy Scheduling add-on
- Integrated Alarm Management add-on

Compatibility

- i-Vu Pro v8.0 or newer
- Building Integration Platform 1.11 or newer
- OnGuard version must be:
  - v7.5 or later, using the OpenAccess interface
- See requirements in OnGuard v1.1 Integration guide for more details

For more information, contact your local Carrier Controls Expert.
Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System

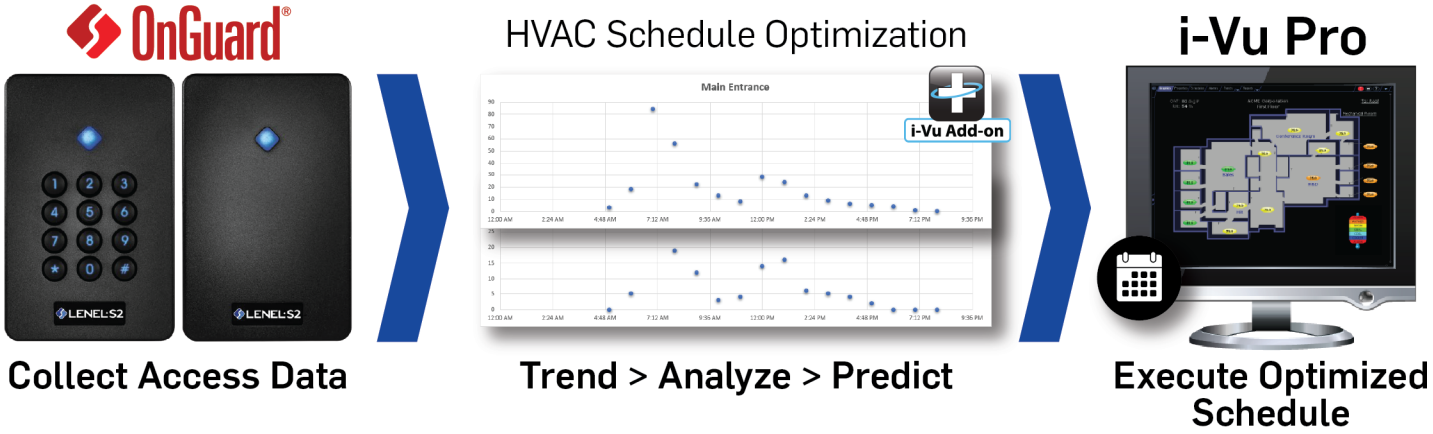
OnGuard® Integration Add-on

HVAC Schedule Optimization (Part# ADD-OG-AOS)

The OnGuard integration allows the i-Vu building automation system and an OnGuard security system to work together. The OnGuard integration solution consists of three add-ons that you can purchase based on your integration needs.

It starts with the Data Connector add-on, which provides the basic communication connection that is needed to transfer data to and from the OnGuard system. The Data Connector is a required component for the HVAC Schedule Optimization add-on.

The HVAC Schedule Optimization add-on predicts and schedules occupancy based on data that comes from the OnGuard system, which promotes optimized energy usage and occupant comfort.



Key Features and Benefits

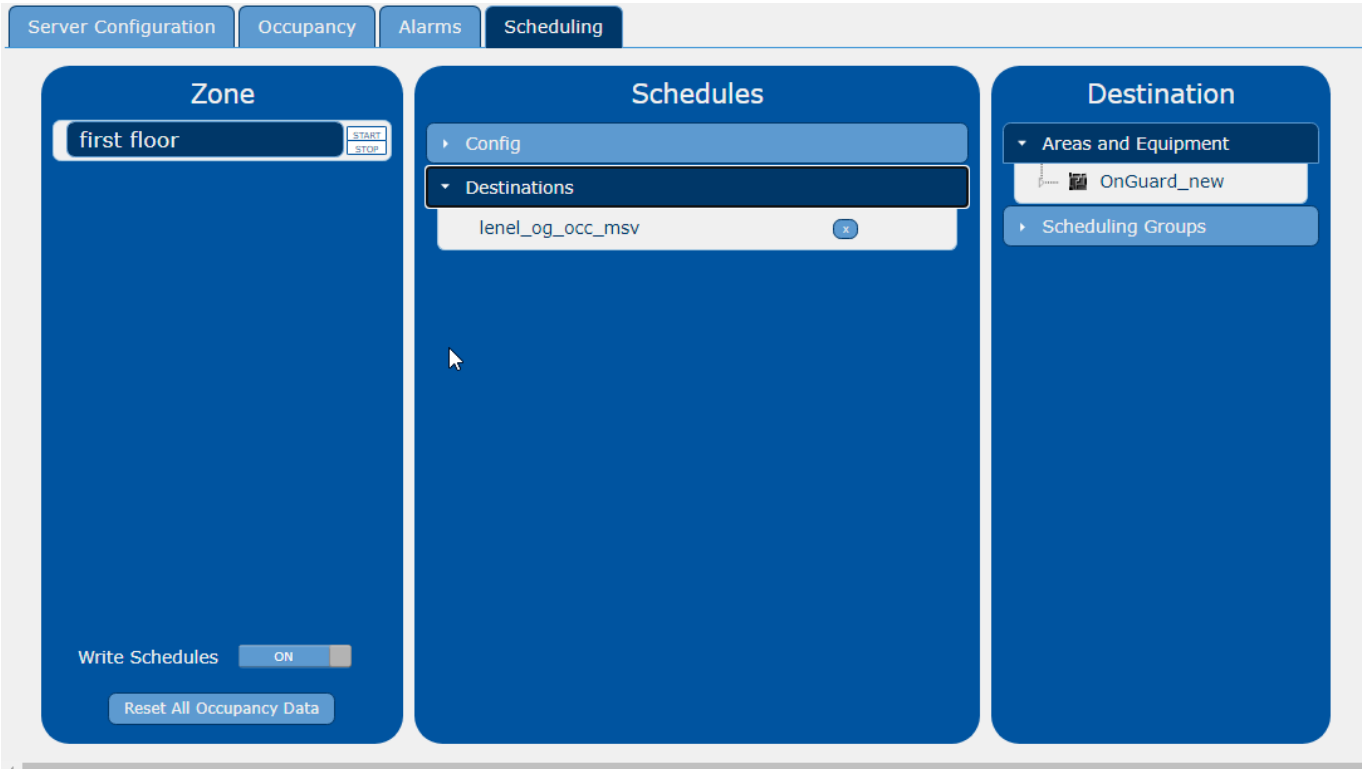
- **Optimal Start Coupling** - Supports comfort at typical occupancy, and covers “early birds”.
- **Rolling Average by “Day of Week”** - Evaluates each day of the week separately to account for daily variances.
- **Dynamic Assessment** - Responds to changes in occupancy profiles over time.
- **Exception Handling** - Analyzes data for unusual occupancy patterns such as holidays and discards them to avoid influencing predictions.

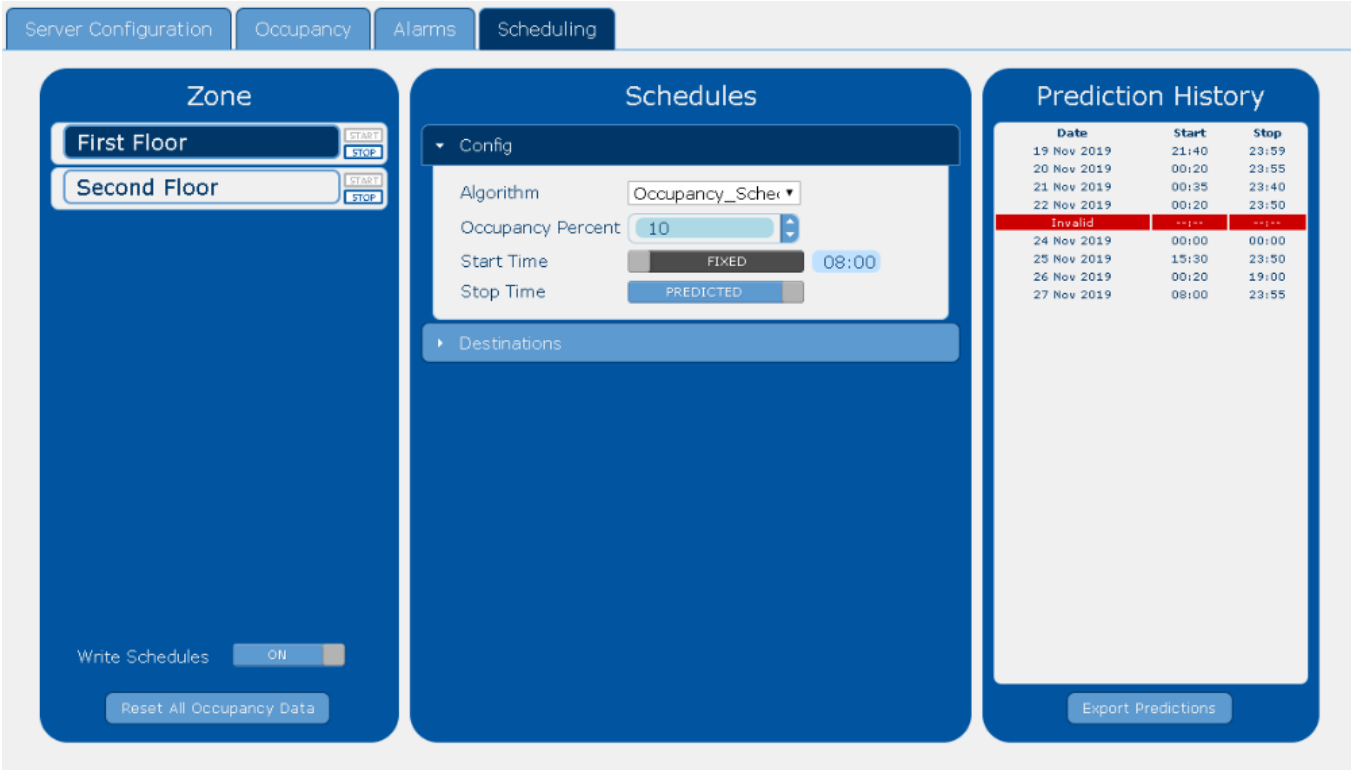
Compatibility

- i-Vu Pro v8.0 or newer
- Building Integration Platform 1.11 or newer
- OnGuard version must be:
  - v7.5 or later, using the OpenAccess interface
- See requirements in OnGuard v1.1 Integration guide for more details
- Requires Data Connector add-on (Part# ADD-OG-DIP)

For more information, contact
your local Carrier Controls Expert.
Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu Building Automation System
OnGuard Integration Add-on
HVAC Schedule Optimization





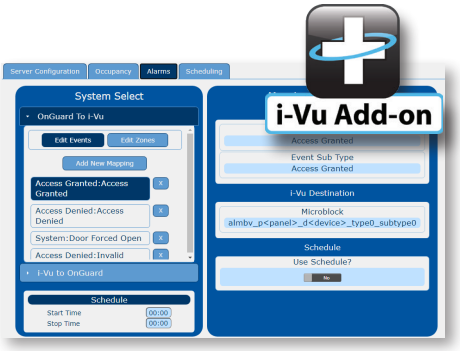
 Cat. No. 11-808-866-01 Rev. 7/22

For more information, contact your local Carrier Controls Expert.
Controls Expert Locator:
www.carrier.com/controls-experts

i-Vu® Building Automation System

OnGuard® Integration Add-on

Integrated Alarm Management (Part# ADD-OG-IAM)



The OnGuard integration allows the i-Vu building automation system and an OnGuard security system to work together. The OnGuard integration solution consists of three add-ons that you can purchase based on your integration needs.

It starts with the Data Connector add-on, which provides the basic communication connection that is needed to transfer data to and from the OnGuard system. The Data Connector is a required component for the Integrated Alarm Management add-on.

The Integrated Alarm Management add-on enables the exchange of alarms between the i-Vu system and the OnGuard system.

Alarm Data from OnGuard System

Alarm Data Sharing

Centralized Alarm Management

Key Features and Benefits

- **Improve Alarm Coverage** - Facility staff and security staff can monitor each other's alarms so that either team can dispatch appropriate personnel regardless of who is currently on shift. Note, the Alarm Management Add-On is used only as a secondary means of notification.
- **Adjust HVAC to Meet Demand** - Specified alarms can interact with the i-Vu system equipment and initiate on-demand ventilation for real time response.

Compatibility

- i-Vu Pro v8.0 or newer
- Building Integration Platform 1.11 or newer
- OnGuard version must be:
  - v7.5 or later, using the OpenAccess interface
- See requirements in OnGuard v1.1 Integration guide for more details
- Requires Data Connector add-on (Part# ADD-OG-DIP)

 Cat. No. 11-808-867-01 Rev. 7/22

For more information, contact your local Carrier Controls Expert.
Controls Expert Locator:
www.carrier.com/controls-experts

OnGuard v1.1 Integration

for v8.0 or later systems

Carrier ©2022 · Catalog No. 11-808-859-01 · 7/28/2022

 Verify that you have the most current version of this document from **www.hvacpartners.com**, the **Carrier Partner Community** website, or your local Carrier office.

Important changes are listed in **Document revision history** at the end of this document.

Contents

What is the OnGuard Integration?

The OnGuard® Integration consists of a collection of add-ons that allow the i-Vu® Pro building automation system and an OnGuard® security system to work together. The OnGuard® Integration enables the i-Vu® Pro system to utilize actual occupancy data in control program logic by monitoring entry and exit events.

Included in the .zip file...	Purpose
Data Connector (page 6) *(onguard.addon)*	You must install the OnGuard® Data Connector add-on before installing any of the other OnGuard® .add-on files. The i-Vu® Pro application can track Occupancy through the security system.
Advanced Occupancy Scheduling (page 9) *(onguard-scheduling.addon)*	Based on historical occupancy trends, the add-on will write predicted scheduling to the i-Vu® Pro system which will allow for optimized energy usage.
Integrated Alarm Management (page 11) *(onguard-alarms.addon)*	Facility staff and security staff can monitor each other's alarms so that either team can dispatch appropriate personnel regardless of who is currently on shift. It also enables OnGuard® Action Groups to initiate control of the i-Vu® Pro system equipment.
Integration Helper Files (page 11) *(OnGuardIntegrationHelper.zip)*	This zip file includes: • alarm-manager.logic-script – Snap script that is used to add configured alarm points to your program. • onguard-alarms.logicsymbol – Logicsymbol that is used by the script above. It includes a template for the microblocks to be added to your program.

See "Installing an Add-on User Guide" for more information on the following:

- Installing an add-on
- Applying a license
- Running an add-on
- Upgrading an add-on

Requirements

- Carrier i-Vu® Pro v7.0 or later system with the latest cumulative patch
- Carrier hardware, if your application requirements include running logic for the transference of data to or from the OnGuard® system
- OnGuard® system with Administrator privilege:
  - v7.5 or v7.6 ONLY, using OpenAccess interface - versions later then 7.6 are not certified compatible at this time
  - Appropriate license applied for OpenAccess (Please see Lenel® pricebook)
  - Single sign-on configured and enabled

- Building Integration Platform (v1.11) (see the Building Integration Platform's installation guide):
  - Building Integration Platform Service installed
  - OnGuard® Connector Service installed
  - Username, password, and port number for the Building Integration Platform
- Network connectivity between the i-Vu® Pro Server, OnGuard® server, and Building Integration Platform server

When upgrading to i-Vu® Pro v8.0

If you are running the OnGuard Integration with a pre-v8.0 version of i-Vu® Pro, perform the following steps when you upgrade to i-Vu® Pro v8.0:

1. During the upgrade to i-Vu® Pro v8.0, choose to keep your existing add-ons. Add-on configurations will be saved.
2. Uninstall Building Integration Platform (BIP) v1.10, following the instructions in the *Building Integration Platform Installation Manual*.
3. Install BIP v1.11, following the instructions in the *Building Integration Platform Installation Manual*.

Running the OnGuard add-ons with i-Vu® Pro v8.0 or later

When running the OnGuard add-ons with i-Vu® Pro v8.0 or later, it may appear that your server is using more memory than it should. This occurs because v8.0 uses a newer version of Java, and most of the memory it reports as used is actually free.

If you would like to see a more accurate report of memory usage, perform the steps below on your i-Vu® Pro server:

1. Go to the **i-Vu Pro<x.x>\bin\launchers** folder.
2. Open the **i-Vu Pro server.launch** file in Notepad.
3. Add this line: `cjgreen.monitoredapp.config.gcimpl=-XX:+UseParallelGC`
4. Save the file.
5. Open the **i-Vu Pro service.launch** file in Notepad.
6. Add the same line of text as above, and save the file.
7. Restart **i-Vu Pro**. Memory usage should now display as significantly lower.

BIP installation and configuration details

To enable communication between the WebCTRL and OnGuard servers, the Building Integration Platform (BIP) must be installed on a server that can connect to both application servers. Refer to the following documents to install and configure the BIP:

- *Building Integration Platform Installation Guidelines*
- *Building Integration Platform Commissioning User Manual*

The BIP is designed to support multiple integrations. This section describes the steps needed specifically for the OnGuard Integration.

BIP Installation

See the *Building Integration Platform Components* section of the *BIP Installation Manua*l for which BIP services must be installed for the OnGuard Integration. Follow the instructions in that document to install each of the indicated services.

BIP Configuration

Refer to the *BIP Commissioning User Manual* to perform the following steps:

1. Refer to the *BIP Commissioning Access* section to log in as the default web admin user using the default credentials, then change the password for the default web admin user.
2. To set up additional web admin users:
   a) If the new user will not be authenticated with Active Directory or Single Sign-On, refer to the *Local Database User Creation* section to create the user in the BIP database.
   b) Refer to the *User Management* section to register the user with the role Admin with Web Login.
3. Register your Lenel-OnGuard System
   a) Refer to the *System Configuration > Add System Configuration* section to add a system. Select "Lenel-OnGuard" as your **System Type**.
   b) Refer to the *Register Lenel-OnGuard System* sub-section to complete the registration.
4. The Configuring the Server section of this document explains how to connect to a BIP Resource. Refer to the *Resource Registration > Add Resource* section to create a BIP Resource for this purpose with:
   a) **Resource IDs**: aaa, dipservice
   b) **Grant Type**: service
   c) **Scopes**: read, write
   d) **Access Token Time**: 1 month

IT considerations

The following information may be useful to network administrators.

Client	Server	Default Port	Traffic
i-Vu Pro – OnGuard® Data Connector	Building Integration Platform	TCP/IP 8443*	Building Integration Platform Rest API secured with TLS 1.2
i-Vu Pro – OnGuard® Data Connector	Building Integration Platform OAuth Service Provider	TCP/IP 8444*	Building Integration Platform OAuth Rest API secured with TLS 1.2

* The Building Integration Platform server ports default to 8443 and 8444, but can be customized in the field.

Building Integration Platform

The OnGuard® Data Connector add-on communicates with OnGuard® Server via the Building Integration Platform.

The OnGuard® Data Connector communicates to the Building Integration Platform using REST and Server Sent Event technologies. The REST APIs are secured using TLS 1.2 and authenticated using a username/password that is configured in the Building Integration Platform. Credentials for the service account are stored to a file by this add-on and secured using AES-128 encryption. The Server Sent Events are only accessible through the REST APIs, so they are secured in a similar way.

Configuring the Server

1 On the **Server Configuration** tab, enter the OnGuard Connector settings. See table below.

2 To allow a Self Signed Certificate, check the checkbox. Note: Choosing this option will result in a less secure configuration, therefore should only be chosen when you are unable to use a certificate signed by a certificate authority.

NOTE Status indicates **Connected** if configured properly. If errors occurred, view the **Activity Log** (to the right) to help diagnose what may be preventing the connection from being established.

Field	Notes
Host	The Building Integration Platform server IP address.
Port	Port number for the Building Integration Platform service.
OAuth Host	IP address of the server that the Building Integration Platform OAuth service is running on.
OAuth Port	Port number for the Building Integration Platform OAuth service.
Client ID	Client ID of the Building Integration Platform Resource associated with this integration.
Password	Client Password of the Building Integration Platform Resource associated with this integration.

NOTE You must configure your Lenel® OnGuard system with the System Name "OnGuard". You can edit this field in the Building Integration Platform's **System Configuration** tab.

Setting up the Data Connector add-on

To track occupancy through the security system, you must define one or more zones.

NOTE For the purpose of this integration, a zone is a geographical area for which occupancy can be detected through the activity of its associated badge readers.

Adding a zone

1 On the **Occupancy** tab, enter a unique name for the new zone in the **Add New Zone** field.

2 Press **Enter** to add the new zone – it appears in the list of zones below.

NOTE To remove a zone from the list, click the **Delete** () button to the right of the zone name.

Setting zone properties

1 On the **Occupancy** tab, click the zone you wish to configure in the **Zone** list.

2 Click **Config** in the **Occupancy** panel.

3 Select a value for the **Full Occupancy Count** lertethe zone.

The zone is considered fully occupied when the occupancy count reaches this number.

4 Enter a time for the **Reset Time**.

The occupancy count is automatically cleared at this time each day to ensure that each day's occupancy tracking does not accumulate errors from the day before.

NOTE If the add-on is shut down at any time, the last known occupancy count is retained.

Exporting and clearing the prediction history

Prediction history can be exported to a .csv file which is named after a selected zone. Exporting the prediction history purges all but the most recent 30 entries from the **Prediction History** panel.

On the **Scheduling** tab, select the desired zone, then click the **Export Predictions** button in the **Prediction History** panel.

Associating microblocks with a zone

A control program can be designed to operate on zone occupancy data from the integration. Do this by associating microblocks in the control program as targets to receive the zone occupancy data. The microblocks are updated 1 minute after startup and every 5 minutes following that. There are four different microblocks that can be configured.

Microblock	Maps too...	And represents...
Occupancy Count	an AV microblock	how many people are currently badged into a zone.
Full Occupancy Count	an AV microblock	the number of people that would be considered 100% occupied.
Occupancy Percent	an AV microblock	the percentage of people in a zone based on the Occupancy Count/Full Occupancy Count.
Comm status	an MSV microblock	the communication status with the Building Integration Platform. MSV values must be configured in the microblock: 1=Comm Failed 2=Comm OK 3=Subscriptions Pending This value is updated both periodically and on change of value.

Auto-mapping with predetermined reference names

Use these predefined reference names in the equipment file:

Set this reference name...	to start with...	for this microblock type
Occupancy Count	onguard_occ	AV
Full Occupancy Count	onguard_full_occ	AV
Occupancy Percent	onguard_pct_occ	AV
Communication Status	onguard_comm_stat	MSV

1. On the **Occupancy** tab, click the zone you wish to configure in the **Zone** list.
2. Click **Microblocks** in the **Occupancy** panel.
3. When the **Equipment** panel appears, navigate the Equipment tree and select the equipment with the predefined reference names (see table above).
4. Drag the selected equipment from the tree to any slot in the **Microblocks** section.

NOTES

- All the predefined reference names will be assigned to the associated points. Depending on the system size, this operation may take a few seconds.
- To remove a microblock association, click the **Delete** () button to the right of the microblock name.

Manual mapping of reference names

1 On the **Occupancy** tab, click the zone you wish to configure in the **Zone** list.

2 Click **Microblocks** in the **Occupancy** panel.

3 When the **Equipment** panel appears, navigate the Equipment tree and select a microblock to associate.

4 Drag the selected microblock from the tree to the corresponding slot in the **Microblocks** section.

NOTE To remove a microblock association, click the **Delete** ( ) button to the right of the microblock name.

Associating badge readers with a zone

Each zone can be assigned entrance badge readers to detect how many people have badged into a zone. Each unique badge entry event increments the occupancy count for that zone. When the badge is detected in another zone the occupancy count is decremented in the original zone and incremented in the new zone.

NOTES

- If no readers are configured under an OnGuard® device panel, the OnGuard® device panel will not show up under **Peripheral Devices**.
- A badge reader can only be mapped to a single zone. Readers that are already mapped will be grayed out (disabled) in the **Peripheral Devices** panel.
- Use the electrical drawing to determine which Access Control Devices belong to which zone.

To associate a badge reader

1 On the **Occupancy** tab, click on the zone you wish to configure in the zone list.

2 Click **Associated Devices** in the **Occupancy** panel.

3 When the **Peripheral Devices** panel appears, select a reader to associate.

NOTE The items in the list are retrieved from the configuration of the connected OnGuard® system.

4 Drag the selected reader to the **Associated Devices** section.

NOTE To remove a reader association, click the **Delete** ( ) button to the right of the reader name.

Setting up the Advanced Occupancy Scheduling add-on

Advanced Occupancy Scheduling is an add-on that predicts and schedules occupancy based on past occupancy data. The schedule that is generated contains no undefined regions and the whole day is scheduled with off and on times. For example, a 9-5 schedule would be written with midnight to 9am as off, 9am-5pm as on and 5pm to midnight as off.

The Occupancy Schedule Optimizer algorithm provided with the algorithm schedules optimal building area operational schedules based on actual building usage patterns. This add-on compares security card logs to occupancy count information in user-defined areas and then schedules equipment based on the average time the area reaches a user-defined occupancy threshold.

The add-on functions by associating data by day of the week and maintaining rolling data sets of the last five occurrences. For example, the add-on schedules equipment on Monday based upon the usage patterns of the five most recent Mondays. This allows the algorithm to accommodate variations of occupancy among the different days of the week and adapt over time as usage patterns change.

The Occupancy Percentage parameter allows the user to define when the building is considered occupied for the purposes of scheduling using a percentage value. For example, for an area with full occupancy of 100 people, setting the parameter to 5% results equipment being scheduled ON when the algorithm predicts five or more occupants will be present. Increasing the parameter conserves energy by allowing a larger occupancy count to be considered unoccupied, with the converse true for reducing it.

Finally, the Occupancy Schedule Optimizer algorithm conducts continuous data quality checks to ensure that irregular occupancy events, such as holidays, do not impact the scheduling function. Any data that deviates significantly from the rolling data set is discarded when predicting schedules.

Setting scheduling properties of a zone

TIP For the scheduling properties described below, you must have either the **Start Time** or **Stop Time** set to **Predicted** before you can configure **Algorithm** or **Occupancy Percent**.

1. On the **Scheduling** tab, click on the zone you wish to configure in the **Zone** list.
2. Click on **Config** in the **Schedules** panel.
3. Set both the **Start Time** and **Stop Time** to either **Predicted** or **Fixed**; if Fixed, select a time.

   NOTE If **Predicted**, select an algorithm and a percent for occupancy.
4. Select an **Algorithm** from the droplist to use for the occupancy prediction.
5. Adjust the **Occupancy Percent** setting to modify how the selected algorithm predicts the start and stop time.

NOTE Use the **Reset All Occupancy Data** button (

) on the **Zone** panel to remove all data used by the occupancy schedule algorithm. The add-on must re-accumulate this data before the algorithm can make schedule predictions. Use this option after an extended period of unusual occupancy activity. For example, when a building has just come out of commissioning and is ready to start recording real occupancy data.

Associating schedulable items to a zone

1 On the **Scheduling** tab, click on zone you wish to configure in the **Zone** list.

2 Click on **Destinations** in the **Schedules** panel.

3 From the **Destination** panel, you can either add **Areas** and **Equipment** or **Scheduling Groups**:

- In the **Areas and Equipment** section of the **Destination** panel, drag the desired **Area** or **Equipment** to the **Destinations** section of the **Schedules** panel.
- In the **Scheduling Groups** section of the **Destination Panel**, drag and drop the scheduling group to the **Destinations** section of the **Schedules** panel.

NOTES:

- To remove a schedulable association, click the **Delete** () button to the right of the schedulable name.
- Toggle on and off the **Write Schedules** button () on the **Zone** panel to enable and disable the writing of predictions to system schedules.
- Use the **Export Predictions** button () in the **Prediction History** panel to export the prediction history to a .csv file named after the selected zone. Exporting the prediction history purges all but the most recent 30 entries from the **Prediction History** panel.

Setting up the Integrated Alarm Management add-on

Integrated Alarm Management is an add-on that enables the exchange of alarms between the i-Vu® Pro system and the OnGuard® system.

Setting up alarms from OnGuard to the i-Vu® Pro system

In order to send alarms from an OnGuard® system to the i-Vu® Pro system, you must define a mapping. The mapping describes the OnGuard® event source and the destination microblock which re-generates the alarm for the i-Vu® Pro system.

Adding an alarm mapping

1 On the **Alarms** tab, click **OnGuard to I-Vu Pro**.

2 Click the **Edit Events** button.

3 Click the **Add New Mapping** button.

4 In the **Mapping Configuration** panel, set the **OnGuard Source**:

a) Click the **Event Type** slot, then select a type from the available choices.

b) With the **Event Sub Type** slot now selected, select a sub-type.

5 In the **Mapping Configuration** panel, specify if this mapping should **Use Schedule**:

- **No** will always transfer alarms regardless of the schedule.
- **Yes** will only transfer alarms during the scheduled time range. See *Setting up the alarm transfer schedule* (page 14) for more information.

NOTES

- To remove a mapping, click the **Delete** (x) button to the right of the mapping.
- You can use an exported configuration to generate an equipment file containing your mapped alarm points. See **Exporting Zone Mapping** below. Alarm points will be given refnames as indicated in the **Refname Template** below.
- To add alarm points to an existing equipment file, locate the **I-Vu® Pro Destination** section on the **Mapping Configuration** panel to see the microblock refname template generated by the add-on. Use this template to construct a refname to be used in the equipment file to map this point to a BV microblock. See the refname template and example below.

RefnameTemplate: almbv_p<panel>_d<device>_type<type>_subtype<subtype>

All of the fields in <> above are numbers provided by the OnGuard system.

EXAMPLE: almbv_p1_d4_type4_subtype8

In this example, the alarm is from Panel 1, device 4, event type 4 (system), sub-event 8 (door forced open)

Adding Zone Mapping

Map the equipment files to the zones to receive OnGuard® events. Once the Zone Mapping is set up, any mapped OnGuard® events will be written to the mapped BV microblocks in the mapped Equipment file.

1 On the **Alarms** tab, click **OnGuard to i-Vu Pro**.

2 Click the **Edit Zones** button to open the **Zone Map** and **Equipment** panels.

3 Drag the equipment from the **Equipment** panel to the desired zone in the **Zone Map** panel.

NOTE To delete a zone's association with a piece of equipment, click the **Delete** () button to the right of the zone.

Exporting Zone Mapping

You can export a JSON configuration file that contains the current **OnGuard to i-Vu Pro** Events and Zones to be used with Snap to build equipment for the selected Alarm Mappings.

1 On the **Alarms** tab, click **OnGuard to i-Vu Pro**.

2 Click on the **Export** () button to download the current configuration file; this downloads an onguardmapping.json file.

Adding Alarm Manager Points to an equipment file

The JSON configuration file can be used in the Snap application to add the mapped points to an equipment file.

To add Snap Script to the Snap application:

1 In the Snap application add the "Scripts plug-in" (refer to Snap Help for this step).

2 In Snap select Tools>Scripts>Configure, then click **Add**.

3 Select the alarm-manager.logic-script from the onguard-integration.zip file.

4 Click **Ok**.

To add Snap Symbols:

1 Create a folder called "onguard_integration_helper" inside of <your_system_name>\extras\tools.

2 Select the onguardalarms.logic-symbol file from the onguard-integration.zip file; then move the file into the onguard_integration_helper folder created above.

To add OnGuard® Alarm Points to an equipment file:

Once the alarm-manager.logic-script and alarm-manager.logic symbol has been properly installed, OnGuard® Alarm points can be appended to existing equipment files with appropriate reference names.

1 Export the current Zone Mapping JSON configuration file (see Exporting Zone Mapping section above) and note where you download the onguardmapping.json file.

2 In Snap, open the equipment file that corresponds to the zone that you want to append the OnGuard® alarm points to.

3 Select Tools>Scripts>alarm-manager to open a script editor.

4 Press the **Execute** button in the script editor to run the script which will bring up a file dialog. Navigate to the onguardmapping.json file created in step 1.

5 Select the onguardmapping.json file and click **Open**.

6 From the drop-down list of available zones, select the zone that corresponds to your equipment file and click **Ok**. The Alarm Manager points are appended to the open equipment file.

7 Close the script editor.

NOTE If constructing an equipment file serving multiple zones, repeat steps 4 through 6 for different zone selections on the same equipment file.

Setting up alarms from the i-Vu® Pro system to OnGuard

In order to send alarms from the i-Vu® Pro system to the OnGuard® system, a source must be defined in the OnGuard® system to act as the originator of the alarms. There can be many sources defined for the i-Vu® Pro system to use, and each source can be configured to transfer i-Vu® Pro alarms by category.

The i-Vu® Pro alarms notifications that are sent to OnGuard® are:

- Alarm is generated
- Alarm is acknowledged
- Alarm point returned to normal

Setting up the alarm source

1 On the **Alarms** tab, click **System Select** > **i-Vu Pro to OnGuard**.

2 Select the **OnGuard Source** to configure.

3 Under the **Category** column to the right, select each alarm category to enable for that source.

4 Next to each alarm category, specify when it should transfer alarms:

- Select **No** to always transfer alarms regardless of the schedule.
- Select **Yes** to only transfer alarms during the scheduled time range. See *Setting up the alarm transfer schedule* (page 14) for more information.

Setting up the alarm transfer schedule

For items that you have selected **YES** for **Use Schedule**, you must specify the alarm transfer schedule. The transfer schedule time range applies to both **OnGuard to i-Vu Pro** and **i-Vu Pro to OnGuard** alarms.

On the **Alarms** tab, set the following from the **System Select** column in the **Schedule** section:

Start Time - to start sending alarms

Stop Time - to stop sending alarms

Troubleshooting

If the connection is not successful and you receive an error message in the Activity Log panel, see the table below.

Error message	Solution
Error reading system Id, No active system named OnGuard	Make sure your Lenel® OnGuard system is configured with the System Name "OnGuard". You can edit this field in the Building Integration Platform's **System Configuration** tab.
Error authenticating with DIP	Check **Allow Self Signed Certificate**. If using a signed certificate, uncheck after the connection is established. If using a self-signed certificate, leave it checked.

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
7/28/22	Requirements	Updated version requirements	AC-PM-LO-O-LO

* For internal use only

Security Best Practices

for an i-Vu® Pro v8.0 system

 • Catalog No. 11-808-848-01 • 6/21/2022

 Verify that you have the most current version of this document from **www.hvacpartners.com**, the **Carrier Partner Community** website, or your local Carrier office.

Important changes are listed in **Document revision history** at the end of this document.

Contents

Security best practices

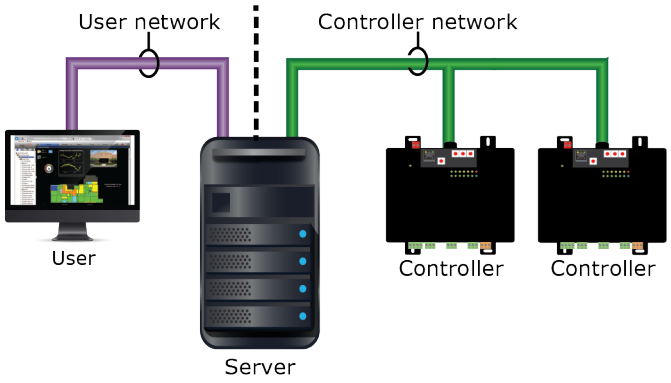
Carrier takes the security of our systems very seriously and you play the biggest part in this by installing and configuring systems in a secure manner. We encourage you to establish security policies for your own company networks and all the systems you install and service.

Follow the best practices in this document when deploying i-Vu® Pro building automation systems.

Use the Security Checklist in Appendix B to track important security steps when designing, installing and commissioning i-Vu® Pro systems.

Network separation

Standard BACnet is an intentionally open system that makes it easy to discover and control any device on its network. Because of this, you should design your system to segregate users from the controller network by having two separate networks. For example, if the users are on a company's enterprise LAN, you would not want controllers on the LAN so that they are easy targets for misuse by anyone with access. Some of the biggest risks come from insiders such as the curious tinkerer, a student on an education system's network, or a disgruntled employee.



You can physically separate the user network and the BACnet network without any IP routing between them, or you can logically separate them at a switch using a Virtual Local Area Network (VLAN).

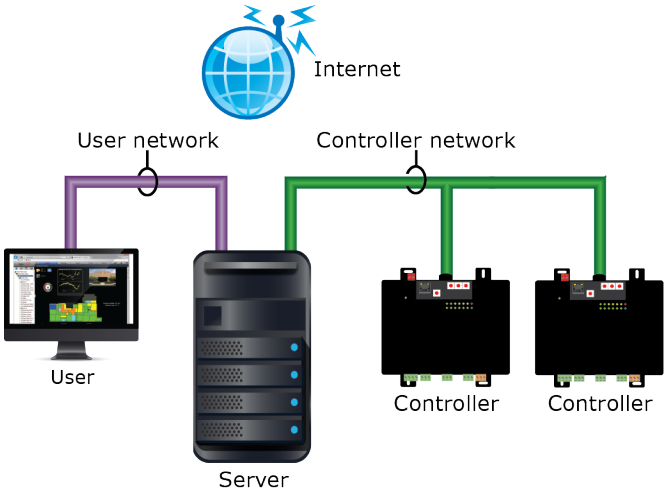
If you have dual NICs (Network Interface Cards), the i-Vu® Pro server must have a different IP address for each network:

- User network - Configure this IP address and subnet mask in SiteBuilder on the **Configure** > **Preferences** > **Web Server** tab.
- BACnet network - Configure this IP address and subnet mask in the i-Vu® Pro interface on the **Driver Properties** > **Connections** page > **Configure** tab.

Internet connectivity scenarios

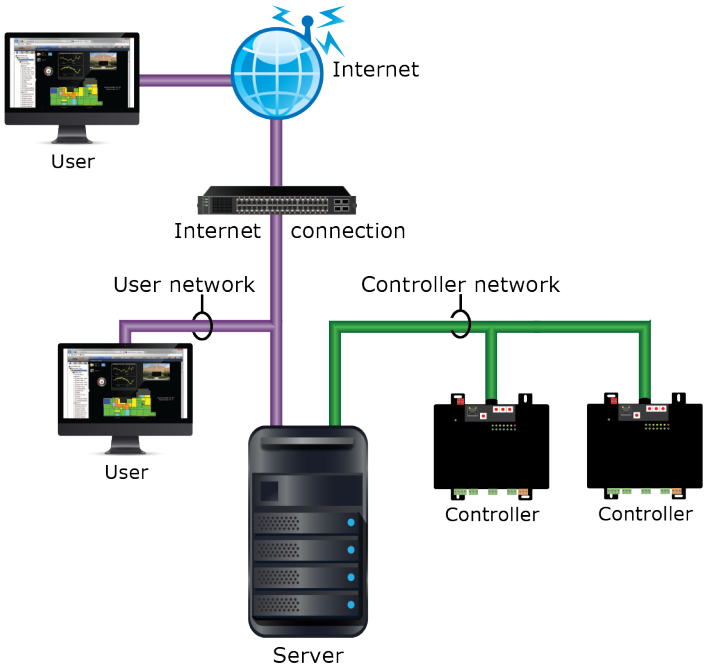
The i-Vu® Pro system's connection to the Internet may vary greatly based on the client's needs and IT capabilities. The following possible network scenarios are listed in order of DECREASING security.

Scenario A: Isolated Network - Low risk



Do not permanently expose the i-Vu® Pro server or the BACnet network to the Internet. You can, however, allow users to access the i-Vu® Pro server through a secure VPN connection. If a NAT router or firewall is present on the LAN for other purposes, it should not have any ports forwarded to the i-Vu® Pro server or any controllers.

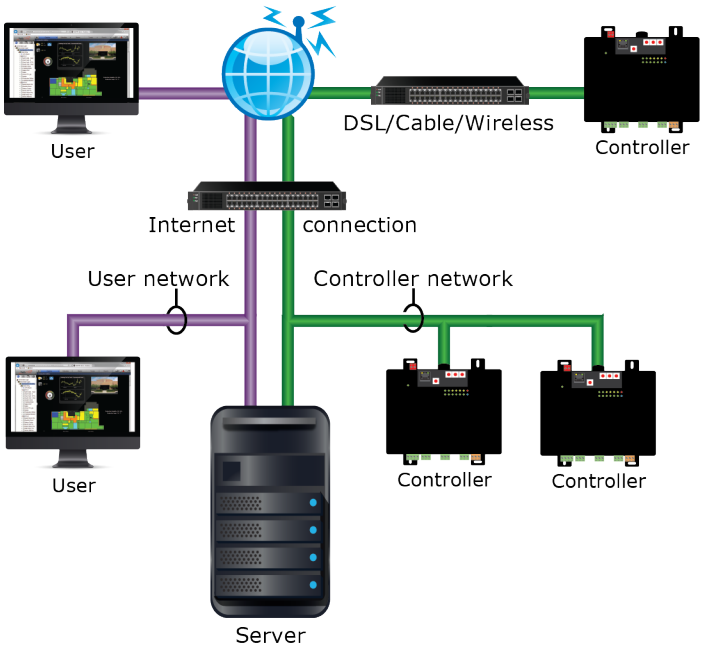
Scenario B: Public Users - Medium risk



It is acceptable to permanently expose the i-Vu® Pro server on the Internet as long as:

- The BACnet network is not exposed.
- The NAT/Firewall device exposing the i-Vu® Pro system exposes only TCP ports 80 and 443 on the i-Vu® Pro server.
- BACnet traffic on UDP port 47808 is not exposed.

Scenario C: Public Users with Distributed BACnet - High risk



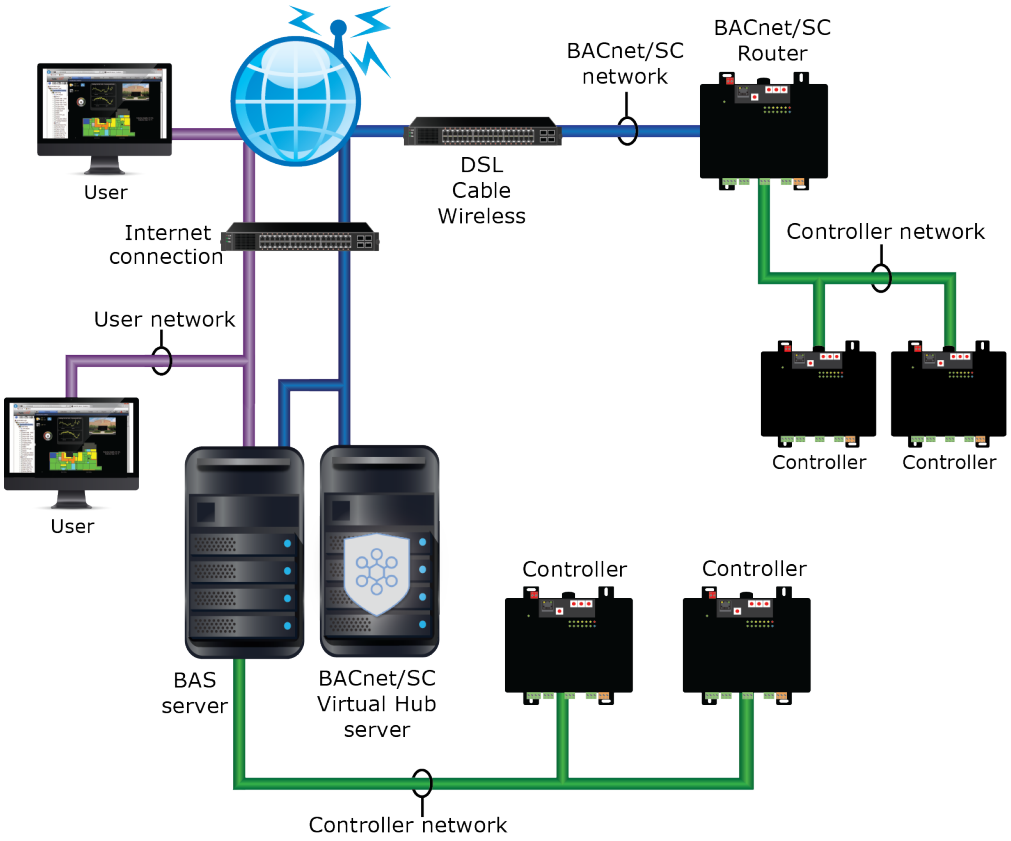
In this configuration, both users and BACnet controllers use a public network/Internet. Carefully plan this configuration to maximize security.

If the i-Vu® Pro server must connect to multiple sites over the Internet, connect them using a VPN to form a Wide Area Network that is secure (changing this to Scenario A).

If this is not possible, use the *BACnet Firewall feature* (page 6) in Ethernet-capable controllers, or protect controllers with a whitelist that your IT department can configure in each Internet connection device where the network connects to the Internet. The whitelist allows communication with your i-Vu® Pro system only from devices whose public IP addresses are in the list. Often, the only address controllers need to talk to is the i-Vu® Pro server. The i-Vu® Pro server firewall's whitelist will have to include the public address of all remote IP controllers.

DO NOT connect BACnet controllers to the Internet without at least whitelist protection! If you do, they could easily be discovered and modified by anyone on the Internet. If a BACnet router is connected to the Internet without protection, then the entire network connected to it is accessible.

Scenario D: Public Users with Distributed BACnet/SC - Low risk



BACnet Secure Connect, or BACnet/SC, is an industry standard way of securing BACnet communications over the internet without the need for VPNs. A BACnet/SC network consists of multiple nodes connecting through a central hub. This hub can be located on premises or hosted on the Internet. The figure above depicts the BACnet/SC Hub installed on premises.

Network firewall

Limit the ports opened through any firewall or NAT port forwarding to the minimum ports required. The i-Vu® Pro system uses the following ports:

Port	Transfer	Protocol/User	Use
80 (default)	TCP	HTTP (Web server)	Client/Server
443 (default)	TCP	HTTPS (Web server)	Client/Server
443 (default)	TCP	WSS (secure WebSocket for BACnet/SC)	Client
47806 (default)	TCP	Alarm Notification Client	Client/Server

Port	Transfer	Protocol/User	Use
47808	UDP	BACnet/IP	Server/i-Vu router
47808	TCP	Diagnostic Telnet *	Client/Server
47812	UDP	CCN/IP	i-Vu CCN router/Server
50005 50007 50008	UDP	CCN/IP	Server/i-Vu CCN router
50005 - 50008	UDP	Firmware CCN/IP	CCN router to CCN router

* This functionality is off by default. You can start it using the `telnetd` console command.

Scenarios B or C in the previous section require TCP ports 80 and 443 to be exposed to the Internet for user access.

Scenario C also requires UDP port 47808 to be exposed for both the server and the controller's firewall. If you do this, you MUST use a whitelist to limit connectivity.

Scenario D may require configuration of an outgoing port for BACnet/SC traffic and/or an incoming port protecting a BACnet/SC Hub.

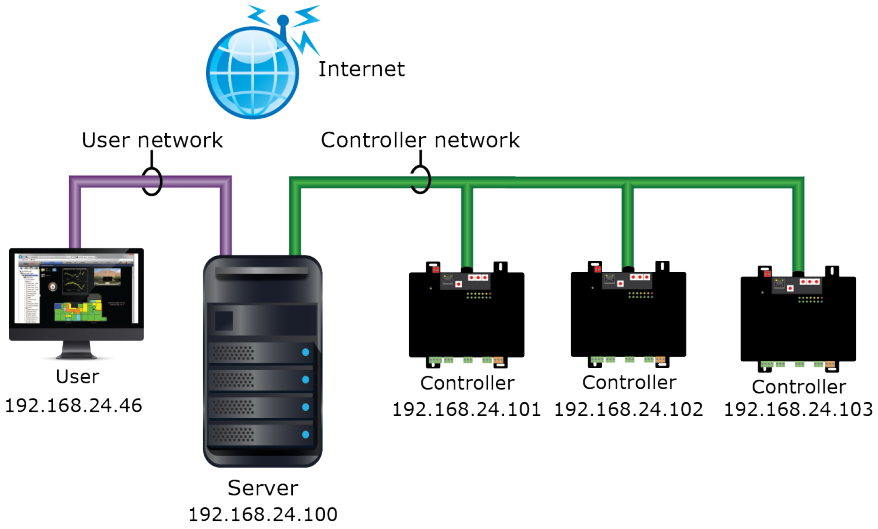
BACnet firewall

The v6-02 drivers for Carrier controllers with Ethernet capability have a BACnet firewall feature that allows you to restrict BACnet/IP communication with the controller to all private IP addresses and/or to a whitelist of IP addresses that you define. This feature provides another layer of security for your system.

The following are examples of use cases for the BACnet firewall and instructions for setting it up.

Case 1: Isolated network

While an isolated network is secure from threats on the Internet, other users or devices on the local network can potentially interfere with controllers.



In this example, each controller's BACnet firewall should allow BACnet communication from the i-Vu® Pro server's IP address and the controller's IP addresses. The user at 192.168.24.46 should not be allowed BACnet communication with the controllers.

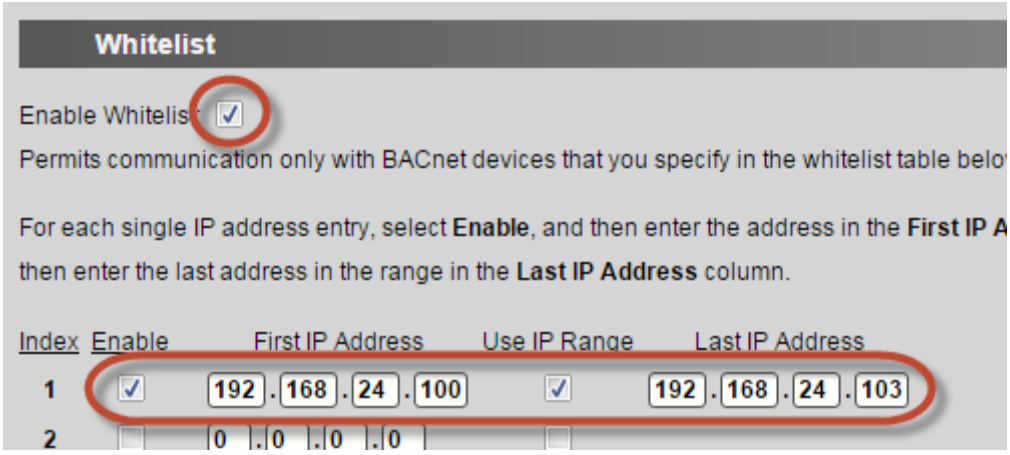
The server and controllers addresses fall within the private IP address range of 192.168.0.0 to 192.168.255.255, but restricting BACnet communication to all private IP addresses is not sufficient since that would allow communication from the user. So a whitelist must be created in the BACnet firewall.

To set up the BACnet firewall:

1. In the i-Vu® Pro interface, right-click each controller and select **Driver Properties**.
2. Select **BACnet Firewall** > **Properties** tab.
3. Check **Enable BACnet firewall**.
4. Uncheck **Allow All Private IP Addresses**.

5 Check **Enable Whitelist**.

6 On the first row, check **Enable**, check **Use IP Range**, and then enter the address range 192.168.24.100 through 192.168.24.103.



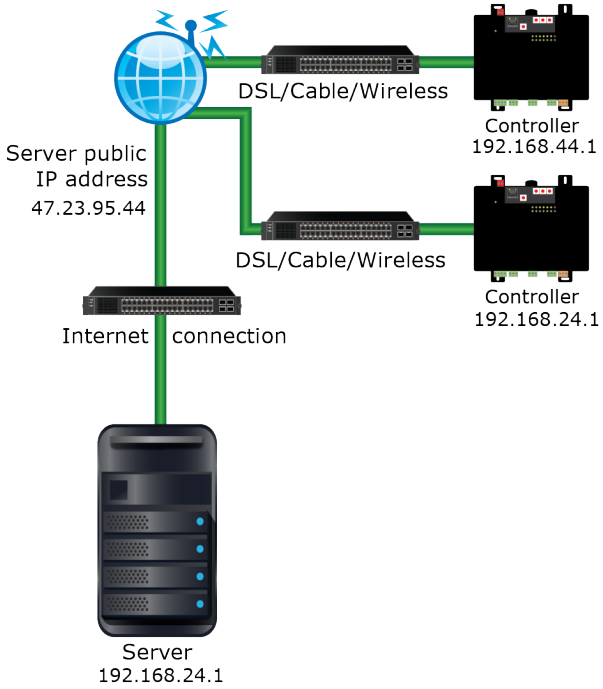
7 Click **Accept**.

8 Wait for the page to update, and then check **Confirm firewall settings**.

NOTE In this example, the server and controllers IP addresses are sequential so the whitelist could have an address range. If you anticipate future controller expansion, reserve extra sequential addresses so that you can simply expand the range in the BACnet firewall settings. If the IP addresses are not sequential, you must enter each IP address on a separate line and check **Enable**.

Case 2: Individual controllers exposed to the Internet

Controllers that are accessible on the Internet (for example, behind a DSL, cable, or wireless device) may not be protected by a network firewall or whitelist. This may be due to the network firewall's lack of capability or difficulty in setting it up.



In this example, each controller needs to communicate with only the i-Vu® Pro server so their BACnet firewall's whitelist should have only the server's public IP address. The controllers do not need to communicate with each other.

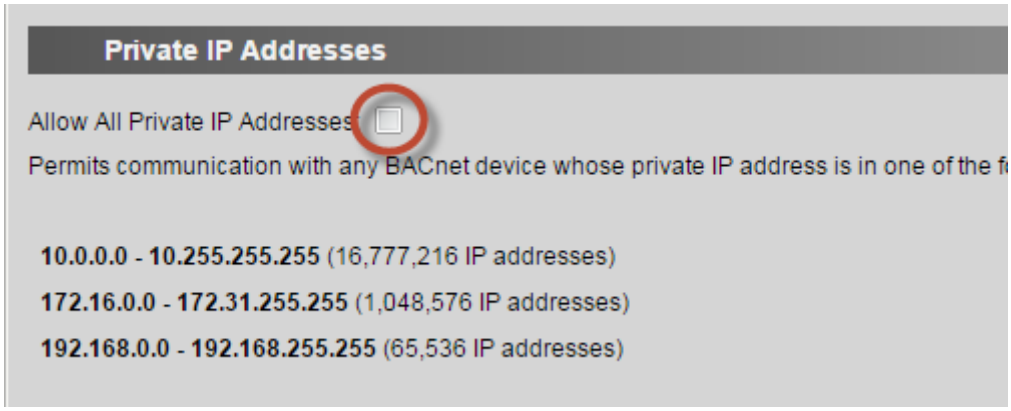
To set up the BACnet firewall:

1 In the i-Vu® Pro interface, right-click each controller and select **Driver Properties**.

2 Select **BACnet Firewall** > **Properties** tab.

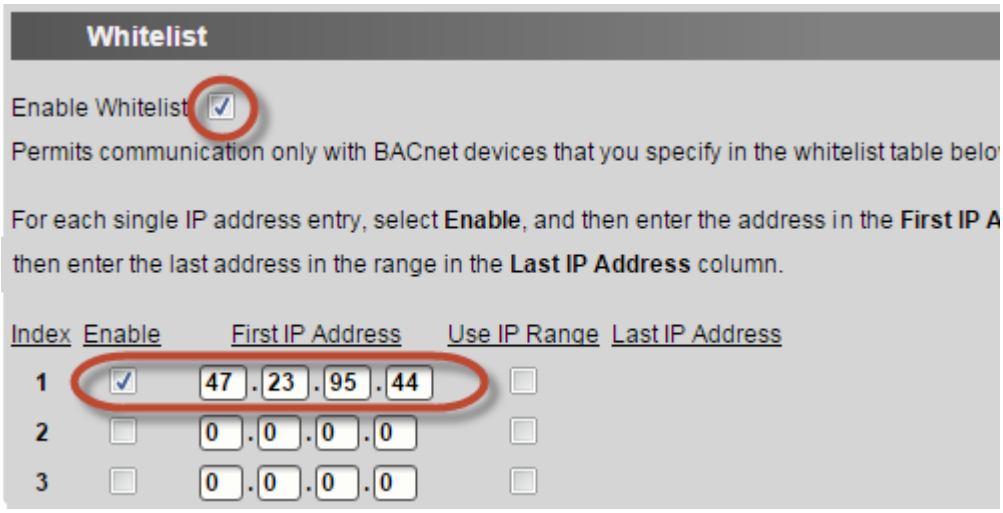
3 Check **Enable BACnet firewall**.

4 Uncheck **Allow All Private IP Addresses**.



5 Check **Enable Whitelist**.

6 On the first row, check **Enable**, and then enter the address 47.23.95.44.

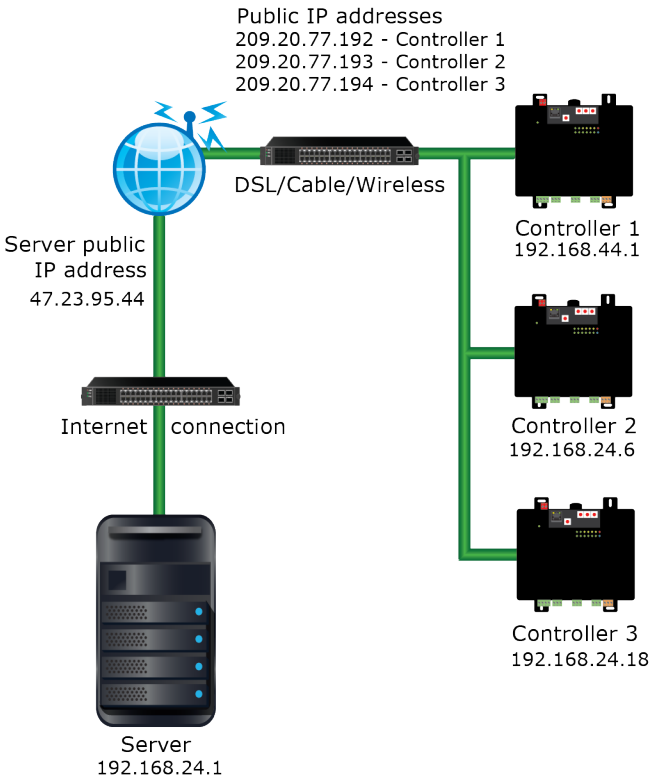


7 Click **Accept**.

8 Wait for the page to update, and then check **Confirm firewall settings**.

Case 3: Multiple controllers exposed to the Internet at one site

Multiple controllers that are accessible on the Internet (for example, behind a DSL, cable, or wireless device) may not be protected by a network firewall or whitelist. The controllers have private IP addresses, but it is their public IP addresses that are exposed to the Internet.



In this example, the controllers need to communicate with the i-Vu® Pro server and each other. The controllers are the only devices on the site's private network, or other devices present are benign.

Each controller's BACnet firewall should allow BACnet communication with the i-Vu® Pro server's public IP address and with all private IP addresses so that the controllers can communicate with each other. The BACnet firewall prevents BACnet communication to the controller's public addresses.

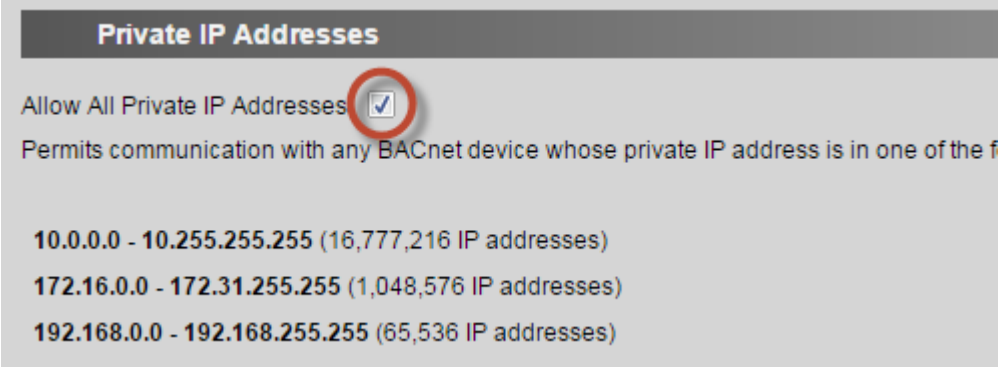
To set up the BACnet firewall:

1 In the i-Vu® Pro interface, right-click each controller and select **Driver Properties**.

2 Select **BACnet Firewall** > **Properties** tab.

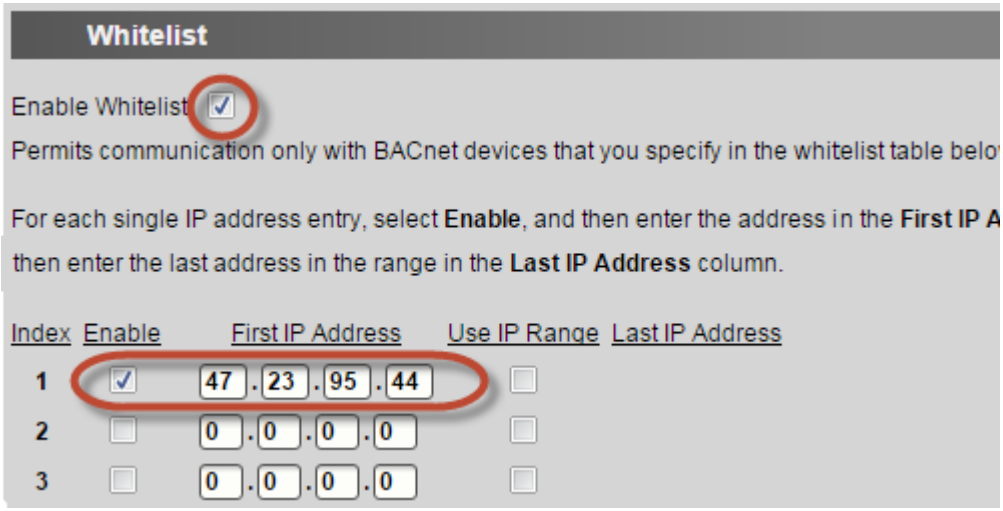
3 Check **Enable BACnet firewall**.

4 Check **Allow All Private IP Addresses**.



5 Check **Enable Whitelist**.

6 On the first row, check **Enable**, and then enter the address 47.23.95.44.



7 Click **Accept**.

8 Wait for the page to update, and then check **Confirm firewall settings**.

Users

Follow the guidelines below to limit unauthorized user access.

- **Administrator account**—A system has a default Administrator user. If you upgraded from a pre-v6.5 system, change the Administrator's login name and add a password. DO NOT leave the password blank. DO NOT use the same password for multiple systems.
  NOTE When you create a new system in v6.5, you will be required to change the name and add a password.
- **Anonymous account**—A pre-v6.5 system had a default Anonymous user that required no user name or password. If you have not upgraded to v6.5, delete this user.
  NOTE The Anonymous user was removed from i-Vu® Pro v6.5.
- **Advanced password policy**—Enable the advanced password policy and require a minimum password length of at least 8 characters. This will disallow blank passwords.
- **No shared accounts**—Create a different account for each user. DO NOT create role-based accounts where multiple users log in with the same login name and password.
- **Delete old accounts**—Manage accounts when people no longer need access to the i-Vu® Pro system. Delete their account or change their password.
- **Auto Logoff**—Verify that **Log off operators after __ (HH:MM) of inactivity** is checked on the **System Settings** > **Security** tab.
  NOTE You can disable this for an individual user (for example, an account for a monitoring center).
- **Lock out users**—Verify that **Lock out operators for __ minutes after __ failed login attempts** is checked.
- **Location-dependent security**—Consider using the optional location-dependent security policy. For large systems with many users, you can restrict users to only the locations they should have access to.

i-Vu Pro server

Follow the guidelines below to protect the i-Vu Pro server.

- **Patches**—Keep the i-Vu Pro system and the operating system up-to-date with the latest patches.
- **Anti-virus protection—**Keep the i-Vu Pro server's anti-virus software and definitions up-to-date.
- **Single-use server**—i-Vu Pro software should be the only application running on the server. DO NOT put other applications on the same server.
- **HTTPS—**Use https:// with a certificate signed by a standard certificate authority, when possible. If using a self-signed certificate, install the server certificate on the client computers so users do not develop the bad habit of ignoring the "unsafe certificate" error.
- **Remote access**—After commissioning, uncheck **Allow remote file management** on the **System Settings** > **Security** tab.
- **Device Password**- This password is only available on systems with one or more controllers with the Gen_5 driver. Setting the **Device Password** as described in the *i-Vu® Pro v8.0 Help* provides an additional level of security.

Database server

Follow the database server vendor's best practices for a secure installation. This should include steps such as changing default accounts and passwords.

Configure the database server to accept connections only from the i-Vu® Pro system. Most database servers have a whitelist mechanism to facilitate this.

Device-specific security

Devices with a drv_gen5 driver support the following device-specific security options.

- Configure the security settings on all service ports, as described in the *Adjusting driver properties and controller setup through the Service Port* section of your devices technical instructions.
- Network Time Protocol (NTP) - NTP provides a more secure means of keeping a device's clock in sync.

Appendix A: Glossary

BAS—A Building Automation System is a collection of BACnet and/or CCN devices, the i-Vu Pro server, and the network(s) they reside on.

LAN—A Local Area Network is a computer network that interconnects computers/devices within a limited area such as an office building.

Firewall—A device that restricts network traffic. Firewall functionality is often combined with IP Router functionality in a single device. A firewall is configured with rules to define what kind of traffic is allowed or blocked. Personal computers and servers have firewall functionality built into them.

IP router—An IP (Internet Protocol) device that connects two or more IP networks. Typically an IP router connects a local network to the larger enterprise/Internet network.

NAT router—An IP router that remaps IP addresses from one network to one or more IP addresses on another network. A NAT router is commonly used to connect devices on a private network to the Internet or enterprise network, and it often has firewall and port forwarding capabilities.

Port—A port is a 16 bit (0-65535) number associated with an IP address that defines an endpoint of a computer network connection. There are two types of ports, TCP and UDP. BACnet uses a UDP port. HTTP, HTTPS and Alarm Notification Client use TCP ports. To manage access to a port in a firewall, you must know its number and type.

Private IP address—An IP address in one of the following ranges:
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

VLAN—A Virtual Local Area Network is partitioned and isolated by the IP network switch (or router). It is typically as effective as physically separating the network.

VPN—A Virtual Private Network is a method for extending a private network across a public network, such as the Internet. A VPN enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and they benefit from the functionality, security and management policies of the private network.

Whitelist—A list of IP addresses that are the only ones allowed through a firewall. Advanced firewall devices can have different whitelists for a given port or protocol.

Appendix B: Security checklist

Designing and Planning

- ☐ Separate user and BACnet networks either physically or with a VLAN.
- ☐ Determine the appropriate Internet connection scenario. See Internet connectivity scenarios.
- ☐ Use BACnet/SC when possible. BACnet/SC encrypts BACnet communications over the network to prevent information disclosure and supports device authentication to prevent spoofing.

Installing

If you have dual NICs:

- ☐ Enter the i-Vu Pro user network IP address and subnet mask in SiteBuilder on the **Configure** > **Preferences** > **Web Server** tab .
- ☐ Enter the i-Vu Pro BACnet network IP address and subnet mask in the i-Vu Pro interface on the **Connections** page > **Configure** tab.

If using Internet connectivity scenario A:

- ☐ Verify that IP addresses for the i-Vu Pro server and controllers are in one of the private IP address ranges.

If using Internet connectivity scenario B:

- ☐ Verify that controller IP addresses are in one of the private IP address ranges.
- ☐ Verify that the NAT router or firewall exposing the i-Vu Pro server only exposes TCP ports 80 and/or 443.

If using Internet connectivity scenario C:

- ☐ Verify that the NAT router or firewall exposing the i-Vu Pro server only exposes TCP ports 80 and/or 443, and UDP port 47808.
- ☐ Verify that each NAT router or firewall used (for both the server and each controller) has been configured with an appropriate whitelist of allowed IP addresses in your Internet connection device, or each controller is protected by its internal BACnet firewall feature.
- ☐ Test the whitelist protection from the Internet. Use a separate i-Vu Pro server on a public network by using a modstat like "modstat mac:0,b:1.2.3.4". Confirm you cannot access any of the system's controllers.
- ☐ Change the Administrator login name and add a password.
- ☐ If you are running a pre-v6.5 system, remove the Anonymous user account.
- ☐ Verify that the i-Vu Pro server's anti-virus software is up-to-date and is set to update automatically.
- ☐ Configure the database server to accept connections only from the i-Vu Pro application using a whitelist.

After Commissioning

☐ Enable the Advanced password policy and set the minimum password length to at least 8 characters.

On the **System Options** > **System Settings** > **Security** tab, verify that:

☐ **Allow remote file management** is not checked

☐ **Log off operators after __ (HH:MM) of inactivity** is checked

☐ **Lock out operators for __ minutes after __ failed login attempts** is checked

On SiteBuilder's **Configure** > **Preferences** > **Web Server** tab, verify that the following are not checked:

Any **TLS Level** below "TLS 1.3"

☐ **Allow SOAP applications over HTTP**

☐ **Allow unsigned add-ons**

☐

☐ Disable access to device service ports (drv_gen5 devices only). See the Configuration Access section of the device's security driver page.

☐ Use NTP (drv_gen5 devices only) rather than BACnet timesync to keep the device's clock in sync.

System Maintenance

☐ Install the latest software updates to keep the system current with the most recent security enhancements.

To quickly check security measures in place

In the i-Vu® Pro interface, use the Manual Command **sreview** to view your system's critical security compliance. These settings are described in more detail in the document above.

The **sreview** report displays the following:

Web Server	Possible responses	Recommendation for the most secure system
SSL Mode	**on**, **off**, or **both**	**on**
TLS in use	**on** or **off**	**true** (when SSL Mode is **on** or **both**)
TLS protocol	Version number	**TLS 1.3**
Allow unsigned add-ons	**true** or **false**	**false**
Allow SOAP over HTTP	**true** or **false**	**false**
Reads X-Forwarded-For Header	**true** or **false**	**false**

Certificate	Possible responses	Recommendation for the most secure system
Self-signed certificate in use	**true** or **false**	false
Certificate issued by	Distinguished Name of the certificate signer	certificate information, not a setting
Certificate expired	**true** or **false**	certificate information, not a setting
Certificate not yet valid	**true** or **false**	certificate information, not a setting
Certificate expires	date and time the certificate becomes invalid	certificate information, not a setting

	Possible responses	Recommendation for the most secure system
Email		
Secure SMTP enabled on email server	**true** or **false**	**true**
Passwords		
Password policy enforced	**true** or **false**	**true**
Software Updates		
Latest cumulative update applied: none or date	**none** or **date**	Keep the i-Vu® Pro system and the operating system up-to-date with the latest patches.

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
6/21/22	Device specific security	New section	X-PM-RB-R
	i-Vu® Pro server	Added note about Device Password	
	Security checklist	Added content about drv_gen5	
8/2/21	Internet Connectivity Scenarios	Added Scenario D	X-PM-LO-O
	Network Firewall	Added a row for BACnet/SC, note for Scenario D	X-PM-LO-O
	All network graphics	Graphics updated to show i-Vu® XT or TruVu™ controllers	D
4/12/21		Corrected Carrier catalog number	D

* For internal use only