ALERTON

VAV and Unitary Controllers

SECURITY GUIDE

DISCLAIMER **2**

INTRODUCTION **3**
Related Security documents 3

SYSTEM DELIVERY **4**
Documentation contains security information 4
Ensure device packaging is in good state 4

SYSTEM OVERVIEW **5**

PLANNING AND INSTALLATION **7**
Physical equipment 7
Compass Planning and Installation 7
Connect Communications Bus and Microset (VAV and Unitary Controllers) 7
Recommended VAV and Unitary Controller Installation Configuration 8
Documentation 9

CONFIGURING A VAV OR UNITARY CONTROLLERS **10**
Control traffic from other subnets 10
Create and maintain a baseline of Controller Configurations 10
Change Default Passwords 10
BLE Password Configuration 10
Compass Configurations 11
About Microset Field Service Mode 11
Considerations for the BAS firewall 12

SECURITY RECOMMENDATIONS FOR USE OF A VAV AND UNITARY **13**
Monitor physical access controls 13
Monitor Paired BLE Mobile Device 13
Monitor network access controls 13
Monitor Compass control access 13
About DDC Logic considerations and disclaimer 13

SECURITY RECOMMENDATIONS FOR MAINTENANCE OF THE VAV AND UNITARY **14**
Compass Workstation Maintenance 14
Update to latest ROC 14
Updating the ROC in Device Manager (VAV and Unitary) 14

SECURITY RECOMMENDATIONS FOR DECOMISSIONING OF THE VAV AND UNITARY **15**
Reset Alerton VAV and Unitary to factory defaults 15

INSTALLATION SECURITY CHECKLIST **16**
Complete the following security tasks for each installed Controller 16
Train end users on documented security maintenance tasks 16

® U.S. Registered Trademark

DISCLAIMER

While we have engaged in efforts to assure the accuracy of this document, Alerton is not responsible for any damages, including consequential damages arising from the application or use of the information contained herein. The information and specifications published here are current at the time of publication and are subject to change without notice. For the latest product specifications please visit our website or contact our corporate office.

Alerton

715 Peachtree Street NE

Atlanta, Georgia 30308

www.alerton.com

INTRODUCTION

This guide contains information on the safe installation and configuration of Alerton VAV and Unitary controllers and safety-related information on operation, maintenance, and decommissioning.
(Models: **VAVi-7u5-IP**, **VAVi-7u5-IP-BLE, VAVi-0-IP, VLC8u8-IP, VLC8u8-IP-BLE, VLC16u8-IP and VLC16u8-IP-BLE**).

Please take some time to read and understand all relevant installation, configuration, and operating manuals and ensure that you regularly obtain the latest versions.

Related Security documents

The table below shows the relationships of other Alerton security manuals:

Document	Description
Compass Dealer Security Guide (LT-SEC-DG-CMPS)	Provides security-related instructions for planning, installing, and configuring a compass system. The intended audience is an Alerton dealer.
Compass End-User Security Guide (LT-SEC-EUG-CMPS)	Provides security-related instructions for maintaining and decommissioning a compass system. The intended audience is the compass system owner and end-user.
ACM Dealer Security Guide (LT-SEC-DG-ACM)	Provides security-related instructions for planning, installing, and configuring an ACM. The intended audience is an Alerton dealer.
ACM End User Security Guide (LT-SEC-EUG-ACM)	Provides security-related instructions for maintaining and decommissioning an ACM. The intended audience is the compass system owner and end-user.
VIP Dealer Security Guide (31-00300)	Provides security-related instructions for planning, installing, and configuring an VIP. The intended audience is an Alerton dealer.
VIP End User Security Guide (31-00301)	Provides security-related instructions for maintaining and decommissioning an VIP. The intended audience is the compass system owner and end-user.

SYSTEM DELIVERY

This section includes activities needed when the Building Management System (BAS) is delivered to the system owner.

Documentation contains security information

The documentation package delivered with your system should include the following:

- Manual
- Controller settings, including network parameters.
- Network settings, especially configurations that isolate the BAS/BACnet® Network and other networks.
- Firewall settings, such as ports that are allowed through, are especially important for maintaining the designed security protections.
- Physical security controls, such as locked cabinets or equipment rooms, restrict physical access to VAV and Unitary Controllers.

Ensure device packaging is in good state.

Inspect that the packaging of the VAV and Unitary modules is intact and not opened, and know that it has not been tampered with en-route.

SYSTEM OVERVIEW

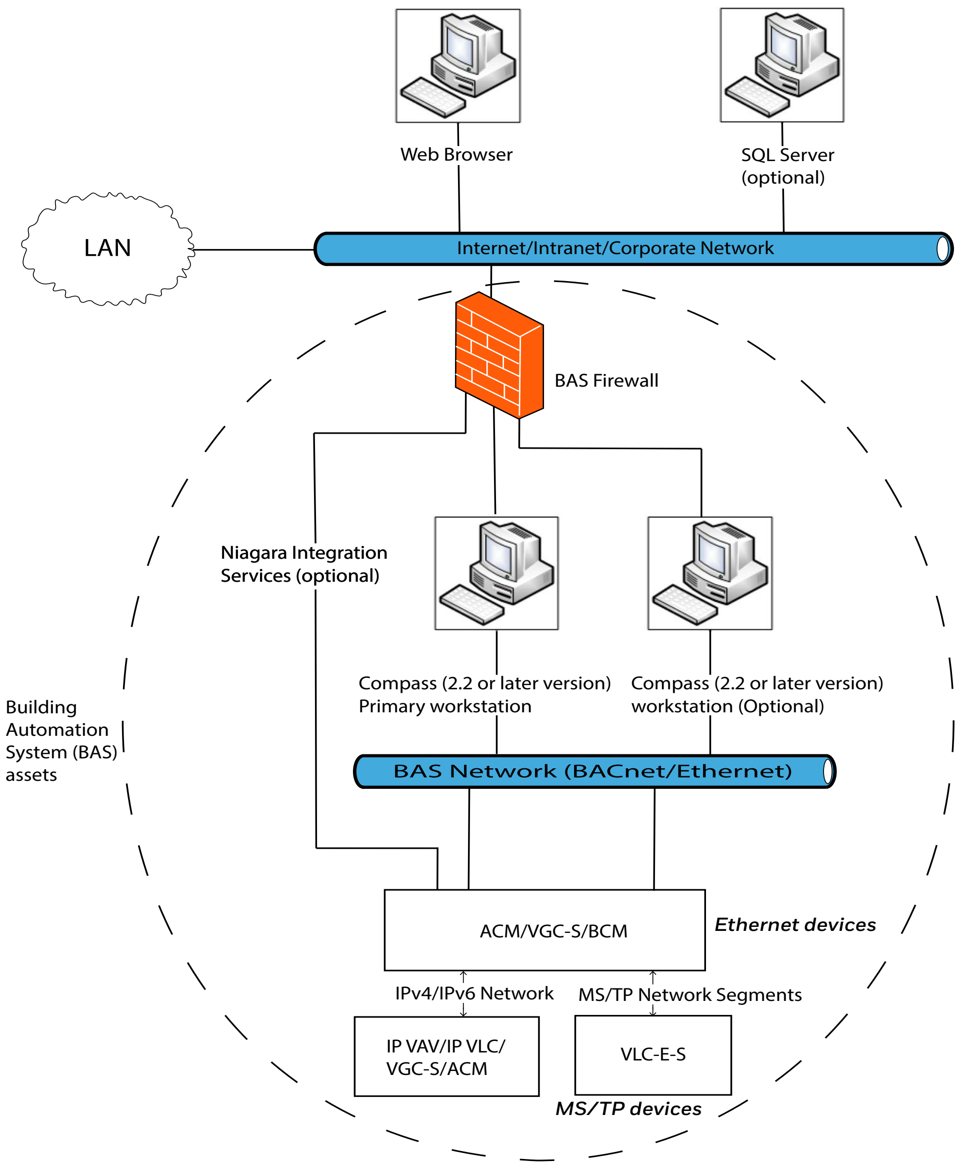

Web Browser
SQL Server (optional)
LAN
Internet/Intranet/Corporate Network
BAS Firewall
Niagara Integration Services (optional)
Compass (2.2 or later version) Primary workstation
Compass (2.2 or later version) workstation (Optional)
Building Automation System (BAS) assets
BAS Network (BACnet/Ethernet)
ACM/VGC-S/BCM
Ethernet devices
IPv4/IPv6 Network
MS/TP Network Segments
IP VAV/IP VLC/ VGC-S/ACM
VLC-E-S
MS/TP devices

Fig. 1 Graphical description of recommended network topology in a global scope

The key elements of the system overview are:

Internet/Intranet/Corporate Network: This is a simplified, logical representation of all networks outside the Building Automation System (BAS) scope. It may provide access to the BAS management interfaces (e.g., the compass primary workstation web user interface). Still, it must give access to the internet so that compass computers can check for and download operating system and virus scanner updates unless other means are provided.

BAS Network: This network is used solely for BAS protocols, which consist of BACnet®/IP, BACnet®/ Ethernet, and any protocols that a VAV and Unitary controller might use. It must not be the same network as the Internet/intranet/corporate network.

BMS Firewall: To provide additional separation and protection to the BAS, use a firewall between the Internet/intranet/corporate network and any BAS device that connects to it, such as the Compass primary workstation, Compass workstations, VAV, and Unitary controllers.

Compass Primary Workstation: The Compass primary workstation is a computer running software. It requires two network connections: one to the management web user interface through a web browser (usually on the Internet/intranet/corporate network) and another to the BAS network.

Web Browser: Compass software provides a web-based management interface that can be accessed through a web browser without a connection to the Internet.

Compass Workstation (optional): If access to the compass primary workstation's thick client interface is not allowed, install a compass workstation on a separate computer to access thick client functionality. For example, if the compass primary workstation is run on a virtual machine as a service or console, access to it is not permitted.

SQL Server (optional): Compass software can be configured to use an external SQL server.

PLANNING AND INSTALLATION

This section includes information for planning and performing a VAV and Unitary controller installation.

Physical equipment

When planning a system installation, it is essential to discuss the physical security of VAV and Unitary controllers with your customer. This discussion should assess the security needs of all Alerton VAV and Unitary IP components and the system owner's requirements and provide suggestions for best practices if the system owner still needs to have their own requirements.

Controlling physical access to Compass workstations, VAV and Unitary controllers, and network equipment is a fundamental security control that must be implemented on all installations. This can range from locating network equipment and controllers in locked rooms or cabinets to using an active access control system that logs access. (As for any log, an access log is only effective if it is monitored and audited regularly).

Compass Planning and Installation

Compass planning and installation security information can be found in the Compass Dealer Security Guide (LT-SEC-DG-CMPS).

Connect Communications Bus and Microset (VAV and Unitary Controllers)

It is required that physical security access to the controllers (VAV and Unitary) connect communications bus and wall module bus wiring be accomplished by:

1. Installing wiring in physically inaccessible locations that restricts physical access to the controller connect communications bus.
2. Or installing wire in conduit.

Physical security access protection is essential to prevent security threats to the control system. Failure to protect the controller connect communication bus and Microset bus can lead to critical security issues. For example, data loss or corruption could result from not following the required protection for the controller connect communication bus.

Modbus Connections Communication Bus Best practices (VAV and Unitary Controllers)

The security of the bus also means that it is electrically reliable for communications. It is important that the bus is installed with one wire type consistent throughout the whole gateway to controller connection to eliminate reflections from bus wire impedance mismatches. Shielded wire is not recommended for normal installations.

Recommended VAV and Unitary Controller Installation Configuration

The following section illustrates the recommended VAV and Unitary installation configuration. Note that the VAV and Unitary have a two-port Ethernet switch. The diagram below (Figure 2) uses the switch functionality to daisy-chain multiple VAV and Unitary controllers.

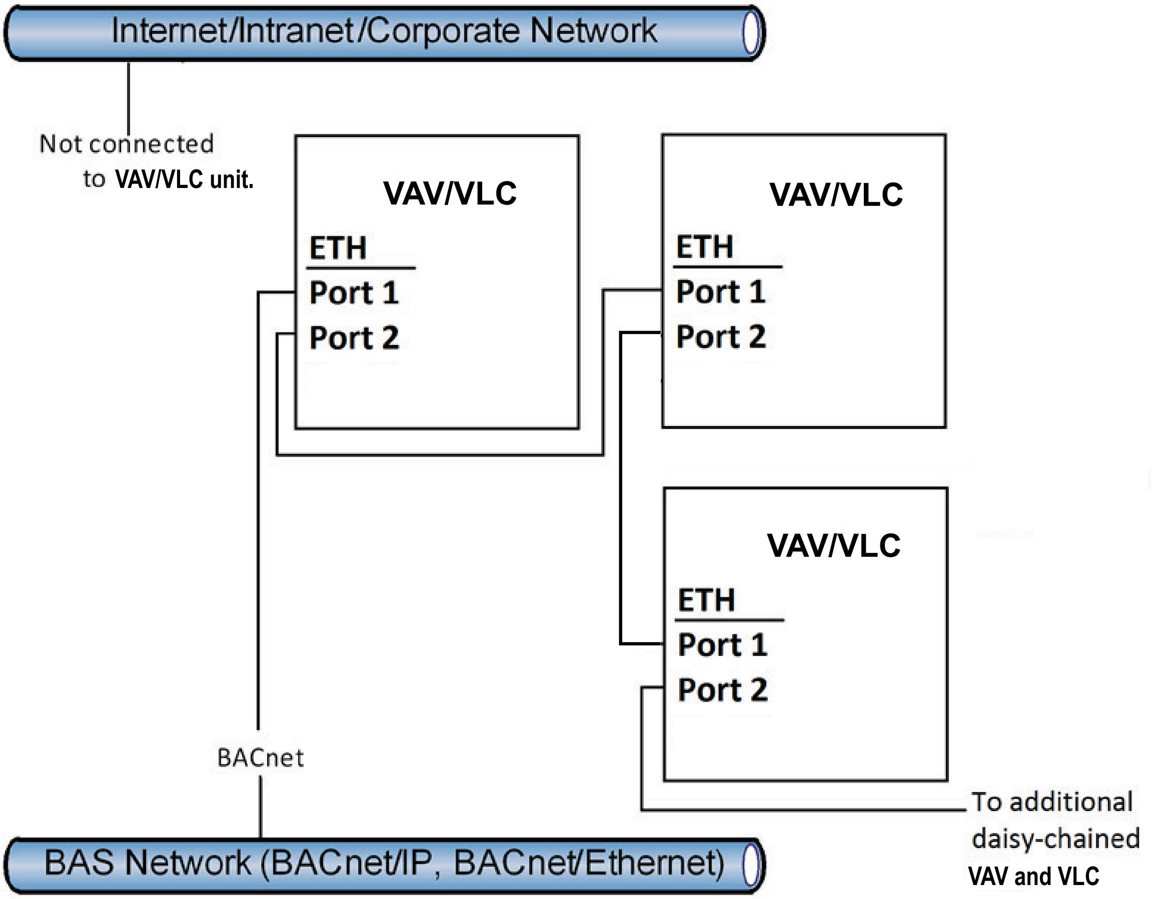


Fig. 2 Graphical description of the recommended VAV and Unitary controller connection in daisy chain.

Segregate and Protect Networks

Alerton recommends the following to secure and protect networks:

Use a separate dedicated physical network (e.g., separate wires) or virtual network (e.g., VLANs) for BACnet® communication. This network must be separate from the Internet/intranet/corporate network; a firewall can be used with special considerations.

Apply a tamper-evident sticker over the controller access panel.

If a customer needs additional assurance that the physical access protecting a VAV and Unitary has not been entered, install a tamper-evident seal or sticker over the access point or use a door switch on the panel connected to an input of the VAV and Unitary to provide an alarm.

Documentation

Documentation is essential in capturing design and configuring information required to maintain a secure system.

Document physical devices and configurations, including key security-related information.

All documentation on devices and configurations must include security-related information to establish and maintain the intended security controls. For example, if changes are made to the default services or ports on the VAV and Unitary, document these so that the settings can be restored at a later date.

Make sure important files for the configuration and operation of the VAV and Unitary unit are stored and safeguarded. Edition or replacement of the files shall be controlled by adding at least one layer of security where machine admin log information, like admin user and password, is required.

Some of these critical files are:

- PointData.mdb: used for Bacnet object configuration.
- DDC.vsdx or DDC.bd9 and its variants: used for the application logic.
- Trendlogbuilder.xlsx or calendarbuilder.xlsx: used to create trendlogs and calendars.
- DCF file: this file is used for configuration of the device.

Document external systems, especially interaction between the VAV, Unitary and its related systems

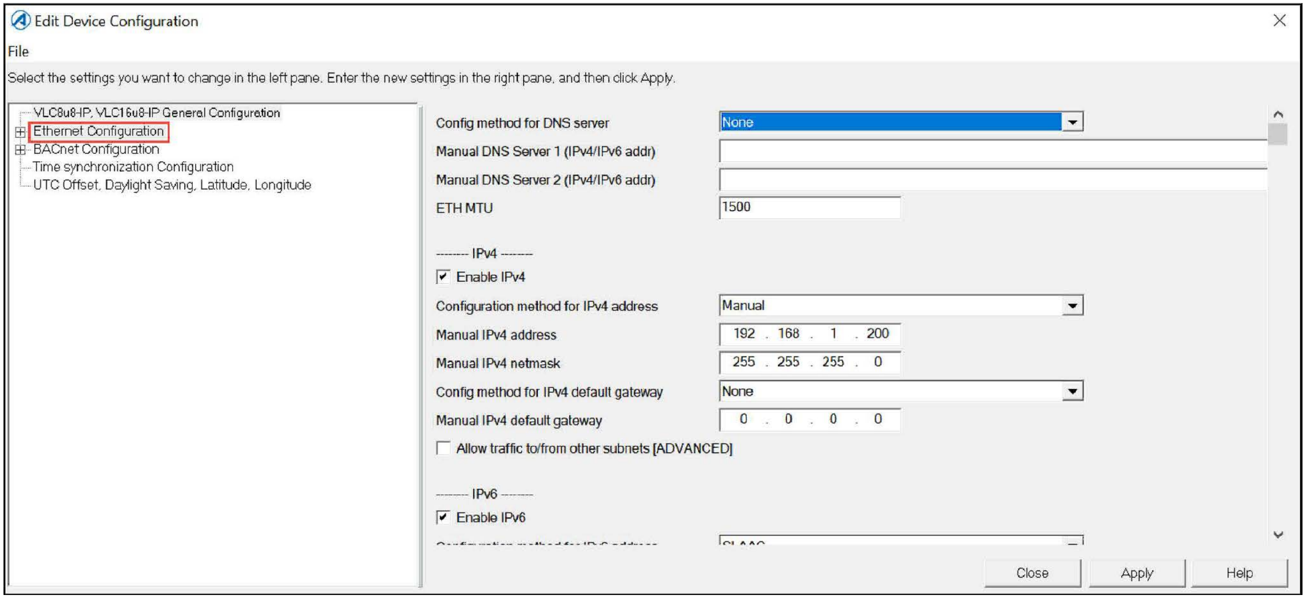
The BAS commonly requires or utilizes external systems functionally, such as network infrastructure, VPN access, virtual machine hosts, and firewalls. If the BAS requires those systems to be configured in a certain way for security, such as a firewall allowing or denying specific ports or a network allowing access to particular systems, you must document this information. If these systems need to be restored at some point in the future, e.g., due to equipment failure, or changes need to be made to the external systems, e.g., upgrading a firewall, documenting this information will help you restore the previous security level.

CONFIGURING A VAV OR UNITARY CONTROLLERS

This section contains information for configuring a VAV and Unitary Controllers.

Control traffic from other subnets

It is recommended that traffic to/from other subnets be permanently disabled. For security reasons, traffic to/from other subnets is disabled by default, preventing devices from other subnets from reaching this device.



Edit Device Configuration

Select the settings you want to change in the left pane. Enter the new settings in the right pane, and then click Apply.

Config method for DNS server: None
Manual DNS Server 1 (IPv4/IPv6 addr):
Manual DNS Server 2 (IPv4/IPv6 addr):
ETH MTU: 1500

-------- IPv4 --------
☑ Enable IPv4
Configuration method for IPv4 address: Manual
Manual IPv4 address: 192 . 168 . 1 . 200
Manual IPv4 netmask: 255 . 255 . 255 . 0
Config method for IPv4 default gateway: None
Manual IPv4 default gateway: 0 . 0 . 0 . 0
□ Allow traffic to/from other subnets [ADVANCED]

-------- IPv6 --------
☑ Enable IPv6

File
VLC8u8-IP, VLC16u8-IP General Configuration
Ethernet Configuration
BACnet Configuration
Time synchronization Configuration
UTC Offset, Daylight Saving, Latitude, Longitude
Close
Apply
Help

Fig. 3 Ethernet Configuration

Create and maintain a baseline of Controller Configurations

Create and maintain a baseline of VAV and Unitary configurations correctly configured for security. Ensure that this baseline also includes DCF files. Do not commit insecure configurations to the baseline to prevent inadvertently applying them in the future. Update any relevant documentation when configurations change.

Change Default Passwords.

There is no default password for Backup/Restore/Restart. Users who do not set up passwords for these features are effectively disabled.

Even with reasonable password strength requirements, some passwords are stronger than others. It is essential to educate users on password strength. More than password strength requirements are required to ensure strong passwords are used. For example, Password10 satisfies all the requirements but is a weak and easily hackable password.

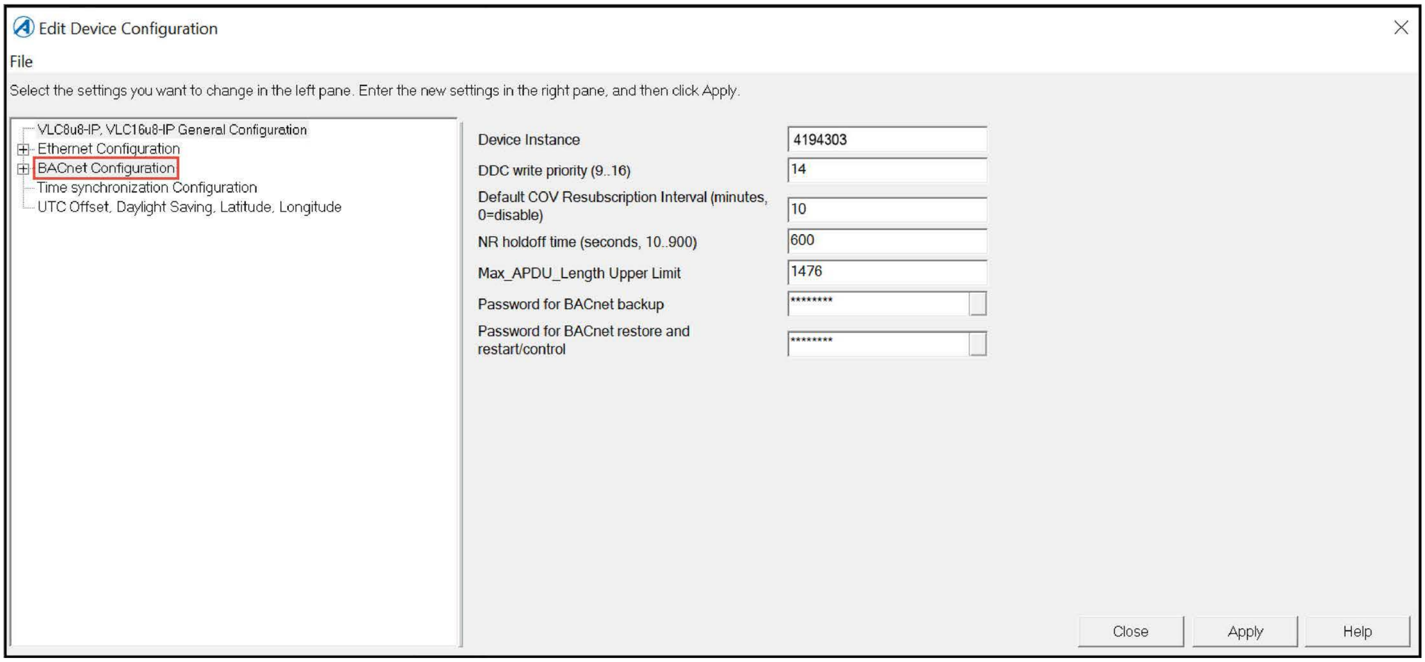
BLE Password Configuration

If not in use it is always advice to disable BLE communications from the DCF.

BLE Configuration allows an 8-character PIN password for pairing authorization and further communication. A strong password is recommended since unauthorized access could modify critical values used in airflow calculations and harm the system and other connected controllers. See the installation and operation guide for Alerton VAV and Unitary for more instructions on how to configure the BLE password.

Changing the backup and Restore/Restart/Control Passwords

To change the backup or restore/restart/control passwords, use Compass to edit the VAV and Unitary configuration.



Select the settings you want to change in the left pane. Enter the new settings in the right pane, and then click Apply.

- VLC8u8-IP, VLC16u8-IP General Configuration
- Ethernet Configuration
- BACnet Configuration
- Time synchronization Configuration
- UTC Offset, Daylight Saving, Latitude, Longitude

Device Instance	4194303
DDC write priority (9..16)	14
Default COV Resubscription Interval (minutes, 0=disable)	10
NR holdoff time (seconds, 10..900)	600
Max_APDU_Length Upper Limit	1476
Password for BACnet backup	********
Password for BACnet restore and restart/control	********

Fig. 4 BACnet Configuration

One password specifically for BACnet® Backup and another password for Restore/Restart/Control. Both passwords are stored as hashed values in the DCF.

> **IMPORTANT!** The backup/restore/restart/control password should differ from passwords used for any other purpose. It is OK to use the same backup/restore/restart/control password for multiple devices, provided the password is safe. It should not be the same password used for user login to any service, including the VAV and Unitary configuration screens.

Compass Configurations

Compass security considerations for its configurations is detailed in Compass 2.2.0 End User – section: "Installation, Configuration and system delivery".

Basic security measure to consider:

- Compass must be configured to use HTTPS even on a private network.
- Extra care must be taken to protect the SQL server system if configured.

About Microset Field Service Mode

It is highly recommended that a connected Microset 4 device has a configured password to prevent unsupervised access to field service mode. In normal circumstances, this mode allows technicians to query and adjust the system's key operating settings, but without prevention, it could allow unsupervised actions with potentially harmful consequences.

Also, the Microset 4 device has the capacity not to allow Field Service mode after the airflow balancing process has finished.

For Microset 4 detailed information and instructions, see Microset 4 Installation & Operations Guide - Service Mode section.

For (Legacy) Microset 2 (which does not count with a password feature), it is recommended to secure the file that contains steps involved in getting access to this mode; these instructions are in the file named Field-Service-and-Balance-Modes-from-LTBT-TM-MSET2-rev0003.

Considerations for the BAS firewall

These next considerations assume that the installation process has followed the network recommended configuration guidelines stated Fig. 2, located in the “Recommended VAV and VLC Installation Configuration” section, in which we are using a firewall to isolate the BAS network from the internet or the corporate network.

Important points regarding UDP port.

- Every BAS unit in the network uses this port for data transmission.
- It is highly recommended that the default port value for UDP (47808) be changed; this is important for automatic cyberattack prevention.
- An installed firewall that successfully isolates the BAS network should not allow UDP traffic flow to the Internet/intranet or any other network. Failure to ensure this could mean that any unsupervised personnel connected to the non-isolated network would have access to unencrypted BACnet® messages by connecting a sniffer.

Important points regarding NTP port.

- This port is used for Time Synchronization from Network Time Server.
- It is not critical to manually change the port default value (100).
- NTP data flow should not be allowed to flow through the BAS firewall. Failure to ensure this could mean that any unsupervised personnel connected to the non-isolated network would have access to unencrypted NTP messages by connecting a sniffer or potentially injecting malicious messages into the network.
- It is recommended that the NTP server be on the same subnet.

The following table summarize information stated above:

Table 1 Configuration BAS Fairwall

Default Port/Protocol	Purpose	Change from Default?	Allow Through BAS Firewall?
47808/UDP	BACnet®/IPv4 network connection	Yes	No
47808/UDPv6	BACnet®/IPv6 Network connection	Yes	No
100/NTP Server	Time Synchronization from Network Time Server.	No	No

SECURITY RECOMMENDATIONS FOR USE OF A VAV AND UNITARY

Monitor physical access controls.

Monitor the physical access control of the VAV and Unitary, such as monitoring the room where they are installed, installing a sensor on the cabinet, or instituting a process for checking out the key to the cabinet where they are mounted. Monitor for unauthorized access.

Monitor Paired BLE Mobile Device.

Monitor physical access to the mobile device, do not save the password on auto loggers, and do not leave an open session after finishing working with the mobile device, which could allow unauthorized access to the app connected to the controller network.

Monitor network access controls.

Monitor firewalls and any other network access controls for unauthorized changes or access. Please consult your specific firewall documentation for more information about its monitoring and logging facilities.

Monitor Compass control access.

The end user should monitor the room where the Compass Primary Workstation is located. Supervise login credentials access and the number of permits those hold. Renew passwords, and do not leave Compass sessions opened if the logged-in session owner is not present.

About DDC Logic considerations and disclaimer.

The end user should prefer not to send custom DDC applications created by someone other than an Authorized Alerton Dealer. The end user should use and secure the DDC logic delivered along the system, save it in a higher-edit administration rights directory, and supervise the last edit every time there is a need to resend the file to the VAV and Unitary controllers.

SECURITY RECOMMENDATIONS FOR MAINTENANCE OF THE VAV AND UNITARY

Compass Workstation Maintenance

Ensure Compass Workstation runs up-to-date virus software and complies with corporate PC security standards. It should also have the last Compass version available, which could include solutions to already-found vulnerabilities and updated third-party libraries; overall, stronger versions in cybersecurity are incrementally delivered. See Compass End-User Security Guide (LT-SEC-EUG-CMPS) documentation for more information on updating its libraries and software.

Update to latest ROC

New ROC files are released regularly and may include security fixes and enhancements. If your dealer does not provide these updates as part of a maintenance agreement, you must periodically monitor for updates and apply them.

Updating the ROC in Device Manager (VAV and Unitary)

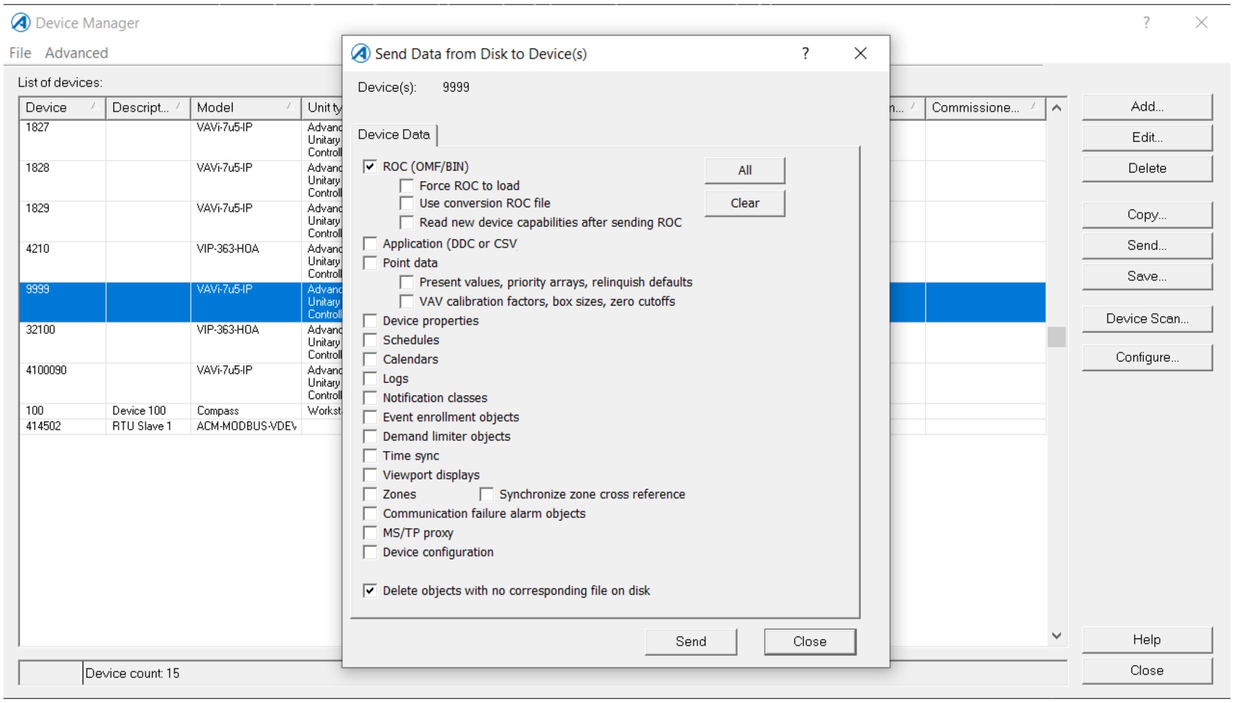
Use the Device Scan feature in Device Manager to scan the network for the VAV and Unitary and save the information to the Device Manager Table. This is an easy way to ensure the VAV and Unitary are communicating. A device record for the VAV and Unitary must exist in Device Manager for you to view and change VAV and Unitary values using Compass. The device record stores set-up information about the VAV and Unitary. An accurate device record is a key to managing DDC, ROC files, and automation features.

Once a device record exists, use Device Manager to send and read data from the VAV and Unitary. For more information about how Device Manager works, see the Compass Installation and Upgrade Guide.

NOTE:

Only add the device record to the Device Manager when the VAV and Unitary do not already exist in the Device Manager table. If the VAV and Unitary exist in Device Manager, save them to the table when Device Properties are sent. Doing so will delete Device Profile parameters.

- Make sure your Compass installation has the most recent VAV and Unitary ROC file.
- Use Compass Device Manager to send the ROC file to the VAV and Unitary. Open Device Manager > select the device(s) > click Send > (check on ROC box) > Send.



List of devices:

Device	Descript...	Model	Unit ty
1827		VAVi-7u5-IP	Advanc Unitary Controll
1828		VAVi-7u5-IP	Advanc Unitary Controll
1829		VAVi-7u5-IP	Advanc Unitary Controll
4210		VIP-363-HOA	Advanc Unitary Controll
9999		VAVi-7u5-IP	Advanc Unitary Controll
32100		VIP-363-HOA	Advanc Unitary Controll
4100090		VAVi-7u5-IP	Advanc Unitary Controll
100	Device 100	Compass	Workst
414502	RTU Slave 1	ACM-MODBUS-VDEV	

n... Commissione...

Device count: 15

Device(s): 9999

- ☑ ROC (OMF/BIN)
  - ☐ Force ROC to load
  - ☐ Use conversion ROC file
  - ☐ Read new device capabilities after sending ROC
- ☐ Application (DDC or CSV
- ☐ Point data
  - ☐ Present values, priority arrays, relinquish defaults
  - ☐ VAV calibration factors, box sizes, zero cutoffs
- ☐ Device properties
- ☐ Schedules
- ☐ Calendars
- ☐ Logs
- ☐ Notification classes
- ☐ Event enrollment objects
- ☐ Demand limiter objects
- ☐ Time sync
- ☐ Viewport displays
- ☐ Zones ☐ Synchronize zone cross reference
- ☐ Communication failure alarm objects
- ☐ MS/TP proxy
- ☐ Device configuration

☑ Delete objects with no corresponding file on disk

Fig. 5 Send Data from Disk to Device(s)

SECURITY RECOMMENDATIONS FOR DECOMISSIONING OF THE VAV AND UNITARY

This section contains information for decommissioning an Alerton VAV and Unitary.

Reset Alerton VAV and Unitary to factory defaults.

Resetting the Alerton VAV/VLC to factory defaults will erase all data stored in its configuration. For more information on how to reset the VAV IP to factory defaults, see Alerton VAV IP Controller_Installation and Operations Guide_ 31-0531-02.pdf and Alerton VLC Unitary Controller - Installation & Operations Guide - 31-00738.

INSTALLATION SECURITY CHECKLIST

Device Instance:

Description:

Location:

Installer: Date:

Complete the following security tasks for each installed Controller:

(**YES/NO**) Design a secure installation considering both software and hardware vulnerabilities.

(**YES/NO**) Develop a Disaster and Recovery Plan documenting configurations important for the network security and integrity.

(**YES/NO**) Install a firewall between the Building Automation System (BAS) and external network, securely configure both the firewall and network.

(**YES/NO**) Physically secure the controller and Compass Workstation in a place with restricted access.

(**YES/NO**) Set a password for the next features:

1. Backup password
2. Restore/Restart/Control password.
3. Microset Field Service Mode Password. (if installed)

(**YES/NO**) Disable Microset Communication port if it is not being used.

(**YES/NO**) Provide all required data to the BAS system owner at delivery.

Train end users on documented security maintenance tasks

This manual provides instructions on security maintenance task for the VAV and Unitary modules, but additional system level tasks also need to be documented. End users should be trained in these tasks:

- Firmware Download process.
- Compass Update Process.
- User should be conscious of the right measures to safeguard files mentioned on Documentation section.

Documents should be delivered along the system, but end user can always find these an other documents on https://buildings.honeywell.com

ALERTON

715 Peachtree Street NE
Atlanta, Georgia 30308
www.alerton.com

ALERTON
Smarter Buildings Start Here