COMPASS 2

End User Security Guide

ALERTON
COMPASS 2

CONTENTS

User Agreement And Limited Warranty

IMPORTANT - PURCHASE OF ALERTON PRODUCTS OR USE OF SOFTWARE, FIRMWARE AND / OR ACCOMPANYING DOCUMENTATION (DEFINED BELOW) IS SUBJECT TO LICENSE RESTRICTIONS AND LIMITED WARRANTY. CAREFULLY READ THIS AGREEMENT BEFORE USING ALERTON PRODUCTS, SOFTWARE, FIRMWARE AND/OR DOCUMENTATION.

This is a legal "Agreement," concerning the purchase of Products and use of Software, Firmware and/or Documentation, between you, the "User" (either individually or as an authorized representative of the company that is purchasing, has purchased, or is using the Products, Software, Firmware or Documentation) and Honeywell, 715, Peachtree street NE, Atlanta, GA, 30308 USA. ("Honeywell").

PURCHASE OF ALERTON PRODUCTS OR USE OF SOFTWARE, FIRMWARE AND / OR ACCOMPANYING DOCUMENTATION INDICATES USER'S COMPLETE AND UNCONDITIONAL ACCEPTANCE OF THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT.

Honeywell provides Alerton products ("Products"), software programs ("Software"), firmware, e.g., protocols, software program code, device drivers and related hardware ("Firmware") and accompanying documentation ("Documentation") and grants a non-exclusive and non-transferable license ("License") to User to use the Software and the Firmware only on the following terms and conditions. Taken together, Products, licensed Software, licensed Firmware, and accompanying Documentation are collectively defined as "Alerton Product(s)" in this Agreement.

1. Copyright. The Software, Firmware, and Documentation are copyrighted and protected by United States copyright laws and international treaty provisions and laws, contain valuable proprietary products, information, and trade secrets, and shall remain the property of Honeywell. User may not and shall not copy or otherwise reproduce or make available to any other party any part or all of the Software, Firmware or Documentation nor decompile, disassemble, reverse engineer, manufacture or modify any portion of the Products, Software, Firmware, Documentation or any portion of the same for any purpose or otherwise attempt to determine the underlying source code of the Software or Firmware or permit any such action; provided however, User may either (a) make one (1) copy of the Software solely for backup or archival purposes, or (b) transfer one (1) image of the Software to a single hard disk, CD or other comparable media, provided User keeps the original solely for backup or archival purposes.

2. License. User is hereby licensed to use one (1) copy of the Software for User's own use in operating the Products. User may not rent, lease or otherwise assign or transfer all or any part of the Software, Firmware, or Documentation. In addition, User may not sublicense, assign or transfer this License or Agreement, or any part thereof. Any attempt to do so shall terminate this License and User's right to use the Software and Firmware and shall subject User to liability for damages to Honeywell. LICENSING TO USER OF THE SOFTWARE AND FIRMWARE COMMENCES WHEN USER USES THE SOFTWARE, FIRMWARE AND / OR ACCOMPANYING DOCUMENTATION.

3. Copies, Modification, or Merger. Except as specifically set forth in Paragraph 1, User may not copy, modify, transfer all or any portion of the Software, Firmware, or Documentation or merge it or them into another program, unless expressly authorized in advance in writing by Honeywell. User must, as a condition of this License, reproduce and include the identifying marks, copyright, and proprietary notices on any permitted copy of the Software, Firmware, and Documentation. "Copies" shall include, without limitation, any complete or partial duplication on any media, adaptations, translations, compilations, partial copies within modifications, mergers with other material from whatever source, and updated works. User will use its best efforts to prevent any unauthorized copying or other activity with respect to the Software, Firmware, and Documentation.

4. Third-Party Beneficiary. For any software or other technology under this Agreement licensed by Honeywell from Microsoft (or other licensors), Microsoft or the applicable licensor is a third-party beneficiary of this Agreement with the right to enforce the obligations set forth in this Agreement.

5. Warranty. Honeywell warrants Honeywell manufactured or produced Alerton Products to be materially free from defects and to substantially conform to Honeywell's published specifications for a period of twenty-four (24) months from date of shipment from Honeywell (the "Product Warranty Period"). This entire Section 5 is defined as the "Warranty."

Honeywell also warrants Alerton Products that it has previously repaired or replaced for the greater of ninety (90) days from the date of their shipment from Honeywell or the remainder of the Product Warranty Period of the originally shipped Alerton Product (the "Repair/Replacement Warranty Period").

During the Product Warranty or Repair/Replacement Warranty Period, Honeywell will repair or replace the applicable Alerton Products without charge and will add applicable engineering changes and upgrades.

This Warranty only applies to defective materials and workmanship of Alerton Products and excludes defects that result from misuse, neglect, improper installation, unauthorized repair or alteration, damage during or after shipping, accident, and/or misapplication of such products. This Warranty does not apply to parts, equipment, software, firmware, components, documentation, or any other item that Honeywell does not manufacture or produce. This Warranty is also voided by removal or alteration of Alerton Product identification labels.

Honeywell's sole responsibility with respect to Alerton Products shall be, within the applicable Product Warranty Period, to furnish a replacement Alerton Product (FOB factory) or, at the option of Honeywell, to repair and return (FOB Factory) the defective Alerton Product. HONEYWELL HEREBY EXCLUDES ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ALL OTHER EXPRESS OR IMPLIED WARRANTIES WHATSOEVER WITH RESPECT TO ALERTON PRODUCTS. In no event shall Honeywell be liable for personal injury, loss of profit, loss of production, loss of business or goodwill, business interruption, loss of business information or data, loss due to delays, any other pecuniary loss, any cost or liability of Users or any other parties, to themselves or to others, increased or uncovered operating or fixed costs, inefficiency, or any other special, exemplary, consequential, incidental, indirect or remote damages in any manner, directly or indirectly, related to design, manufacturing, supply, installation or use of, or inability to use, Alerton Products, or any other act or failure to act by Honeywell or its agents or contractors.

HONEYWELL MAKES NO CLAIMS OR WARRANTIES WITH RESPECT TO THE SOFTWARE OR THE FIRMWARE AND SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND EXPRESS OR IMPLIED WARRANTIES THAT THE OPERATION OF THE SOFTWARE OR FIRMWARE OR ANY PORTION THEREOF WILL BE INTERRUPTION OR ERROR-FREE. Notwithstanding anything to the contrary contained in this Warranty, Honeywell shall not be liable to Users or any other parties for any damages, including, but not limited to consequential, incidental, indirect, special, exemplary remote or pecuniary damages and any stated or express warranties set forth in this warranty are in lieu of all obligations or liability for any damages arising out of or in connection with the use or performance of, or inability to use, Alerton Products and the licensed Software and Firmware.

User's exclusive remedy and Honeywell's entire liability arising from or in connection with the Alerton Products, Software, Firmware, Documentation and/or this License and Agreement (including, without limitation, any breach of any warranty, express or implied) shall be, at Honeywell's option, the repair or replacement of the Products or Software or Firmware as applicable, as stated above. ACCORDINGLY, HONEYWELL AND ITS DESIGNATED DEALERS AND THEIR DESIGNATED ASSOCIATE DEALERS HAVE EXCLUDED AND DISCLAIM ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WHATSOEVER, WITH RESPECT TO THE PRODUCTS, THE SOFTWARE, THE FIRMWARE, THE DOCUMENTATION AND/OR THE LICENSE. USER HEREBY ACKNOWLEDGES THE SAME.

6. Remedies of Honeywell. IF USER BREACHES THIS AGREEMENT, USER'S LICENSE HEREUNDER SHALL BE AUTOMATICALLY TERMINATED. Upon termination, User shall return the Software, Firmware, and all Documentation to Honeywell and destroy any copies of the Software, Firmware, and the Documentation or any portions thereof which have not been returned to Honeywell, including copies resident on electronic or digital media. If User breaches this Agreement, Honeywell shall be entitled to all damages suffered by Honeywell resulting from such breach and Honeywell shall be entitled to equitable and injunctive relief in addition to all other remedies at law. In this regard, User acknowledges that its breach of any provision of this Agreement will cause Honeywell immediate and irreparable injury for which there are inadequate remedies at law. The prevailing party in any dispute concerning this Agreement shall be entitled to the costs of collection and enforcement, including but not limited to reasonable attorneys' fees, court costs, and all necessary expenses, regardless of whether litigation is commenced.

31-00212-01

7. Export. Alerton Products are subject to regulation by local laws and United States government agencies, which prohibit export or diversion of certain products, information about the products, and direct products of the products to certain countries and certain persons. User agrees that User will not export in any manner any Alerton Product or direct product of Alerton Product, without first obtaining all necessary approval from appropriate local and United States government agencies.

8. RESTRICTED RIGHTS NOTICE. Alerton Products, Software, Firmware, and Documentation have been developed entirely at private expense and are commercially provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the U.S. Government or a U.S. Government subcontractor is subject to the restrictions pursuant to DFARS 227.72013 (October 1988) and DFARS 52.227-19 (June 1987), as amended and as applicable. Manufacturer, licensor, and publisher is Honeywell, 715, Peachtree street NE, Atlanta, GA, 30308 USA.

9. Statute of Limitations. No action for any breach of a warranty, if any, deemed or actual, may be commenced more than one (1) year following the expiration of such warranty.

10. Other. User further agrees that this Agreement is the complete and exclusive statement of the agreement between User and Honeywell and supersedes any proposal or prior agreement or any other communications between Honeywell or any of its representatives and User relating to the use of the Software, Firmware, Documentation, and purchase of the Products. This Agreement may only be modified by a physically signed writing between User and Honeywell. Waiver of terms or excuse of breach must be in writing and shall not constitute subsequent consent, waiver, or excuse. If any provision of this Agreement is finally determined to be unenforceable, the remaining provisions shall remain in effect. The laws of the State of Georgia and the United States, including U.S. copyright laws, shall govern this Agreement. Venue in the event of any suit, proceeding, or claim shall be in the courts located in Fulton County, Georgia, USA. If User has any questions regarding this Agreement, User may contact Honeywell by writing Honeywell at the above address.

This Agreement shall inure to the benefit of and be binding upon the parties and their successors, administrators, heirs and permitted assigns. Notwithstanding any termination of this Agreement and not in limitation of any other provision of this Agreement, User shall specifically continue to be fully obligated to comply with all of the requirements of paragraphs one (1) through four (4), as if the Agreement were not terminated and all remedy provisions hereunder shall apply to any breach of such obligations.

Welcome to Compass Security

Welcome to Compass, Alerton's operator workstation software for building automation systems. Compass is your command and control center for facility operations from HVAC equipment to irrigation, lighting, security, and more. Here, you can view and command site equipment and systems with unprecedented flexibility and power.

Disclaimer

While we have engaged in efforts to assure the accuracy of this document, Alerton is not responsible for damages of any kind, including without limitations consequential damages arising from the application or use of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found on our website or by contacting our corporate office in Atlanta, Georgia.

Alerton
715, Peachtree street, NE
Atlanta, GA 30308, USA
tech.support@alerton.com

31-00212-01

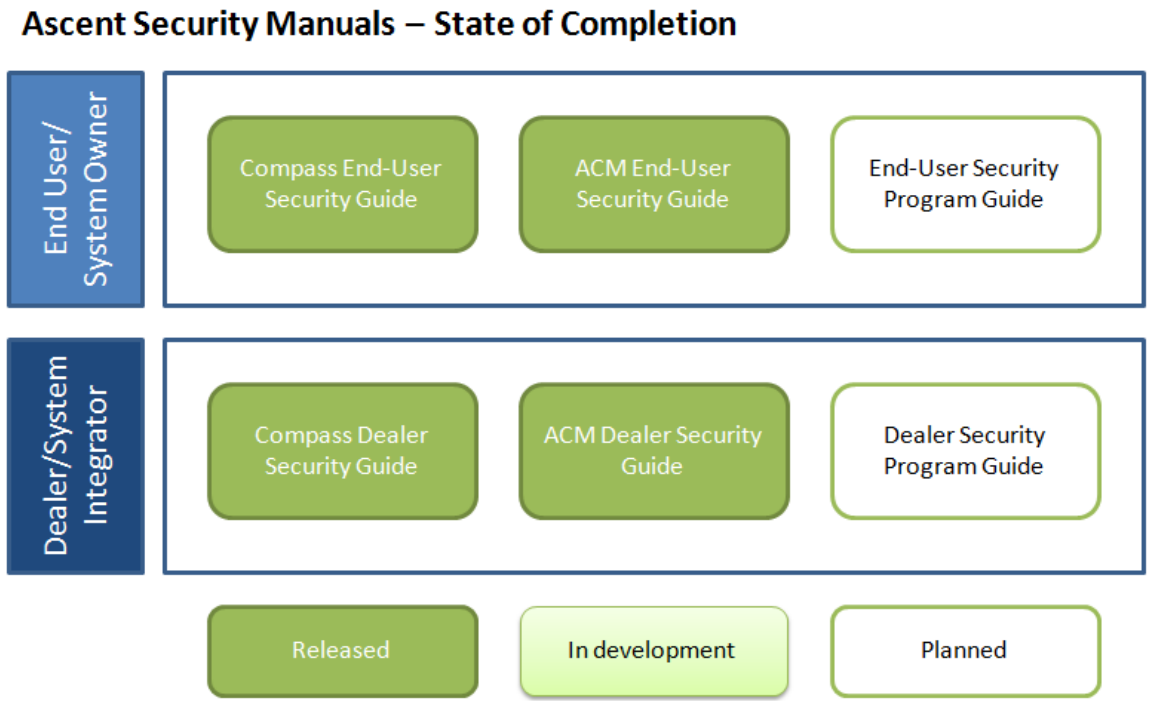
INTRODUCTION AND INTENDED AUDIENCE

This manual contains information to guide the end-user or owner of a Compass system to securely maintain and decommission their system.

Please take the time to read and understand the information in this manual and regularly obtain the latest version of documentation and software updates.

Related security documents

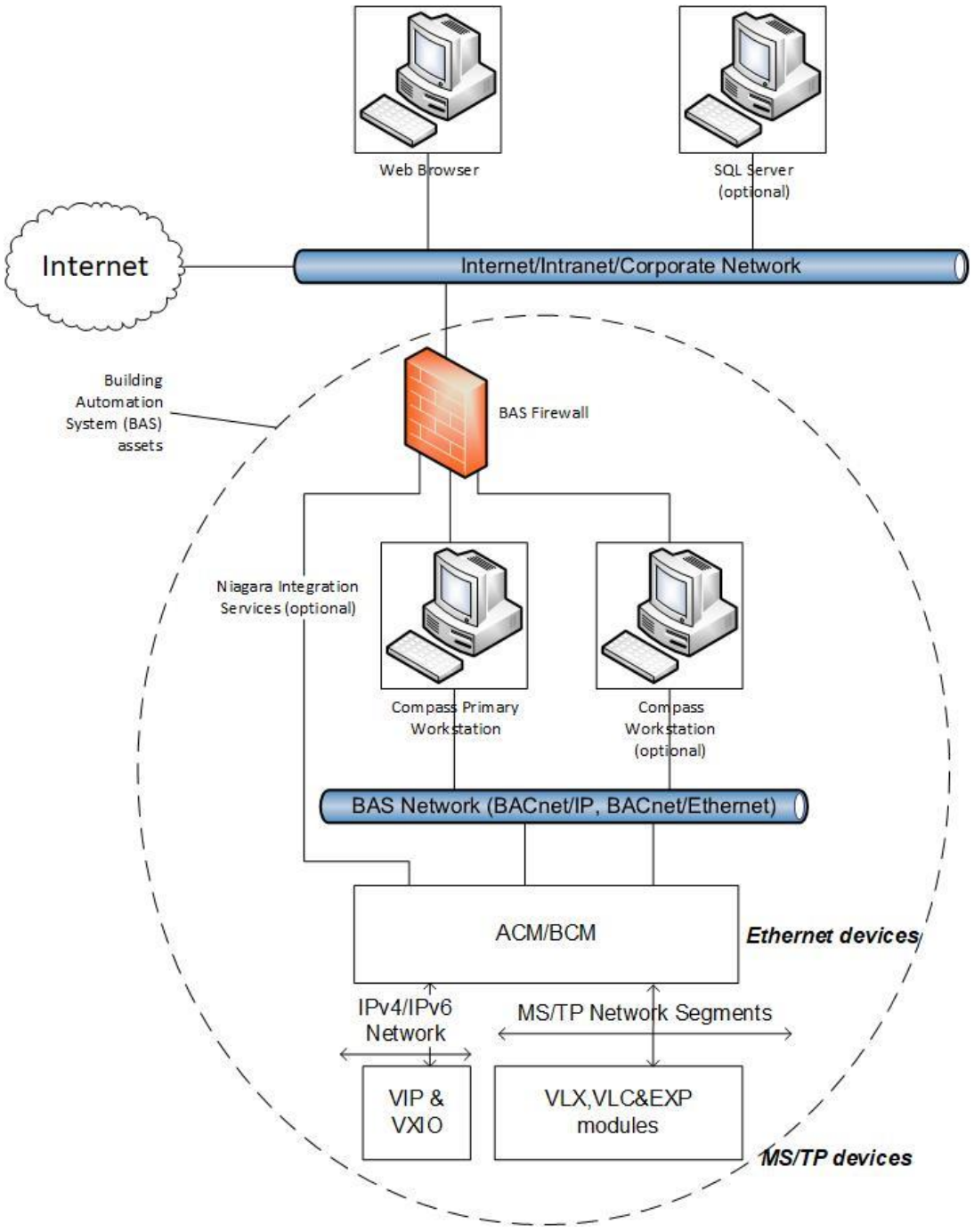
The following diagram shows the relationships and current state of the other Ascent security manuals.



Document	Description
Compass Dealer Security Guide (31-00211)	Provides security-related instructions for planning, installing, and configuring a Compass system. The intended audience is an Alerton dealer.
Compass End-User Security Guide (31-00212)	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 (31-00213)	Provides security-related instructions for planning, installing, and configuring an ACM. The intended audience is an Alerton dealer.
ACM End-User Security Guide (31-00214)	Provides security-related instructions for maintaining and decommissioning an ACM. The intended audience is the Compass system owner and end-user.

SYSTEM OVERVIEW

The following is a diagram of a typical Ascent system installation.



The key elements of the diagram are:

Internet/intranet/corporate network: This is a simplified, logical network representation of all networks outside of the building automation system (BAS) scope. It may provide access to the

31-00212-01

BAS management interfaces (e.g. the Compass primary workstation web user interface) but must provide access to the Internet so that Compass computers can check for and download operating system and virus scanner updates unless another means to do this is provided.

BAS network: This network is used solely for BAS protocols, which consists of BACnet/IP, BACnet/Ethernet, and any protocols that Niagara Integration Services on an ACM might use. This network must not be the same network as the Internet/intranet/corporate network.

BAS firewall: To provide additional separation and protection to the BAS, a firewall must be used between the Internet/intranet/corporate network and any BAS device that connects to it, such as the Compass primary workstation, Compass workstations, and ACMs. This firewall limits access to the BAS to only computers that are authorized and may help reduce the risk of attacks, such as a denial-of-service attack.

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

Web browser: Compass software provides a web-based management interface that is accessed through a web browser.

ACM and BCMs: The Alerton Control Module (ACM) and BACtalk Control Modules (BCMs) are global controllers that connect to an Ethernet network and host MS/TP network segments. MS/TP is a low-bandwidth connection that is used to connect controllers and sensors.

- **ACM Niagara Integration Services:** The ACM has an instance of Niagara and so it can run Niagara code, including a web server. If this functionality is used, then connect the ACM's second network to the Internet/intranet/corporate network through the BAS firewall.

Compass workstation (optional): If access to the Compass primary workstation's thick client interface is not allowed, for example, the Compass primary workstation is run in a virtual machine or console access to it is not allowed, then install a Compass workstation on a separate computer to access thick client functionality.

VIP & VXIO: The Alerton VisualLogic IP Controller (VIP) is a BACnet Advanced Application Controller (B-AAC) with a real-time clock, high resolution 16-bit universal inputs and outputs, and a 32-bit processor.

VLX, VLC, or EXP: The Alerton controllers are advanced application controller with a high-resolution converter and new, high performance processor and real-time clock that supports its own schedules, trendlogs and alarms. The controllers include monitored on-board Hand-Off-Auto (HOA) switches, Ethernet or MS/TP connectivity, and additional math functions beyond the standard VLC/VAV controllers.

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

DESIGN AND PLANNING

During the design and planning phase, you should discuss the following with your Alerton dealer:

- Your needs and requirements for physical and network security of the BAS and its components, such as devices, computers, and networking equipment. Also consider regulatory requirements, such as compliance with PCI (credit card processing security standards), FDA, etc.
- Your needs and requirements for accessing the system outside of your internal networks, such as using the Internet or a VPN.
- Your organization's current knowledge level and capabilities in maintaining security of the system.

Remember that while a BAS might not necessarily be the primary target of an attack, it might be targeted as a way to access other systems.

Disaster recovery planning

Another design and planning activity is to develop a Disaster Recovery Plan.

Developing a disaster recovery plan

As part of your security strategy, define a comprehensive backup and restore policy for disaster recovery. If you don't already have a policy or a group that handles this, your Alerton dealer may be able to help in creating one. In formulating this policy, consider:

- How quickly data or the system needs to be restored. This will indicate the need for a redundant system, spare offline computer, or file system backups.
- How long data needs to be kept.
- The frequency of changes to critical data and configuration settings. This will dictate the frequency and scope of backups.
- The safe onsite and offsite storage of full and incremental backups.
- The safe storage of all Microsoft operating system and Compass installation media, license keys, and configuration information.
- Who will be responsible for creating backups, and the testing, storage, and restoration of backed up files.

Backup and recovery strategy

Performing backups is one of the most important risk mitigation tasks for securing your Compass system. If backups of important data are not made, then data will be lost if a hardware or software failure occurs, if configuration files are deleted, if the system is infected with a virus or worm, or in the event of a natural disaster like fire or flood.

Choosing an appropriate backup strategy allows you to minimize downtime due to situations that cause loss of data. When determining your backup strategy, consider the types of situations that can occur:

31-00212-01

- Media failure: If one or more disk drives fail, there is a potential for a complete loss of data unless the system was properly backed up.
- User error: If a user makes invalid modifications to configuration data, then an effective way to undo these changes is to restore the data from backup.
- Permanent loss of a server: If a server becomes permanently unusable, then the system and data have to be reconstructed unless you have a backup.
- Virus or worm infection: If a virus infects the Compass workstation, then it could delete or corrupt files making it difficult or impossible to restore the system configuration.

Also consider:

- CD and DVD are not considered to be reliable backup mediums.
- Backups can be CPU- and disk-intensive operations on a large system. Perform backups at times that do not have a lot of system load.
- Do not store backup images on the Compass primary workstation or, if used, the SQL Server computer.
- Do not store backup images on the same computer being backed up.
- Backup images should be stored on network drives.
- If network drives are not available, then store backup images to a connected drive using USB.
- Not all backup products support backing up SQL Server, especially when SQL Server is running with open files.
- Configure your backup software product to do a full backup weekly and incremental backups nightly to lower the load and performance impact from backup activities.
- Ensure that you have enough file storage space to hold all backups.
- Ensure that verification is performed after the backup has completed to guarantee that the data was backed up correctly.

An effective Disaster Recovery Plan must be documented and all personnel involved must be knowledgeable of its content and storage location.

INSTALLATION, CONFIGURATION, AND SYSTEM DELIVERY

Alerton provides instructions and guidance for your dealer on how to properly install and configure your Compass system. Compass must be configured to use HTTPS, even on a private network. If Compass is configured to use SQL Server as its database, extra care must be taken to protect the SQL Server system and ensure its operation as it is critical to Compass's operation. As part of system delivery, your dealer should:

- Provide documentation that includes security information, configuration settings, administration usernames and passwords, disaster and recovery plans, backup and restore procedures
- Train end-users on security maintenance tasks.

31-00212-01

MAINTENANCE AND MONITORING

Regular maintenance and monitoring are required to maintain the security of the system.

Access control system

Monitor logs and system alerts for unauthorized access. Inspect and maintain the system to ensure it is operating as intended and has not been circumvented.

Security updates and service packs

An important part of the overall security strategy is to ensure that the operating system is kept up-todate with the latest patches and updates.

Microsoft security updates

Discuss with your Alerton dealer your strategy for checking for and applying Windows Updates. For example, for a computer running a Compass primary workstation, you may wish to manually apply updates so that you can control the time that the primary workstation is unavailable, but for other computers, you may decide to let Windows Updates automatically apply updates.

Microsoft service packs

Check with your Alerton dealer before applying a service pack to see if there are any known issues or incompatibilities.

Compass patches and updates

Check with your Alerton dealer on a regular basis to see if there are Compass patches or updates available.

Virus protection

Ensuring that antivirus software is installed, properly configured, regularly updated, and monitored is an essential part of system security.

Installing antivirus software

If antivirus was not installed by your Alerton dealer, then install it on every computer in the network, including:

- Compass primary workstation
- Compass client workstations and web clients

After installing antivirus software, check the Windows Event Logs to ensure no errors are reported. If the system starts experiencing failures, the inability to read or write files, the logs show deadlock errors, or the system shows any other unusual behavior, disable the antivirus software to see if the failures continue. Note that some antivirus software may need to be completely uninstalled in order to be disabled.

Ensure frequent updates to antivirus signature files

It is important to update antivirus signature files frequently by:

- Subscribing to the updates of your antivirus software vendor(s)
- Leveraging enterprise antivirus policies and practices when available

Since new viruses are released every day, the system will remain vulnerable to attack if the signature files are not updated at the same rate. Where it is not practical to perform updates daily, monitor reputable web sites that publish information about new virus attacks so that the system can be isolated if a specific threat appears.

Receipt of new signature files generally requires Internet access so that the files can be downloaded from the antivirus software vendor. If possible, set up servers for the controlled distribution of antivirus signature files.

Configuring active antivirus scanning

Adopting an active virus scanning strategy as on-access scanning provides the best real-time protection for your system. Additionally, run on-demand scans during regular, scheduled maintenance to catch any malicious files or programs which may be dormant on the computer.

Configure both on-access and on-demand scanning to:

- Scan the boot sectors of all disks.
- Move infected files to a quarantine directory and notify the user that an infected file was found. Allow the user to clean up the infection.

System performance

If Compass is experiencing problems and you suspect antivirus software might be an issue, then contact your Alerton dealer.

System monitoring

Diligent system monitoring will help guard your system against unauthorized access. However, there is always the possibility that an attacker will succeed in circumventing all the safeguards and compromise the system. If this happens, it is important to discover the breach and prevent further damage as rapidly as possible. The earlier a system breach is detected and the more evidence that is captured, then the less damage is likely to occur and the greater the chances of identifying the intruder. Logs that may be collected in the system are:

- Windows Audit Logs (if enabled)
- Antivirus software logs or reports
- Access control system

Detecting network intrusion

Network Intrusion Detection Systems (NIDS) can take many forms. NIDS can be a dedicated server on the same network branch, freeware software available under GNU or similar licenses (most of these are aimed at UNIX systems), or commercial products aimed specifically at Windows systems.

31-00212-01

The purpose of NIDS is to scan incoming network packets and look for unusual traffic or for specific malformed packets known to be associated with attacks. If anomalies are found, NIDS take action such as raising alerts or even disconnecting the computer from the network. The latter is a dangerous option which causes its own denial of service while preventing damage to the system by closing network ports, and so on.

Most firewalls, switches, and routers have reporting capabilities that can report various levels of events ranging from debugging to emergency failure. These reports can be viewed using telnet, collected by a central logging server, or emailed to an administrator. For example, the Cisco PIX firewall and Catalyst 4500 switches can be configured to send selected levels of events to a central syslog server where further analysis can occur and significant events can be detected.

Syslog servers are common on Unix systems, and third-party syslog services are available for Windows. They vary in functionality and cost, from freeware, which simply writes to a log file, to sophisticated NIDS that analyze the logs in detail. As well as being able to control the level of severity of events, the PIX firewall allows the suppression of individual messages. This can significantly reduce clutter and also provide some ability to recognize common attack signatures and raise appropriate alarms.

When you configure network event logs, maintain a balance between collecting too many events (and missing something important) and filling storage disks and deleting information (which is subsequently needed for an intrusion investigation).

Other forms of intrusion detection will search event logs looking for unusual events, or will compare the current file system to a known good image. Be careful when running such tools to prevent them from using too many resources and interfering with the control system.

Disaster recovery maintenance activities

Schedule regular job backups according to your Disaster Recovery Plan. Configure your backup software product to do a full backup weekly and incremental backups nightly to lower the load and performance impact from the backup activities. The frequency of backups depends on two major criteria:

- How often job configuration is changed.
- Where job data is stored.

If job data is stored in SQL Server, then the Compass Backup and Restore functionality does not back that data up. You must ensure Compass's SQL Server database is periodically backed up through an external mechanism. The backup policy is best managed by the site's database administrator (DBA); see Backup Overview (SQL Server) on Microsoft's Developer Network at http://msdn.microsoft.com/en-us/library/ms175477.aspx for more information.

Restoring the Compass job and database

If loss of data occurs, both the job and the SQL Server database may need to be restored.

The process for restoring the job backup can be found in the Compass online Help by searching for Restore Utility.

Restoring a SQL Server backup is best handled by the site's DBA; see Restore a Database Backup (SQL Server Management Studio) on Microsoft's Developer Network at http://msdn.microsoft.com/en-us/library/ms177429.aspx for more information.

DECOMMISSIONING AND DISPOSAL

Dispose of equipment and data securely. Consider the following:

- How sensitive is the data?
- Are there any regulatory requirements relating to retention time periods or proof of destruction for data or devices?
- Are there backups of the data that also need to be disposed of? This might consist of backup devices, tapes, or cloud storage.
- Are there adjacent systems that must also be modified? For example, do you need to remove system-specific users from an authentication database or SQL Server accounts?
- Are there networking or other infrastructure systems that need to be modified? For example, do you need to close firewall ports, remove router configurations, or disable VPN access?
- If there was a different BAS, were these items considered when it was removed?

COMPASS INSTALLATION SECURITY CHECKLIST

Compass Job Name: _____

Compass Job Location: _____

Installer: _____ **Date:** _____

Complete the following security tasks for your Compass installation.

- ☐ Develop a Disaster and Recovery Plan. See page 10.
- ☐ Develop a Backup and Recovery Strategy. See page 10.
- ☐ Verify that the system is well-documented upon delivery. See page 12.
- ☐ Monitor system logs and alerts for unauthorized access. See page 13.
- ☐ Update the operating system with the latest patches and updates. See page 13.
- ☐ Discuss your Windows Updates strategy with your Alerton dealer. See page 13.
- ☐ Check with your Alerton dealer for new Compass patches or updates. See page 13.
- ☐ Install and configure anti-virus software. See page 13.
- ☐ Set up network intrusion detection. See page 14.
- ☐ Schedule regular job backups according to your Disaster Recovery Plan. See page 15.
- ☐ For decommissioning, dispose of data securely. See page 17.

31-00212-01

This page is intentionally left blank.

ALERTON

715 Peachtree St NE
Atlanta, Georgia 30308
alerton.com

31-00212-01 I 2022-04