Honeywell

LCBS Connect End–User Security Guide

TECHNICAL REFERENCE MANUAL

CONTENTS

31-00131-01

INTRODUCTION AND INTENDED AUDIENCE

This manual contains security-related information to guide the contractor, end-user or owner of Honeywell LCBS Connect to plan, install, operate, maintain and decommission it.

It is the responsibility of the contractor, end-user or owner to ensure proper understanding of the information in this manual and ensure proper security of the LCBS Connect System. The information in this manual is intended to provide guidance for the contractor, end-user, or owner on current industry practices; provided, however, it is the responsibility of the contractor, end-user, and owner to ensure the proper and secure installation, operation, maintenance, and decommissioning of the Honeywell LCBS Connect System.

THE LCBS CONNECT SYSTEM IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. FURTHER, HONEYWELL DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE OF THE LCBS CONNECT SYSTEM IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, SECURITY, TIMELINESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE LCBS CONNECT SYSTEM IS ASSUMED BY THE CONTRACTOR, END-USER, AND OWNER. IF THE LCBS CONNECT SYSTEM IS DEFECTIVE OR INOPERATIVE, THE CONTRACTOR, END-USER, AND OWNER, AND NOT HONEYWELL ASSUMES THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. THE CONTRACTOR, END-USER, AND OWNER AGREE TO COMPLY WITH ALL INDUSTRY AND HONEYWELL STANDARDS WITH RESPECT TO CYBERSECURITY. HONEYWELL DISCLAIMS ALL WARRANTIES INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, TITLE AND FITNESS FOR A PARTICULAR PURPOSE.

UNDER NO CIRCUMSTANCES WILL HONEYWELL BE HELD LIABLE FOR ANY HARM RESULTING FROM DOWNLOADING OR ACCESSING ANY INFORMATION OR MATERIAL THROUGH THE LCBS CONNECT SYSTEM, ANY DELAY OR FAILURE IN PERFORMANCE RESULTING DIRECTLY OR INDIRECTLY FROM ACTS OF NATURE, FORCES OR CAUSES BEYOND ITS REASONABLE CONTROL, INCLUDING, BUT NOT LIMITED TO, INTERNET FAILURES, COMPUTER EQUIPMENT FAILURES, TELECOMMUNICATION EQUIPMENT FAILURES, OTHER EQUIPMENT FAILURES, WIRING, INTERNET SERVICE PROVIDERS, MOBILE DEVICE CARRIERS, SATELLITE PROVIDERS, ELECTRICAL POWER FAILURES, SECURITY BREACHES, STRIKES, LABOR DISPUTES, RIOTS, INSURRECTIONS, CIVIL DISTURBANCES, SHORTAGES OF LABOR OR MATERIALS, FIRES, FLOODS, STORMS, EXPLOSIONS, ACTS OF GOD, WAR, GOVERNMENTAL ACTIONS, ORDERS OF DOMESTIC OR FOREIGN COURTS OR TRIBUNALS, NON-PERFORMANCE OF THIRD PARTIES, OR LOSS OF OR FLUCTUATIONS IN HEAT, LIGHT, OR AIR CONDITIONING.

There can be no assurances whatsoever that the LCBS Connect System will protect any individual or his or her property from harm. Appropriate safety precautions must always be taken and experienced installers and operators must be utilized when installing, setting up, operating or maintaining any building systems. Incorrect processes may result in property loss, severe injury, or death. Honeywell assumes no responsibility or liability for any injury or damage to any persons or property resulting from the use of the LCBS Connect System.

SYSTEM OVERVIEW

Fig. 1 is a system diagram of the LCBS Connect system in an example installation in a corporate network.

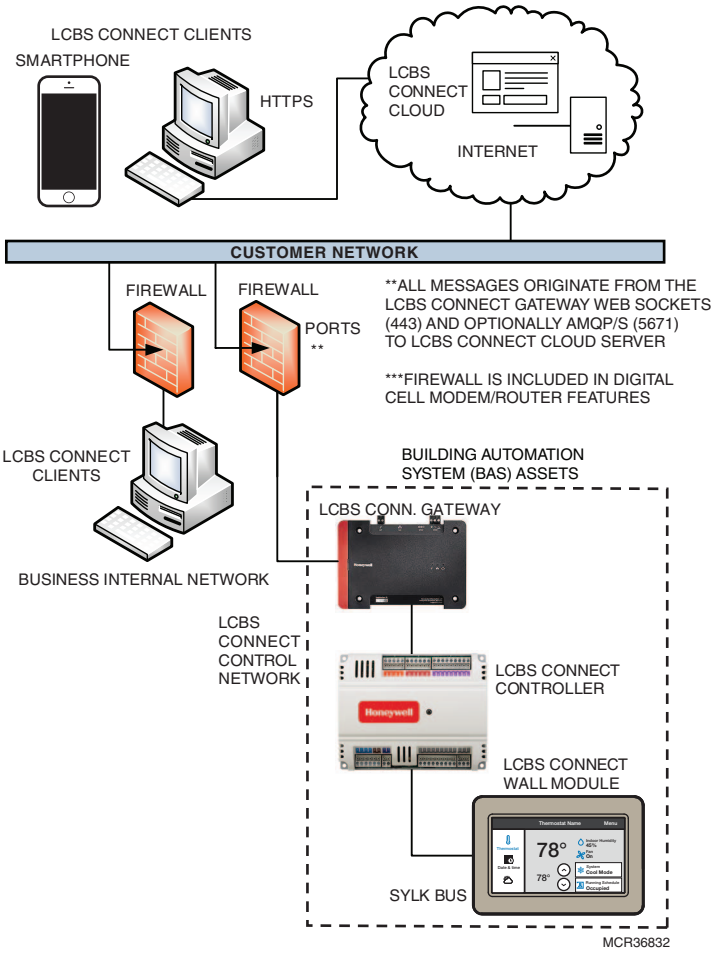

Fig. 1. Example: LCBS Connect system installed in a corporate network.

Fig. 2 is an optional system diagram of the LCBS Connect system for use in the special case that requires a digital broadband provider network for internet access.

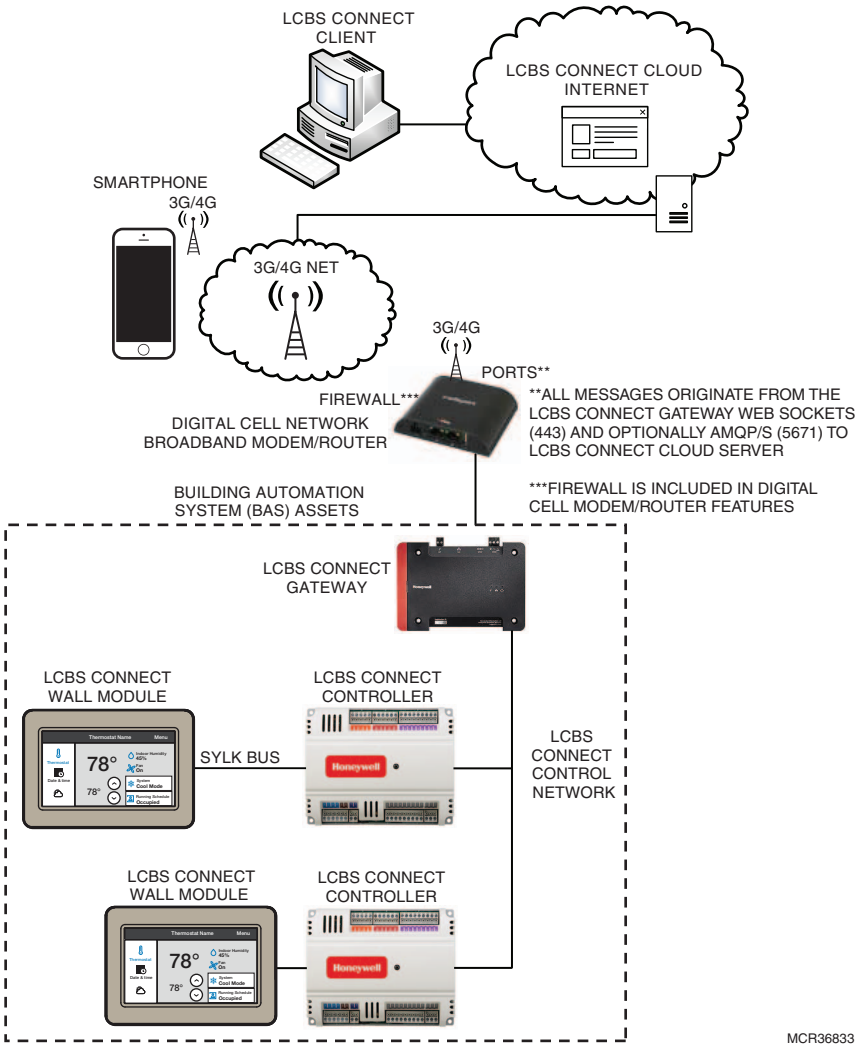

Fig. 2. Example: optional system diagram of LCBS Connect system for use with a digital broadband provider network.

Some key elements of the diagram are:

Internet/Intranet/Customer Network: This is a simplified, logical network representation of all networks outside of the LCBS Connect scope.

The network provides access to the Internet so that the LCBS Connect Gateway can communicate and download operating system updates. It is a requirement for the customer to provide a connection from the gateway to the internet so that the gateway can communicate with the LCBS Connect Cloud.

LCBS Connect is accessed through the Internet through a LCBS Connect client such a PC running a browser, a tablet or a smart phone.

A customer network LCBS Connect client does not access the LCBS Connect gateway directly but will communicate to the LCBS Connect Cloud applications.

LCBS Connect Clients: The user will be able to access their buildings under management through a client browser. The web browser connects securely via HTTP/S to a LCBS Connect Cloud Server. The LCBS Connect Cloud Server is in the Honeywell Cloud which communicates securely to the buildings and LCBS Connect Gateway.

LCBS Connect Cloud: LCBS Connect servers that host the LCBS Connect application which includes remote monitoring, control and other LCBS Connect applications and services.

Firewall: The firewall is used to create the trusted network and prevents unrestricted access to local computers and network resources. The firewall is used to protect the trusted/internal network from unwanted intrusions from the internet. A firewall is typically installed between the facilities network and the general internet.

LCBS Connect Wall Module: A color touch screen wall module interface with integrated temperature and humidity sensor that sends and receives information from the LCBS Connect controller and gateway. The LCBS Connect Wall Module talks to the LCBS Connect controller through the Sylk bus.

LCBS Connect Controller: The physical controller mounted in the Roof top unit.

LCBS Connect Gateway: The device linking the LCBS Connect controllers to the Internet and Honeywell Cloud. The LCBS Connect system will not react to any communication that is not initiated by the gateway. The gateway also connects the LCBS Connect controller through the LCBS Connect control network bus.

Digital Network Broadband Modem/Router/Firewall: An alternative network option in place of an on premise Customer Network. The broadband modem/router provides access to internet without using a customer network using a cellular 3G/4G network.

The cellular network broadband Modem/ Router solution is to facilitate a situation where requirements specify a separate network or there is no other way to get an internet connection to the site.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.

For the LCBS Connect solutions, the AMQP/s and Web Sockets(HTTPS) secure protocols are used for all communications. Communications are initiated from inside the firewall (LCBS Connect Gateway) to a known endpoint (LCBS Connect Cloud).

The secure HTTPS is used within the LCBS Connect Cloud. For example: communications from a LCBS Connect Client Browser to the LCBS Connect Contract portal.

LCBS Connect Network Bus: This is the LONworks communication network between the LCBS Connect gateway and controller and is designated by “Net” on the gateway’s connection labels.

SYSTEM DESIGN AND PLANNING

Physical Security of Components

It is important to have a plan for physical security of system components. It is recommended that the contractor identify the security needs of the building owner and provide guidance for implementation in addition to the requirements of the building owner.

It is recommended that the organization responsible for providing security for network assets be involved in the planning. The Building owner/customer’s IT groups needs to approve and connect the LCBS Connect gateway to the system so that the IT system will work with the LCBS Connect gateway through the corporate network.

Physical security controls, such as a locked cabinet or equipment room that restricts physical access to the LCBS Connect gateway and controllers are necessary to prevent system tampering, power interruption, and other security issues.

Ensure that LCBS Connect components requiring high reliability are protected with secure power sources and emergency power systems. Honeywell recommends strongly that you consider reliable power for the LCBS Connect control system. System reliability is an important security issue and following these requirements and recommendations allows continuous monitoring and ensures HVAC control system reliability.

IT Network

LCBS Connect system requires a connection to the public internet in order to support remote monitoring and operation of the system.

Firewall setup may require coordination with your IT provider staff for network provisioning and testing. Proper coordination and planning with IT staff will result in a secure and fast installation of the LCBS Connect system.

To ensure the cyber safety of your system and data, Honeywell requires you to use a network firewall. Note that the system can functionally operate without the use of a firewall, but it is not safe nor recommended.

Honeywell recommends strongly that you setup the Firewall including ports that are essential to maintaining the designed security protections.

The IT group and contractor need to test communications from the LCBS Connect gateway (using ports 443 and 5671 originating from the gateway to outbound) to the Honeywell Cloud Server. This test can be as simple as plugging the gateway to the wall via power and Ethernet.

Honeywell recommends that network settings be planned and recorded.

IF a static IP address for the gateway is required, then refer to the instructions provided on the LCBS Connect Cloud detailing how to do this via the LCBS Connect wall module advanced configuration screens.

Honeywell strongly recommends that Point of Sale (POS) and other critical business networks be kept separate from the LCBS Connect gateway through network segmentation. Honeywell will not accept any liability if this recommendation is not adhered to.

See additional notes in Appendix 1 on IT network notes.

See additional notes in Appendix 4 for Installation Security Issues

See additional information in Appendix 8 for installation of 3g/4g Data Modem Routers.

LCBS Connect Controller Configuration

LCBS Connect controller configuration information is recommended to be stored in locally accessible backup records for each installation site to allow rapid recovery in case of emergency or internet loss. It is recommended that the contractor keep a record of individual RTU names, configuration, wiring, and setpoints/schedules.

LCBS Connect Communications Bus and Sylk Bus

It is required that physical security access to LCBS Connect communications bus and wall module bus wiring be accomplished by
1) installing wiring in physically inaccessible locations that restricts physical access to the LCBS Connect communications bus
Or
2) installing wire in conduit.

This required physical security access protection is important to prevent security threats to the control system. Failure to protect the LCBS Connect communication bus and Sylk bus can lead to critical security issues. For example, data loss or corruption could result due to not following the required protection for the LCBS Connect communication bus.

See Appendix 2 for Installation Best Practices

LCBS Connect Cloud Application

Access to the LCBS Connect Cloud is granted through the use of secure and unique passwords. Like your bank password, care should be taken to protect user identity. Users invited to participate in LCBS Connect should also be restricted to essential personnel only.

See Appendix 3 for Security Maintenance Tasks

LCBS Connect Clients

Each client for LCBS Connect must be protected as a secure platform. Maintaining a secure client platform will involve OS updates, anti-virus software, and protection of local ports from attacks including spam, phishing, and physical compromise.

See Appendix 4 for Installation security issues

See Appendix 5 for LCBS Connect Client security information

NETWORKS AND FIREWALLS

This section contains information on securely configuring networks and firewalls.

Table 1 describes the ports and processes in a LCBS Connect system. This includes the processes that are part of PC web browsers and network devices such as router.

Table 1. Network ports and firewall settings.

Default Port/ Protocol	Purpose	Device Name	Change from Default	Description	Allow through BAS Firewall?	Note
80/TCP	Access to public web from LCBS Connect network	Network Router / Broadband Cell Router/Browser	Yes	Access to public web from LCBS Connect may be needed if a workstation computer on LCBS Connect network requires access to internet. Incoming port can be blocked.	Incoming port: blocked; Outgoing port possibly open	1
443/TCP	Access to public web from LCBS Connect network and access to LCBS Connect Cloud servers from LCBS Connect Gateway	Network Router/ Broadband Cellular Router	Yes	LCBS Connect Gateway requires access through an outgoing port to LCBS Connect Cloud servers. Incoming ports can be blocked.	Incoming port: blocked; Outgoing port must be open for LCBS Connect Gateway	1
5671/AMQP	Access to LCBS Connect Server	Network Router/ Broadband Cellular Router	Yes	LCBS Connect Gateway requires access through port outgoing to LCBS Connect Cloud servers. Incoming ports can be blocked	Incoming port: blocked; Outgoing port must be open for LCBS Connect Gateway	
NOTES Many users expect that they only need to enter the web address for websites, so if HTTP is enabled, then the web server will automatically redirect the request to HTTPS. If this is desired, then this port must be allowed through the Windows firewall.						

See Appendix 6 for Additional Firewall and Network Intrusion issues

See Appendix 7 for Hardening and Physical Computer Issues

MAINTENANCE

Make sure LCBS Connect clients are running up to date virus software and comply with Corporate PC security standards.

The LCBS Connect gateway is associated with the building during commissioning and should be inspected periodically for connection. If there is no connection, the connection issues should be resolved in a timely manner.

DECOMMISSIONING

The LCBS Connect gateway is associated with the building during commissioning and should be removed after decommissioning. If the LCBS Connect gateway is not decommissioned from the LCBS Connect Cloud, the gateway will appear to work from a remote location like it is in the original building.

LCBS CONNECT INSTALLATION SECURITY CHECKLIST

Job Name:_____

Job Location: _____

Contractor: _____ Date: _____

IT Representative: _____ Date: _____

Complete the following security tasks for your installation.

- ❑ Design a secure installation considering both software and hardware vulnerabilities.
- ❑ Develop a Disaster and Recovery Plan.
- ❑ Develop a Backup and Recovery Strategy.
- ❑ Install, configure, and keep antivirus software updated on LCBS Connect Clients.
- ❑ Keep the LCBS Connect Client devices operating systems updated.
- ❑ Secure access to the LCBS Connect Client's operating system using user accounts.
- ❑ Secure access to LCBS Connect using LCBS Connect Clients individual user accounts.
- ❑ Set up monitoring and logging services to scan for unauthorized access on your LCBS Connect system
- ❑ Securely configure networks and firewalls.
- ❑ Set up network intrusion detection.
- ❑ Secure or eliminate wireless access points.
- ❑ Harden the network system to further safeguard against unauthorized access.
- ❑ Eliminate LCBS Connect Client anonymous logon capabilities.
- ❑ On LCBS Connect Client software, disable the caching of previous logon capabilities.
- ❑ Disable unused subsystems on LCBS Connect Clients. This adds risk to the LCBS Connect system.
- ❑ Deliver all required system information upon delivery to the system owner.
- ❑ Train end-users on security maintenance tasks at system delivery.
- ❑ Assess security risks.

APPENDIX 1 – IT NETWORK NOTES

Businesses with critical Point of Sale infrastructure (POS) or other important assets must use internal network segmentation. Proper network segmentation can be accomplished in a small business with the use of a security gateway or firewall.

Industrial Society of Automation / Industrial Electrotechnical Commission ISA/IEC 62443 Network and system security for industrial-process measurement and control is a recommended security standard that prescribes a clear definition of zones and network segmentation. IEC 62443-Segmentation allows the best control over access and security within an automation network.

NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security is a useful reference for security topics and is available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

APPENDIX 2 – INSTALLATION BEST PRACTICES

LCBS Connect Communication Bus
Security of the bus also means that the bus is electrically reliable for communications. It is important the bus is installed with one wire type consistent throughout the whole gateway to controller connection as to eliminate reflections from bus wire impedance mismatches. Shielded wire is not recommended for normal installations. See installation instructions for details.

APPENDIX 3 – SECURITY MAINTENANCE TASKS

It is important to train end-users on documented security maintenance tasks

Disaster Recovery Planning
Creating, implementing, and maintaining a disaster recovery plan is import for the contractor and customer as the system can be restored in the event of a security breach or equipment failure. As a contractor, you may assist in helping the customer develop a plan or provide services to help implement and maintain the plan. The plan needs to ensure clearly documented procedures, document the person or organization responsible, and provide review of the plan during planned maintenance intervals.

Backup and Recovery Strategies
Performing backups of operating data is a risk mitigation task to secure your LCBS Connect system.

Important configuration information may be lost if there are failures due to a natural disaster, hardware or software failure, or computer virus.

Backup strategies should take into account hard drive failures, user errors, and permanent loss of computer connection, virus infection or other problems.

Do not store backup images on the same computer being backed up. If network drives are not available, store backup images to a connected drive using USB.

Configure your backup software to do full backup's weekly and incremental backups nightly to lower the load and performance impact of backup activities. Ensure that the data was backup up correctly after the backup is complete.

APPENDIX 4 – INSTALLATION SECURITY ISSUES

This section contains security issues and information on security issues related to each individual installation step for LCBS Connect.

Table 2. Installation Security Issues.

Step ID	Name	Security issues and information
1a	Plan, install, test Internet access with IT	Ensure physical and network security is in place and access to necessary ports is restricted. Router and firewall setting must be specified and tested. If a digital cellular broadband network is used, additional security accounts must be managed by the network provider. The signal strength at the installation location should be established with a test 3G/4G Router using the planned data plan provider in the actual installation location. The signal strength should be at or exceed 3 bars at the modem/router for greater than 95% of a day. Planning for maximum reliability may require an external antenna be mounted on the roof and connected to the Digital broadband router.
1b	Install LCBS Connect gateway in a physically secure location with power, network, controller communication bus	Ensure physical and network security is in place and access to necessary ports is restricted as necessary.
2a	Review power and I/O specifications for controller	Ensure physical and network security is in place and access to power, Sylk bus, I/O wires, and controller network wires are restricted.
2b	Mount controllers, wire power/sensors and plan power	
2c	Controller bus wiring planning and installation	
2d	Mount, wire LCBS Connect wall module	Ensure physical and network security is in place and access to power, Sylk bus, I/O wires, and controller network wires are restricted.
2e	Perform initial setup from LCBS Connect wall module – at least password MUST be completed	It is important to create controller name, create secure, unique password, and configure RTU locally to ensure security. If the controller already has a password, ensure that it has been set by the contractor per specification.
3a	Unplug IT LAN network connection to gateway. Power the gateway and diagnose local controller communications using lights on gateway. Troubleshoot local controller communication using wall module status screen and gateway lights. Solid green light indicates good communications to controller.	Ensure physical and network security is in place and access to power, network, Sylk bus, and controller network wires are restricted.
3b	Connect gateway to network and diagnose network gateway lights. Blinking Blue light will occur meaning the gateway is ready to be registered.	
4a	Honeywell creates distributor	Ensure password protection of distributor account. Ensure security of distributor password.
4b	Honeywell creates Contractor.	Ensure password protection of contractor account. Ensure security of distributor password.
4c	Honeywell links contractor to a designated distributor.	
4d	Honeywell invites distributor	

Table 2. Installation Security Issues.

Step ID	Name	Security issues and information
4e	Distributor accepts the invitation. Distributor now has username and temporary password. First login will request change to the temporary password.	Ensure secure email account and secure email platform app and OS.
4f	Distributor invites contractor.	
4g	Contractor accepts the invitation. Contractor now has username and temporary password. First login will request change to the temporary password.	Ensure secure email account and secure email platform app and OS.
4h	Contractor creates building and specifies a building owner. Contractor request access from building owner. Building owner accepts request. Now contractor can add and register gateway.	Ensure secure email account and secure email platform app and OS.
4i	(optional) Distributor invites additional users to help manage system	Ensure secure email account and secure email platform app and OS.
4j	(optional) Contractor invites additional users to help manage system	Ensure secure email account and secure email platform app and OS.
4k	Connect gateway to network and diagnose network gateway lights. Solid Blue light now indicates a registered gateway associated with a building communicating to the cloud.	Ensure physical security to gateway and communication bus.
4l	Additional configuration of controller occurs from cloud	Ensure audit log of changes. Ensure secure password of users.
4m	Contractor can access configurations, alerts and analytics via web page or receive text messages/email.	Authenticate users. Audit Logs of changes.
5a	Access to the wall module day-to-day operations has limited privilege. Contractor has more features available via password on wall module	Ensure wall module password is secure and not shared. Change wall module passwords as needed.
5b	Supported web browsers are Chrome, Firefox, Edge, Safari. User is responsible for maintaining password security and maintaining Platform security updates to OS, LCBS Connect application, and password security.	Ensure password protection of distributor, contractor, building owner and all delegates account. Ensure security of all password.
6	Gateway firmware is pushed remotely on scheduled intervals	Schedule regular audits to verify unused accounts are deleted. Automated password resets and complexity verification.
7	Cloud system security issues	Schedule regular audits to verify unused accounts are deleted.
8	Obsoleted users	Schedule regular audits to verify unused accounts are deleted.
9	Validate security	Regular tests of network security are performed and corrective action taken.
10	Disaster recovery plan created to allow system restoration after a security breach or equipment failure.	Plan tested and in place that allows for rapid recovery from security breach or equipment failure.
11	Backup of configuration information	Information of configuration must be documented and available to ensure risk mitigation for securing LCBS Connect.
12	Software and operating system security	Ensure up to date Virus protection, Virus signature file updates, and active antivirus scanning automation. Service packs and security updates to browser application and operating system.

APPENDIX 5– LCBS CONNECT CLIENT SECURITY INFORMATION

Software and Operating System Security

This section includes information to installing and configuring non-LCBS Connect software and the operating system.

Virus Protection
Although some modern threats can bypass even the best antivirus checks, antivirus software is still an essential element of a comprehensive security strategy.

Installing Antivirus Software
Install antivirus software on every computer in the network, including the LCBS Connect primary workstation,

LCBS Connect client workstations, and devices used for web browser access.

After installing antivirus software, check the Event Logs and 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) and 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. Configure the virus scanner to 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.

Regularly review virus scan reports as part of the active scanning strategy.

Tuning Antivirus Scanning for System Performance
When formulating your virus scanning strategy you must take into account the potential impact on critical system resources. For example, if the LCBS Connect workstation is experiencing problems due to low system resources, you may need to:
- Ensure that antivirus software only runs when system resources on the computer are adequate to meet system needs.
- Limit system resources that are used by antivirus software during scanning.

To find the proper balance between browser workstation performance and virus protection you need to make configuration choices such as disabling scanning on reading of files and changing the default process-based scanning to per-process scanning. Do not automatically schedule full system scans, as this can result in severe degradation of performance, which could impact the ability of operators to respond to an incident.

Service Packs and Security Updates
An important part of the overall security strategy is to ensure that the operating system is kept up-to-date with the latest patches and updates. Before turning the system over to the customer, ensure that you have:
- Installed the latest supported web browser version.
- Updated Windows to the latest service pack supported by LCBS Connect (this information is available on the LCBS Connect web site or by contacting Technical Support).
- Configured Windows Update to automatically check for updates.

For the LCBS Connect primary workstation, discuss with the customer about how to automatically or manually apply updates. The customer may opt to install them manually in order to control when the LCBS Connect primary workstation gets rebooted. For client workstation computers, updates should be installed automatically.

User Accounts

Securing Access to the Operating System
LCBS Connect does not use Windows user accounts for application security; Windows user accounts are used to secure access to the operating system and still provide a very valuable layer of protection. Ensure that only authorized users have access to computers.

Windows User Accounts and Passwords
Access is gained to the Windows operating system by logging onto the computer using a user account name and password. This is true for both local and remote terminal services access. Because user accounts may be well known or easily guessed within an organization, the password becomes the prime vehicle for authentication. User account and password policies are therefore important security measures.

User and Password Policies and Settings
Since users are not authenticated using Windows, configure LCBS Connect so that each user has a unique login name and password. Ensure that when an employee, or any other user with permanent or temporary access,

leaves the organization or no longer needs access, their user accounts are disabled. For example, when a subcontractor is on the job working on the LCBS Connect HVAC system, they are given access to the system. Monitor their access while the work is in progress and then disable their credentials once the work is complete. In addition, because LCBS Connect software is available using a browser, ensure that the LCBS Connect user account is also disabled.

Follow Windows user and password policies to secure access to the operating system running LCBS Connect. As a general rule:
- Review user accounts on a regular basis.
- Disable or delete all unused accounts.
- Disable all anonymous accounts
- Disable all guest accounts.

Configure password policies so that Windows account passwords are difficult to guess and they are changed often. The following settings are suggested:
- Maximum password age set to 45 to 90 days – this forces the choice of a new password after this time. Configure the setting for the Administrator account shorter than a normal system user. A maximum of 30 days is recommended.
- Minimum password age set to 1 to 5 days— this prevents cycling passwords too rapidly
- Minimum password length set to 11 characters – This improves encryption and makes guessing harder. Using several words to form a phrase can make a stronger password that is also easier for the user to remember. For example, “My dog Fido has 50 fleas!” is a much stronger password, and much easier to remember, than “X$9d8oc-@Ek”
- Enforce password history set to 24 passwords remembered – This prevents reuse of the same password too quickly.
- Password must meet complexity requirements set to enabled improves encryption and makes guessing harder. Suggest requiring at least three of the following: Uppercase Character, Lowercase Character, Number, and Special Character
- Store passwords using reversible encryption set to disabled – this prevents passwords from being stored in (the equivalent of) clear-text.
- Account lockout threshold set to 5 invalid logon attempts – this prevents continual password guessing by disabling an account after the specified number of attempts. Consider disabling account lockout for operator (or other user) accounts where denial of service or loss of view would be detrimental to safety or the continued operation of the facility.
- Account lockout duration set to 30 minutes – this specifies the period of time during which a user will not be able to log on following an account lockout. (Note that the administrator can re-enable the account before the expiration of the specified lockout period.)
- Reset account lockout counter after 29 minutes --- this sets the time before the account lockout is reset to zero. For example, with the account lockout set at 10, and the lockout counter set at 29 minutes, lockout will occur if there are 10 invalid logon attempts within 29 minutes. Note that the lockout counter must be less than the lockout duration.

Service and Primary Workstation Accounts
Run Windows services and PC browser required by LCBS Connect under an account with the lowest possible set of privileges. The following classes of accounts are suggested in order of preference:
- Local service accounts.
- Local accounts with minimum rights.
- Domain accounts with minimum rights.
- The Network Service account.
- Local or domain user accounts belonging to the Local Administrators group.
- The local system account.

Monitoring and Logging

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.

Setting Up and Analyzing Windows Audit Logs
Enable the auditing of your file system and registry access. If you suspect that the system is being misused, then Windows auditing provides a useful tool to track who did what and when. Once Windows auditing is enabled, review the Windows audit logs frequently and take action if unexpected activity is seen.

Restricting Access to Event Logs
By default, anonymous accounts and guest accounts can view Windows Event Logs when logged in to a Windows computer. Restrict this access on the LCBS Connect primary workstation, because the system, application, and security logs may contain sensitive information about the system and its operations.

IMPORTANT

Back up your system and then back up the registry hive before making any modifications in the Windows registry. If a mistake occurs, you can then recover by reverting back to the backup of the hive—or worse case, revert back to the system backup—to recover and minimize downtime.

⚠ CAUTION

Possible Equipment Damage

Mistakes made while editing the Windows registry can cause serious issues with your computer. Follow these steps precisely. If you make a mistake you cannot fix, restore your backup and start over.

To restrict access to administrators and system accounts only on Windows machines:
1. Choose Start > Run to open the Run window.
2. Type regedit and then click OK.
3. Expand the HKEY_LOCAL_MACHINE tree until you open the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog registry key.
4. Select the Security sub key.

5. Right-click in the right window and then choose New > DWORD Value to create a new registry value.
6. Name the new value RestrictGuestAccess.
7. Right-click RestrictGuestAccess and then select Modify.
8. Type 1 in the RestrictGuestAccess value data field and then click OK.
9. Repeat steps 5 through 8 for the Application and System sub keys.
10. Close the Registry editor.

APPENDIX 6– FIREWALL AND NETWORK INTRUSION ISSUES.

Configuring the Windows Firewall on Windows PCs Running the Web Browser
The Windows firewall provides another layer of protection and must always be enabled. When the firewall is on, it will reject any incoming connections by default. Exceptions must be put into the firewall to allow incoming connections to succeed. By default, the LCBS Connect uses the designated browser and does not automatically configure the Windows firewall. If not manually configured, on first usage the Windows firewall will prompt the user to add a firewall exception. Use the following configuration settings:

- The firewall is on.
- The firewall is on for all network locations (Home or work, Public, or Domain).
- The firewall is on for all network connections.
- The firewall is blocking all inbound connections except those that you previously specified.

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.

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 varying 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 then raise the 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.

Wireless Access Points
Follow these guidelines when setting up and configuring a wireless network:

- Do not use the default Service Set Identifier (SSID); configure a unique SSID.
- Disable SSID broadcast.
- Use Wi-Fi Protected Access II (WPA2-Personal) or (WPA2-Enterprise) encryption. Wired Equivalent Privacy (WEP) is not sufficiently secure.
- Use the correct class of network equipment. For example, do not use home or small office equipment for large enterprise jobs.
- Change the default administrator password.
- Ensure access points are running the latest firmware.
- Physically secure access point devices.
- Use a separate access point for public, non-secured access, such as WiFi for guests or customers.
- When feasible, enable media address control (MAC) filtering and enter the MAC addresses for all the wireless devices.

APPENDIX 7 – HARDENING AND COMPUTER ISSUES

Hardening
Hardening involves taking additional actions to make it more difficult to obtain unauthorized access or to circumvent security mechanisms.

Physical Computer
Implement additional steps to harden computers against unauthorized access:

- If computers with DVD drives are readily accessible, fit locks or remove the DVD drives. Disable unused USB ports to prevent USB drives or other uncontrolled devices from being connected to the system. Such devices may be used to introduce a virus or other malware. Also disable or physically protect the power button to prevent unauthorized use.
- Set the BIOS to boot only from the operating system's root partition/drive.
- Set a BIOS password (ensure that this does not prevent automatic startup).
- Remove the floppy and CD/DVD drives from the computer.
- Disable USB ports and other ports capable of being used for memory sticks and other portable storage devices.

- Prevent drives, like the DVD drive, from being visible to Microsoft Windows Explorer by using the group policy.
- See Using Group Policy Objects to hide specified drives at http://support.microsoft.com/kb/231289 for more information.
- Note, however, that hiding the drives in Windows Explorer does not prevent those drives from being accessed using a command prompt.

Operating System
Many additional configuration options can be applied to harden the operating system against threats.

The following recommendations apply to desktop security policy settings:
- Configure Windows to display a warning against unauthorized use of the computer.
- You can configure computers to display a message when someone logs on. A typical message would be “It is an offense to continue without proper authorization.” Historically, legal prosecutions of intruders have failed because no such warning was displayed. The banner can be defined using Group Policy or the local registry.
- Use Group Policy (if the computer is part of a Windows domain) or the local registry to: Hide the last user name on the logon window. By default, the Logon dialog box displays the name of the last user to log on. This saves time if the same user is logging on again.

APPENDIX 8 – 3G/4G DATA MODEM/ ROUTER INSTALLATION

If a 3G/4G Data Modem/Router is to be used instead of the corporate LAN, configuration and password information needs to be planned and documented.

The signal strength at the installation location should be established with a test 3G/4G Router using the wireless provider in the actual installation location. The signal strength should be at or exceed 3 bars at Modem/Router for greater than 95% of a day.

Maximum reliability of 3G/4G Data Modem/Router may require an external antenna be located outside and connected to the Digital broadband router.

Home and Building Technologies

In the U.S.:

Honeywell

1985 Douglas Drive North

Golden Valley, MN 55422-3992

customer.honeywell.com

Honeywell

31-00131—01 M.S. 05-17
Printed in United States