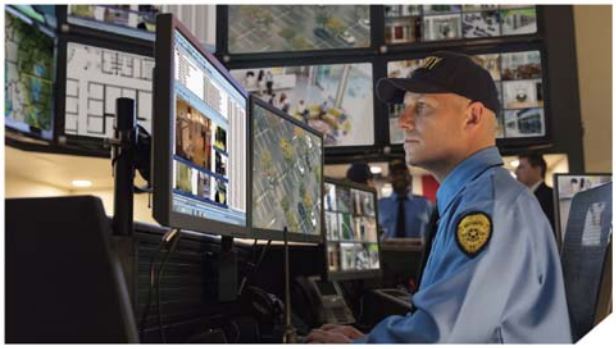
OnGuard® 7.4

Hardening Guide





LENEL
United Technologies

Lenel® OnGuard® 7.4 Hardening Guide
This guide is item number DOC-8000-EN-US, revision 8.010, August 2018.

Product Warnings and Disclaimers

THESE PRODUCTS ARE INTENDED FOR SALE TO, AND INSTALLATION BY, AN EXPERIENCED SECURITY PROFESSIONAL. UTC FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY "AUTHORIZED DEALER", IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL SECURITY RELATED PRODUCTS.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED BY UTC FIRE & SECURITY AMERICAS CORPORATION ("LENEL") "AS IS". LENEL MAKES NO WARRANTIES OR CONDITIONS OR REPRESENTATIONS OF ANY KIND WHETHER EXPRESS OR IMPLIED, AND LENEL, ITS PARENT, AFFILIATES AND SUPPLIERS EXPRESSLY DISCLAIM THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND THOSE ARISING BY STATUTE OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT, LACK OF VIRUSES OR BUGS, ACCURACY OR COMPLETENESS OF RESPONSES OR RESULTS WITH REGARD TO THE SOFTWARE. LENEL AND ITS PARENT, AFFILIATES AND SUPPLIERS DO NOT REPRESENT OR WARRANT THAT THE SOFTWARE WILL MEET ANY OR ALL OF ANY ORGANIZATION'S PARTICULAR REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE OR UNINTERRUPTED OR THAT THE SOFTWARE WILL PREVENT OR MINIMIZE OCCURRENCES OF PROPERTY DAMAGE, THEFT, LOSS OR PERSONAL INJURY. LENEL AND ITS PARENT, AFFILIATES AND SUPPLIERS FURTHER DISCLAIM ANY OTHER IMPLIED WARRANTY UNDER THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT OR SIMILAR LAW AS ENACTED BY ANY STATE.

LENEL DOES NOT REPRESENT THAT THE SOFTWARE OR ITS RELATED SERVICES MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED. LENEL WILL NOT BE LIABLE FOR UNAUTHORIZED ACCESS (I.E. HACKING) INTO THE CLOUD SERVERS OR YOUR TRANSMISSION FACILITIES, PREMISES OR EQUIPMENT, OR FOR UNAUTHORIZED ACCESS TO DATA FILES, PROGRAMS, PROCEDURES OR INFORMATION THEREON, UNLESS AND ONLY TO THE EXTENT THAT THIS DISCLAIMER IS PROHIBITED BY APPLICABLE LAW.

THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. LENEL ASSUMES NO RESPONSIBILITY FOR INACCURACIES OR OMISSIONS AND SPECIFICALLY DISCLAIMS ANY LIABILITIES, LOSSES, OR RISKS, PERSONAL OR OTHERWISE, INCURRED AS A CONSEQUENCE, DIRECTLY OR INDIRECTLY, OF THE USE OR APPLICATION OF ANY OF THE CONTENTS OF THIS DOCUMENT.

THIS PUBLICATION MAY CONTAIN EXAMPLES OF SCREEN CAPTURES AND REPORTS USED IN DAILY OPERATIONS. EXAMPLES MAY INCLUDE FICTITIOUS NAMES OF INDIVIDUALS AND COMPANIES. ANY SIMILARITY TO NAMES AND ADDRESSES OF ACTUAL BUSINESSES OR PERSONS IS ENTIRELY COINCIDENTAL.

For more information on warranty disclaimers and product safety information, please check https://www.utcfssecurityproducts.eu/productwarning/ or scan the following code:

Table of Contents

CHAPTER 1

Introduction

Scope of this Guide

Below is a brief description of the type of information covered in this hardening guide.

Chapter 1: Introduction
This section covers hardening basics and prerequisite skills, identifies industry-accepted tools and guidelines, and defines the architectural scope of this document.

Chapter 2: Hardening Fundamentals
This section provides hardening guidelines for areas outside of the OnGuard® system, such as the network, operating system, database, communication ports, and protocols, that should be addressed prior to installing and hardening the OnGuard system.

Chapter 3: OnGuard Application Server Hardening
This section provides hardening guidelines for specific OnGuard-related servers and applications, including removing services, closing ports, and reviewing the default configuration of any additional operating system, network, and application hardening specific to the related OnGuard servers.

Chapter 4: Device Communication Hardening
This section provides hardening guidelines for communication between OnGuard and the Lenel Access Series controllers and downstream interface modules, including identifying critical information on features, options that should be enabled, and best practices for using the controller.

Appendix A: System Diagram
This section consists of a system diagram that depicts the installation of OnGuard in a hardened environment.

Appendix B: Ports and Endpoints
This section identifies and defines the server sockets and associated operating system privileges that pertain to an OnGuard system.

Appendix C: Scope of OnGuard Features for a Highly Secured Environment
This section lists the features that are not included in this document for the hardening of an OnGuard system in a highly secured environment.

Acronyms Used in this Document

AES
Advanced Encryption Standard

CEIP
Customer Experience Improvement Program (Microsoft®)

CN
Common Name

CIS
Center of Internet Security®

CSRF
Cross-site Request Forgery

DIP
Dual In-line Package

DCOM
Distributed Component Object Model (Microsoft)

DDOS
Distributed Denial of Service

DEK
Database Encryption Key

DMZ
Data Management Zone

DNS
Domain Name Service

DOS
Denial of Service

EAP
Extensible Authentication Protocol

EEPROM
Electrically Erasable Programmable Read-Only Memory

EKM
Encryption Key Manager

FQDN
Fully Qualified Domain Name

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol Secure

IIS
Internet Information Services (Microsoft)

IP
Internet Protocol

ISO
International Organization for Standardization

IT
Information Technology

IVAS
OnGuard® IntelligentVideo™ Application Server

IVS
OnGuard IntelligentVideo Server

LED
Light Emitting Diode

LS
Lenel Service

MIME
Multipurpose Internet Mail Extensions

NIC
Network Interface Card

NIST
National Institute of Standards and Technology

NVR
Network Video Recorder (Lenel)

OEM
Original Equipment Manufacturer

OSDP
Open Supervised Device Protocol™ (access control)

OWASP
Open Web Application Security Project

PII
Personally Identifiable Information

QPID
Qwest Protected Internet Delivery (data transport interface)

RSA
Rivest, Shamir, & Adleman (public key encryption technology)

SANS
SysAdmin, Audit, Network and Security Institute

SHA
Secure Hash Algorithm

SNMP
Simple Network Management Protocol

SSL
Secure Sockets Layer

TDE
Transparent Data Encryption

TLS
Transport Layer Security

VLAN
Virtual Local Area Network

XSS
Cross-site Scripting

Overview

This document has been created primarily for OnGuard system administrators and IT and security administrators who are responsible for the technical aspects of securing OnGuard servers. It is to be used as a companion document to the OnGuard Installation Guide (DOC-110).

IMPORTANT: Each installation (installer/administrator) should understand the system usage requirements and compliance directives to determine the hardening configuration applicable to client requirements. You should take your specific environment into consideration before applying recommendations and make efforts to secure additional elements of your environment as well.

The practices recommended in this document are designed to help mitigate the risks associated with servers. They build on and assume the implementation of practices described in the NIST publications on system and network security.

Ensure that all customer IT regulations are considered when applying the hardening guidelines covered in this document. Some guidelines will require you to:

- Disable one or more ports
- Stop one or more services
- Remove one or more features of the operating system
- Uninstall software
- Locked down shares
- Disable access to Null sessions/anonymous connections
- Ensure all patching is current
- Ensure virus detection, malware and personal firewall software is installed
- Enable strong password and least privilege policies
- Ensure sufficient logging enabled
- Enable effective Microsoft® Active Directory® design and management
- Enable encryption for data “at rest” and in transit

Guidelines also involve changing or turning off default settings and removing unnecessary features or applications. For example, some computers come with software pre-installed that are unnecessary or may expose the system to unnecessary security exposures. For more information about the pre-installed software, refer to its documentation.

This document will cover the steps and guidelines that should be implemented and maintained in the OnGuard environment with the goal of placing the environment in a recommended secure state.

These guidelines were developed using highly recognized industry standards, applicable third-party recommendations, and security hardening best practices. Before proceeding with hardening of any system, there are some key points to be aware of:

- Understand what you have and how it is at risk. It is recommended that you perform an information risk assessment (in-house or via an independent expert) that looks at both technical and operational issues related to the security of your environment.
- Hardening standards should not be construed as one-size-fits-all. Every network and server is different. It all depends on your line of business, the regulations that you are governed by, the risks, the criticality of each server and the information it stores and/or processes.
- The customer OnGuard environment may contain necessary third-party or customer-specific integrations that could be affected when the system is hardened.

Prerequisite Skills

The material in this document is technically oriented, and it is assumed that readers have at least a basic understanding of system and network security, and have a basic understanding of the following:

- Installing software on server and client computers
- Basic knowledge of operating systems, including configuration of and management tools
- Basic knowledge of Microsoft Active Directory Domain Services (AD DS), Microsoft® SQL Server® database software, and Microsoft Exchange Server
- How to set up and configure dependent technologies such as AD DS, SQL server, Microsoft® SharePoint® services, and Microsoft Exchange Server
- Basic knowledge of enabling or disabling protocols, ciphers, hashes, and key exchange algorithms

Note: For a complete list of supported firmware, operating systems, database software, and other third-party components, refer to the versioning information in the OnGuard Release Notes (DOC-10120-EN-US), or the compatibility charts on the Lenel web site: https://partner.lenel.com/downloads/onguard/software. Once there, select **Compatibility Charts** from the **Choose type of download** menu.

Recommended Industry Tools

Throughout this document, there are references to common third-party or open source tools that may be useful during a particular hardening step.

Note: These tools should be considered as examples only and are neither provided nor supported by Lenel. Review any such tool carefully and make choices based on your company policies. Any resulting issues while using such tools should be directed to the third-party vendor of that tool.

Steps to Hardening Your OnGuard System

Hardening your OnGuard applications is only one step in securing your environment. Taking the below hardening steps should be part of a comprehensive “defense-in-depth” security plan:

1. Plan the installation and deployment of the operating system and other components for the server.
2. Install, configure, and secure the underlying operating system.
3. Install, configure, and secure the server software.
4. Ensure that all servers are installed in a physically secure environment.
5. Use strong passwords.
6. Follow “least privilege” privilege assignments and segmentation of duties for operating system accounts and OnGuard user accounts.
7. Ensure all critical servers/services are part of your business continuity and disaster recovery plan.
8. Employ appropriate network protection mechanisms (e.g., firewall, packet filtering router, and proxy). Choosing the mechanisms for a particular situation depends on several factors, including the location of the server's clients (e.g., Internet, internal, and remote access), the location of the server on the network, the types of services offered by the server, and the types of threats against the server.
9. Employ secure administration and maintenance processes, ensuring application of patches and upgrades are up to date for both software and firmware, monitoring of logs, backups of data and operating system, and periodic security testing.
10. Maintain proper alerts, records and logs. This information can be used to alert of a potential attack, as legal and forensic evidence, part of recovery plan, for continuous improvement.
11. Implement ongoing security training practices.

Industry Accepted Guidelines

Below is a list of organizations that publish common industry-accepted standards that include specific guidelines relevant to system hardening:

- Center of Internet Security (CIS)
- International Organization for Standardization (ISO)

- National Institute of Standards and Technology (NIST)
- Open Web Application Security Project (OWASP)
- SysAdmin, Audit, Network and Security (SANS) Institute

Architectural Assumptions of Scope

The architectural guidelines that follow identify the environmental conditions used during the development and testing of this hardening guide. As OnGuard can be deployed in many and varied environments, you may find that your environment has elements not referenced within this scope.

IMPORTANT: You should take your specific environment into consideration before applying recommendations and make efforts to secure additional elements of your environment as well.

Updates to this document may be published periodically, as the OnGuard product evolves and as new software releases are commercialized for use.

The scope of this hardening guide includes:

- OnGuard Enterprise environment with services, servers, and access control devices based on support included with OnGuard 7.4. Video support and devices are not included at this time.
  - For a list of Lenel Access Series controllers and downstream interface modules considered in this guide, refer to Hardware Scope on page 15.
  - For a list of applications considered in this guide, refer to Software Scope on page 16.
  - For a list of legacy services exceptions excluded from hardening considerations, refer to Deployment of OnGuard in a Highly Secure Environment on page 17.
- For the support of integration to the OnGuard environment, the solution provides the Lenel® OpenAccess API (and Lenel® DataConduIT API) for custom application access, as well as Lenel® DataExchange for scripted data import/export operations. When using these integration methods, it is the responsibility of the entity making the connection to ensure that security practices are observed to protect the data entered or removed into the system.
- Microsoft Server 2016 configured with a benchmark-hardened Level 1 v1.0.0.13-L1 virtual image from the Center for Internet Security, Inc. (CIS) that meets the minimum and essential security requirements. The CIS benchmark configuration setting for Microsoft Server 2016 is available at https://www.cisecurity.org/benchmark/microsoft_windows_server/.
- To support encryption of data “at rest,” it is necessary to select a version of Microsoft SQL Server that supports Transparent Data Encryption (TDE).

Hardware Scope

Various generations of intelligent system controllers and interface modules exist within the Lenel Access Series product portfolio. Product capabilities improve over time and therefore some security parameters and hardening instructions differ across products. The following intelligent system controllers and interface modules are covered in this hardening guide.

Lenel Access Series Controllers

LNL-2210, LNL-2220, LNL-3300, LNL-4420

Series-3 Downstream Interface Modules
LNL-1100-S3, LNL-1200-S3, LNL-1300-S3, LNL-1320-S3

Series-2 Downstream Interface Modules
LNL-1100, LNL-1200, LNL-1300, LNL-1300e, LNL-1320

Migration Bridge Controllers
LNL-2240-RS4, LNL-3300-ACUXL, LNL-3300-GCM, LNL-3300-M5

Note: The migration bridge controllers follow the Access Series functionality in this hardening guide.

Software Scope

This section identifies the thick and thin client applications, and the servers and services covered in this hardening guide of the OnGuard environment. For more information on the OnGuard environment, refer to System Diagram on page 57 and Ports and Endpoints on page 59.

OnGuard Thick Client Applications

OnGuard consists of a set of thick client applications that can be individually installed and licensed on the OnGuard workstation to meet the needs of the user at that workstation:

- Alarm Monitoring
- Area Access Manager
- Badge Designer
- Forms Designer
- ID Credential Center
- Map Designer
- Replication Administration
- Replicator
- System Administration
- Video Viewer
- Visitor Management

Note: To reduce the attack surface of your OnGuard system, install only the thick client applications that are required to support the user at that location.

OnGuard Thin Client Applications

The OnGuard system can be enhanced by a set of web-based thin clients applications that are individually licensed and installed on the OnGuard server:

- OnGuard Access Manager
- OnGuard Cardholder Self Service
- OnGuard Credentials
- OnGuard Monitor

Note: To reduce the attack surface of your OnGuard system, install on the server only the thin client applications that you expect to be used on your system.

OnGuard Servers and Services

The following servers and services are installed with OnGuard:

- LS Client Update Server
- LS Communication Server
- LS Config Download Service
- LS DataConduIT Message Queue Server
- LS DataConduIT Service
- LS DataExchange Server
- LS Event Context Provider
- LS Global Output Server
- LS ID Allocation
- LS License Server
- LS Linkage Server
- LS Login Driver
- LS Message Broker
- LS Module Manager
- LS Lenel OpenAccess
- LS Replicator
- LS Site Publication Server
- LS Web Event Bridge
- LS Web Service

Deployment of OnGuard in a Highly Secure Environment

This document focuses on the promotion of security and sustaining solutions for customers. This document covers several applications, features, practices, and recommendations in the optimization of OnGuard security defenses. If you require the implementation of additional features for legacy web technologies that do not support the level of security that today's customer systems require, refer to the documentation for the legacy web technologies. Lenel continues to replace these applications in future releases of OnGuard. For a complete list of legacy web technologies, refer to Appendix C: Scope of OnGuard Features for a Highly Secured Environment on page 67.

CHAPTER 2

Hardening Fundamentals

Overview

This section provides hardening guidelines for areas outside of the OnGuard system, such as the network, operating system, database, communication ports, and protocols, that should be addressed prior to installing and hardening the OnGuard system.

Protocols

Hardening TLS Against Man-in-the-Middle (MITM) Attacks

It is important for system administrators to secure their networks and machines for TLS to be able to protect the data in transit. Although TLS can provide strong encryption, subverting this on Microsoft® Windows® can be accomplished if an attacker can install their own private key in the trusted root store and deploy a transparent proxy. Once this is done all data being transported, including credentials, can be vulnerable to modification and exfiltration.

For more information, refer to the following article from Microsoft TechNet: https://technet.microsoft.com/en-us/library/dd277328.aspx.

TLS 1.2

The following recommendations reflect an application of NIST 800-52r1 and related best practices to hardening TLS/SSL settings for Microsoft Windows client and server operating systems.

Notes: Some organizations contain a mix of newer and older operating systems. To avoid any connectivity disruptions to older systems, standard practice is to start with the highest security levels and then enable lower security levels until a level that works best with the intended user base is reached.

The list of available features changes across Microsoft Windows versions and updates. The naming conventions of some features across versions has changed as well. The features listed below may not be available on all versions of Microsoft Windows.

Protocols

Enable TLS 1.2.

Disable the following: TLS 1.1, TLS 1.0, SSL 3.0, SSL 2.0, and PCT 1.0.

Cipher Suites

The following ciphers are listed in sets of comparable security, in decreasing order of strength. Ideally, only the first set should be enabled, however there is a risk that connectivity could be disrupted. If necessary, enable the second set to connect users and continue, only if absolutely necessary.

IIS Crypto is a free tool that allows administrators to enable or disable protocols, ciphers, hashes and key exchange algorithms on Microsoft® Windows Server® 2008, 2012, and 2016. For more information about IIS Crypto, refer to https://www.nartac.com/Products/IISCrypto.

Note: Unless absolutely needed for connectivity to older systems, disable any ciphers not listed below to reduce system vulnerability.

TLS 1.2 AEAD SHA-2 only:

- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS 1.2 SHA2 (non-AEAD):

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256

TLS 1.0 and 1.1 with modern ciphers and outdated hashes:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS 1.0 and 1.1 with older but still reasonable ciphers and outdated hashes:

- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

In addition to the high security cipher suites, the following cipher suites should be enabled to support the strongest security currently available for the Lenel Access Series controllers. As newer releases of firmware become available (at https://partner.lenel.com/downloads/hardware/firmware), it is recommended to install them as soon as possible, and to refer to the firmware release notes to see if updated ciphers are available.

IMPORTANT: If you are using an LNL-4420, enable the TLS_RSA_WITH_AES_256_CBC_SHA256 cipher suite. If you are using any other Lenel Access Series controller, enable the following cipher suites: TLS_RSA_WITH_AES_256_CBC_SHA and TLS_RSA_WITH_AES_128_CBC_SHA.

Digital Certificates

To best support TLS/SSL, a strong private key is needed to prevent attackers from carrying out impersonation attacks. Equally important is to have a valid and strong certificate, allowing the private key the right to represent a particular hostname.

Administrators should generate unique TLS/SSL keys per service and store these keys in secure ways to prevent casual access. Consider using a hardware security module (HSM) to secure digital keys.

Consult Microsoft Windows key management practices for guidance on securing keys. Keys should be generated on a trusted computer with sufficient entropy. Ensure these keys are signed by a trusted certificate authority and follow all guidelines set forth by NIST, such as using an industry-accepted cryptography. Always password-protect keys and if compromised, revoke certificates and generate new keys.

For networks using the Microsoft Windows Internet Name Service (WINS) architecture, refer to the following sections in the OnGuard Installation Guide (DOC-110):

- “Configure SSL”
- NGINX (LS Web Server) sub-section in “OnGuard and the Use of Certificates”

Note: The OnGuard Installation Guide is available on the Lenel Web Site: https://partner.lenel.com/downloads/onguard/user-guides. (You will need your Lenel login to gain access to this site.) When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

For networks using the Domain Name Service (DNS) architecture, the Common Name (CN) must use the Fully Qualified Domain Name (FQDN) and not the host name. For more information, refer to instructions from Microsoft on setting up FQDN.

OnGuard Services

Since the OnGuard services (**LS*.exe**) are run as the LocalSystem account or local administrator account, it is recommended that the logon user (the server account) be an elevated privileged account.

Unnecessary Services and Files

Since unnecessary services provide additional opportunities for an attacker to gain access to a system, it is important that administrators review their business and operational needs for services that are not necessary for the operation of the system. It is possible that the operating system retains some services, but they are not needed for the operation of the system. For example, all versions of SQL Server include the Microsoft Customer Experience Improvement Program (CEIP). Although this service is not needed to operationally support OnGuard, administrators should review the purpose of the service and determine if it is necessary for their business needs.

Services that are not vital to the operation of the system may include undetected vulnerabilities. Because these services are not considered vital, they may not be monitored for patches and updates. Additionally, the system's end user may not be aware of the existence of certain non-vital services, and therefore may not provide or apply sufficient controls to safeguard the system against any vulnerabilities present in these non-vital services.

It may not be sufficient to simply disable or turn off unnecessary services. The existence of the service can be leveraged by an attacker in order to simplify an exploit of an unrelated vulnerability. For example, an attacker can use a command injection to execute a command on the system and further gain a foothold to elevate privileges.

It is recommended that administrators at least disable, or preferably, remove all unnecessary services on the system, prior to placing the OnGuard system in production. Use a network scanning tool, such as **nmap**, to ensure the services are actually disabled. It is not best practice to use only a firewall as a means of disabling certain services. The problem with using a firewall only is that an attacker may gain access to localhost services, once a foothold is established on the system. Access to localhost services may allow an attacker to further compromise the system in ways that would otherwise not be possible. Further, the firewall may be disabled by accident in the future or on purpose by an attacker with a foothold on the system.

Microsoft Customer Experience Improvement Program (CEIP)

The Customer Experience Improvement Program (CEIP) is used by Microsoft Windows to collect and send information to Microsoft. This information includes, but is not limited to, the following:

- Program crashes
- The performance of different components in Microsoft Windows
- System configuration
- Which programs are being used
- The number of network connections in use

Periodically, CEIP also uploads a small file to Microsoft servers containing a summary of the information collected.

CEIP does not collect or send any personally identifiable information (PII).

CEIP is enabled by default, but it can be disabled. To disable CEIP, refer to documentation provided by Microsoft.

Unnecessary Files on the OnGuard System

While the following files do not pose any security threat or vulnerability to the integrity of the OnGuard system, they are not needed and can be safely removed or edited.

1. On the workstation or server where OnGuard is installed:
   a. Go to ***C:\Users***\, and open the folder that matches your Microsoft Windows username.
   b. Locate the OnGuard **installation.log** files and delete them.

      If OnGuard has been re-installed or upgraded, there may be files for each version of OnGuard that was installed. For example, **OnGuard_7_3_Installation.log** and **OnGuard_7_4_Installation.log**.
   c. Locate the **Lnl.OG.WebEventBridgeService.exe.config** file and open it in a text editor.
   d. Scroll to the `<appSettings>` section and delete the following lines:
      - `<add key="Username" value="guest" />`
      - `<add key="Password" value="guest123" />`
   e. Save the changes made and close the file.
2. On each workstation where OnGuard Cardholder Self Service is installed, go to ***C:\Program files (x86)\OnGuard\CSS\api\config***.
3. Locate and delete the following files:
   - **test.json**
   - **e2e.json**

CHAPTER 3

OnGuard Application Server Hardening

Overview

This section provides hardening guidelines for specific OnGuard-related servers and applications, including removing services, closing ports, and reviewing the default configuration of any additional operating system, network, and application hardening specific to the related OnGuard servers.

To see how OnGuard is installed in a hardened environment, refer to Appendix A: System Diagram on page 57.

Isolating the OnGuard Resources within a VLAN

While it is common for organizations to run all of their network infrastructure on a topology that handles security segmentation through a few well-placed firewalls (such as public-to-DMZ-to-Internal-to-Higher Security), another approach offering significantly higher security is the utilization of a Virtual LAN (Local Area Network). A VLAN allows a subset of network infrastructure to operate on a network that is normally isolated from all other networks by leveraging the capabilities of managed switches.

There are several security benefits when using a VLAN as another layer of defense to isolate your OnGuard resources, such as:

When used as an additional layer of defense to isolate your OnGuard resources, a VLAN can:

- Significantly reduce the attack surface against attackers who have penetrated parts of the local network.
- Restrict access to sensitive data by placing only those users who have access to the data on the VLAN, thus reducing the chances of an outsider gaining access to the data.
- Control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion.
- Help defend OnGuard against threat vectors inherited from older Microsoft and third-party technologies that do not have updated replacements.

Since a VLAN is highly dependent on the vendor, the selection of network equipment, and local topologies, its design and deployment is not covered in this document. However, in general terms, the standard practice may consist of the following steps:

1. Define a new (private or isolated) VLAN within your network administration tools.
2. If the VLAN is not isolated, configure a DMZ rule for VLAN access; for partial isolation, configure a jumpbox.
3. Migrate all of the clients, servers and network-attached devices to the VLAN.

Databases

Encrypting the Database

To support encryption of data “at rest,” it is necessary to select a version of Microsoft SQL Server that supports Transparent Data Encryption (TDE).

TDE performs real-time I/O encryption and decryption of the database and database log files.

The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data “at rest,” meaning the data and log files.

TDE does not provide encryption across communication channels.

For more information about TDE and how to enable it in an OnGuard environment, refer to the OnGuard Advanced Installation Topics (DOC-100).

Enabling TLS/SSL Encryption for an Instance of SQL Server

To support encryption of data “in flight,” it is necessary to encrypt the communication between the ODBC driver on the client and the SQL Server. This is accomplished by enabling TLS/SSL encryption at the SQL Server.

To enable TLS/SSL encryption for SQL Server using Microsoft Management Console, follow the steps provided by Microsoft: https://support.microsoft.com/en-us/help/316898/how-to-enable-ssl-encryption-for-an-instance-of-sql-server-by-using-mi

SQL Server Database Roles

The database account used by the Lenel thick client has SYSADMIN privileges on the target database. As a result, all databases on the target database can be accessed, and potentially compromised, by a SYSADMIN account. This account can also execute commands on the installed operating system, which can result in a full compromise of the operating system.

A user who has successfully compromised the database credentials can abuse the SYSADMIN privileges to compromise not only the Lenel database, but other databases residing on the same server and installed operating system.

It is recommended that the permissions of the Lenel database user are changed during the installation of the OnGuard system.

Note: For general, everyday use of OnGuard, the Lenel user does not need the SYSADMIN role.

1. In SQL Server Management Studio, expand the Security tab and select **Logins**.
2. Locate the database accounts that OnGuard uses.
   - Database account creating during OnGuard installation
   - Service account

     This account is typically the logon account that is used to run the following services:
     - LS Application Service
     - LS Client Update Server
     - LS Event Context Provider
     - LS Site Publication Server
3. For each account specified in Step 2, right-click on the account name and select **Properties**.
4. Select **Server Roles**.
5. Clear the check boxes for **serveradmin** and **sysadmin**.
6. Select the OnGuard database.
7. Specify the following role memberships for the given user account:
   - **public**
   - **db_datareader**
   - **db_datawriter**
   - **db_ddladmin**
   - **db_executor**

Note: If the db_executor role does not exist, it must be created in the Object Explorer pane of SQL Server Management Studio using the following SQL command:

```
CREATE ROLE db_executor
GRANT EXECUTE TO db_executor
```

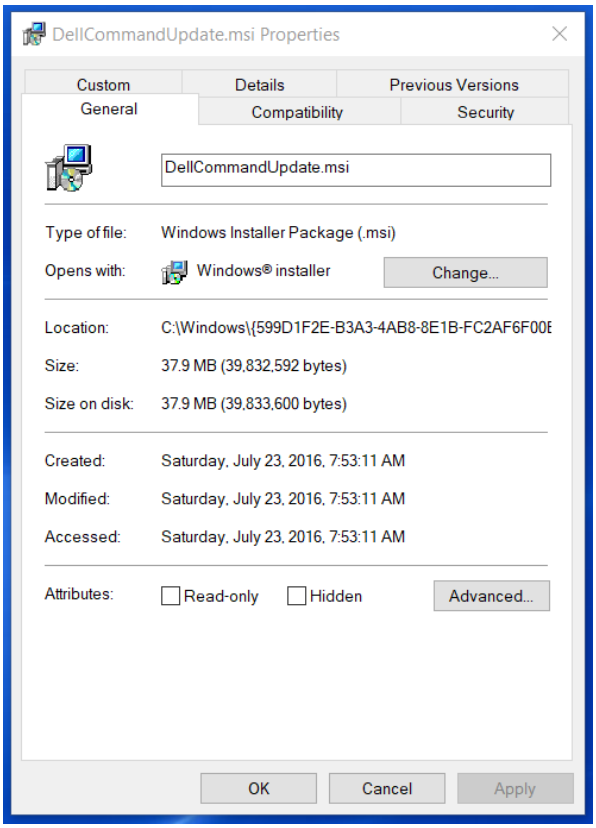
8. Click **OK** to apply the changes made.

Lenel Installation Packages

Use the following steps to verify that the certificate issued by VeriSign for a Lenel installation package is valid and can be trusted.

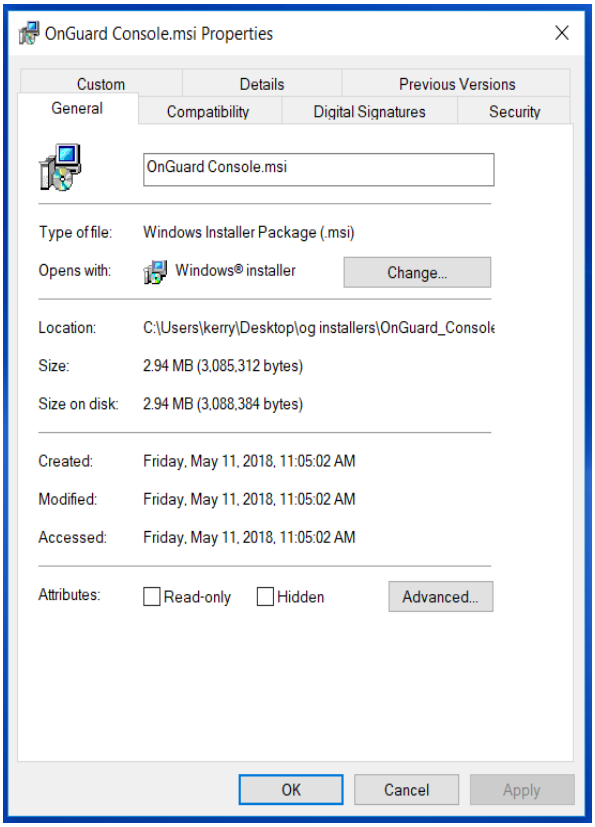
1. Using Windows Explorer, view the **.msi** file.
2. Right-click on the **.msi** file.
3. Select **Properties**.
4. Verify that the **Digital Signatures** tab is present. If it is not, the installer is not signed and should not be trusted.

Unsigned .MSI File



5. Select the **Digital Signatures** tab.

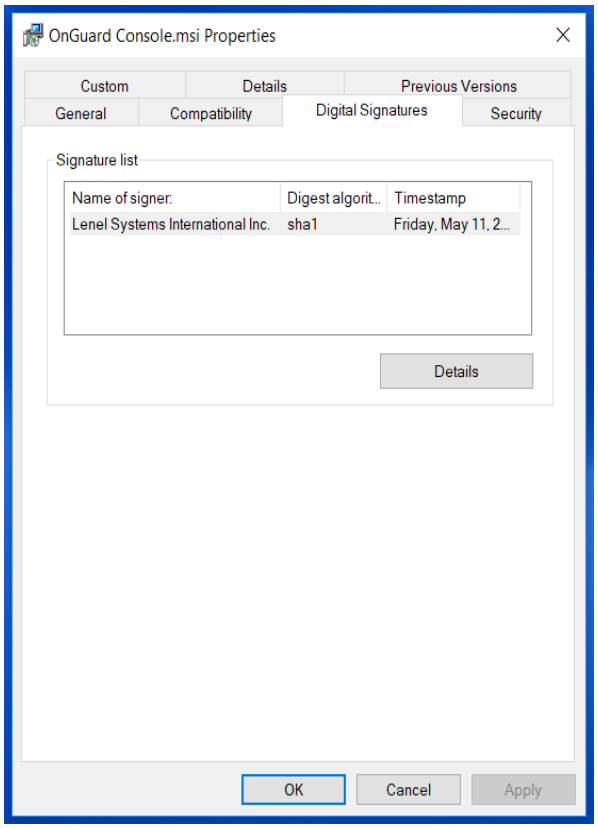
Signed .MSI File



6. Under **Signature list**, verify that an entry named "Lenel Systems International, Inc." is present. If not, the installer was not signed by Lenel and should not be trusted.

Note: A new code signing certificate is in process and it will reflect the official company name of "UTC Fire & Security Americas Corporation, Inc."

Digital Signatures Tab

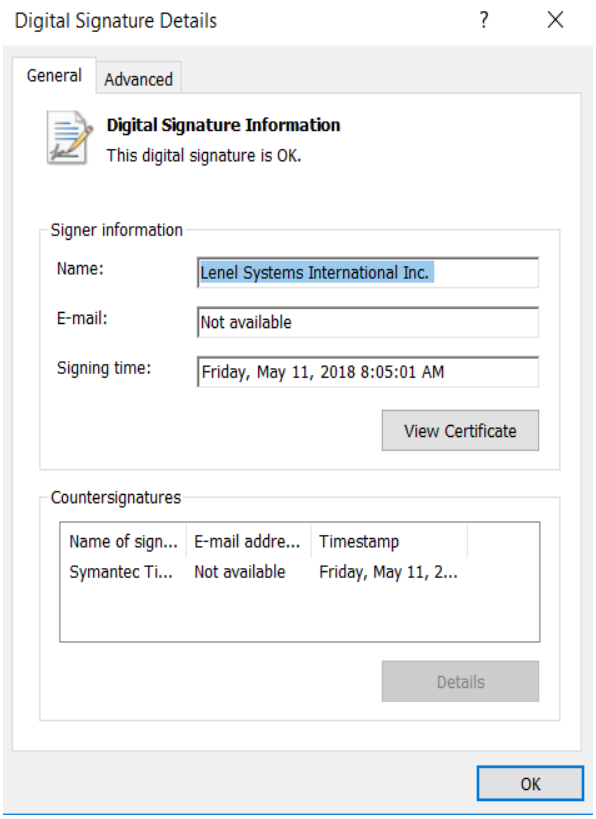


7. Select the “Lenel Systems International, Inc.” signature line and click **Details**.

Note: A new code signing certificate is in process and it will reflect the official company name of “UTC Fire & Security Americas Corporation, Inc.”

8. On the **General** tab under **Digital Signature Information**, a line that states “This digital signature is OK” should be present. If not, then the signature is invalid and the installer should not be trusted.

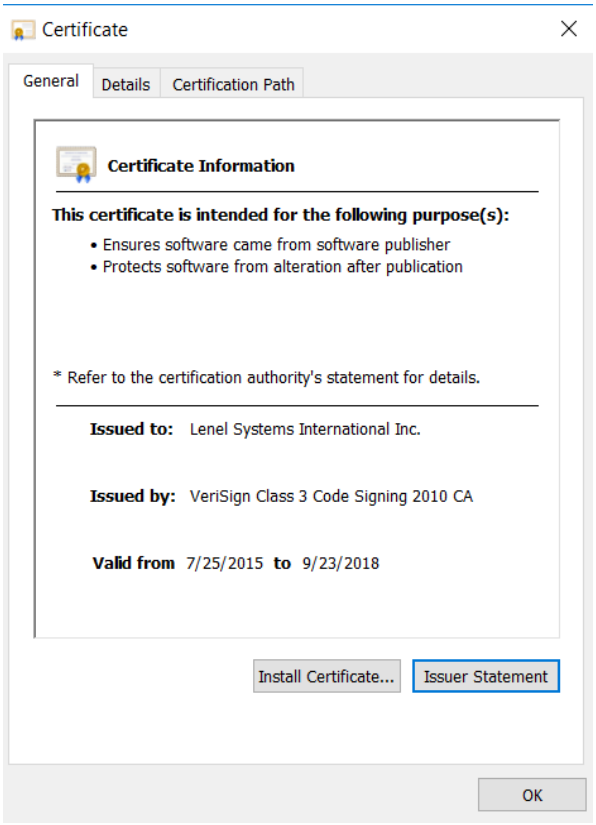
Digital Signature Details



9. Click **View Certificate**.
10. On the **General** tab, a line that starts with “Issued By: VeriSign Class 3 Code Signing” should be present. If not, then the certificate is not signed by the certification authority used by Lenel and should not be trusted.

Note: A new code signing certificate is in process and it will reflect the official company name of “UTC Fire & Security Americas Corporation, Inc.”

Certificate Information



11. If the installation package from Lenel successfully passes each of these steps, it can be assumed that the certificate issued by VeriSign to Lenel is valid and can be trusted.

Note: A new code signing certificate is in process and it will reflect the official company name of "UTC Fire & Security Americas Corporation, Inc."

OnGuard Servers, Services, and Utilities

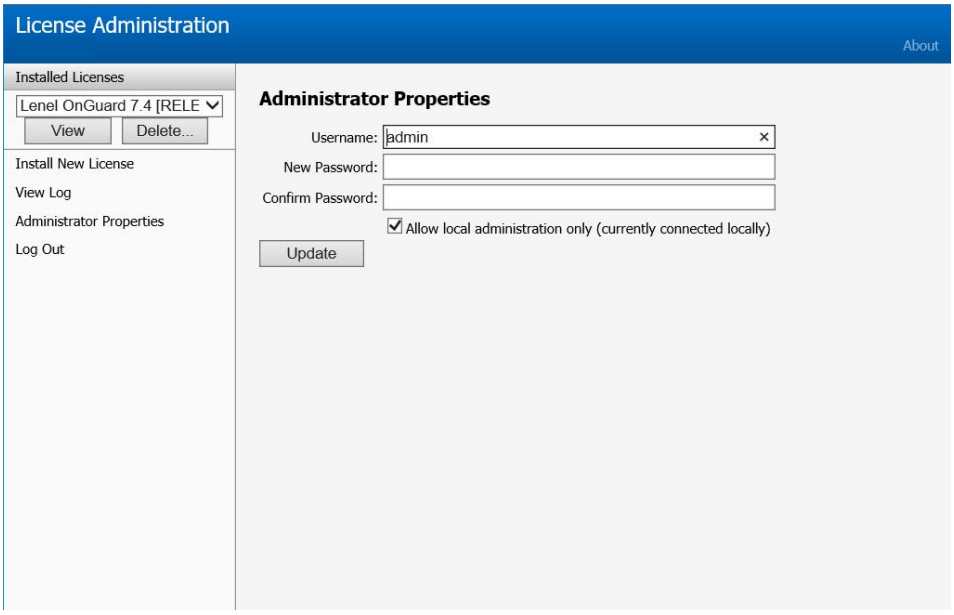
License Server

By default, the License Server is configured to be used across a network. In a hardened system, such operation should be disallowed. Follow the steps below to configure the License Server to only operate from a local system.

1. Select ***Start*** > ***OnGuard 7.4*** > ***License Server.***
2. Right-click on **License Server** and select **Run as administrator**.
3. To access the License Server user interface, enter **http://localhost:9999** into a web browser.
4. Enter a valid username and password.
5. From the menu, select **Administrator Properties**.
6. Click the **Allow local administration only** check box.

   This option can only be activated when logged in from the local server.

License Administration Administrator Properties



7. Click **Update**.

   The License Server is now hardened.

QPID Message Broker

The QPID Message Broker does not authenticate users, but there are credential application settings for the Message Broker. These credentials are not used in OnGuard. However, to ensure that the OnGuard system is properly hardened, remove the following app settings from the **Lnl.OG.WebEventBridgeService.exe.config** and **Lnl.OG.EventContextProviderService.exe.config** files:

- **<add key="Username" value="guest"/>**
- **<add key="Password" value="guest123"/>**

NGINX Web Service

To provide additional application-level defenses against DOS/DDOS attacks targeting your web server, add the following settings to your NGINX configuration.

In OnGuard, the NGINX configuration file is located at ***C:\ProgramData\Lnl\nginx\conf\nginx.conf***.

Add the following lines to the http and its server block:

```
http {
  limit_conn_zone $binary_remote_addr zone=conn_limit_per_ip:10m;
  limit_req_zone $binary_remote_addr zone=req_limit_per_ip:10m
rate=5r/s;


  server {
```

```
    limit_conn conn_limit_per_ip 10;
    limit_req zone=req_limit_per_ip burst=10 nodelay;
  }
}
```

For more information, visit the following websites:

http://nginx.org/en/docs/http/ngx_http_limit_conn_module.html

http://nginx.org/en/docs/http/ngx_http_limit_req_module.html

Login Driver

It is strongly recommended to change the default password for the Login Driver. For more information, refer to “Change the Database Password” in the OnGuard Installation Guide (DOC-110).

The default Login Driver user name for the database is “Lenel.” While this user name can be changed at installation, it should only be changed if compliance with your organization’s IT guidelines prohibits the use of default user names. If the name is changed, make sure to update or create a corresponding user account in the database.

OnGuard Security Utility

The Security Utility in OnGuard is designed to ensure that the correct configurations for the Windows operating system are enabled so that the OnGuard client or server functions as expected.

Security Utility functionality is embedded into Setup Assistant. You should run Security Utility again whenever a Windows Update or Service Pack is installed on the OnGuard Server, client workstations, or Lenel NVR video recorders. For more information, refer to “Manually Running Security Utility” in the OnGuard Installation Guide (DOC-110).

The version of Security Utility that is delivered with OnGuard 7.4, or earlier versions, is not a signed file and will not run on a CIS instance of a Windows operating system. A signed version of Security Utility can be downloaded from the Lenel Web site: https://partner.lenel.com/downloads/onguard/.

In order to run Security Utility on CIS instance of a Windows operating system, a Windows policy setting may be required:

1. Open the Local Group Policy Editor by doing one of the following:
   - Simultaneously press the [Windows]+[R] keys on the keyboard, or
   - At the “Run” window, type `gpedit.msc` and press [Enter].
2. From the left pane of the Local Group Policy Editor, navigate to ***Computer Configuration*** > ***Windows Settings*** > ***Security Settings*** > ***Local Policies*** > ***Security Options***.
3. From the right pane, double-click the **User Account Control: Only elevate executables that are signed and validated** policy.
4. Change the security setting to **Disabled** and click **OK**.
5. Close the Local Group Policy Editor and restart the computer.
6. Once the computer has restarted, open and run Security Utility from the OnGuard file by clicking **Agree** and then **Apply**.
7. When the Security Utility is done, repeat Steps 1-3 to re-enable the security setting for the **User Account Control: Only elevate executables that are signed and validated** policy.
8. Close the Local Group Policy Editor and restart the computer.

Security Utility has successfully been updated. Repeat these steps when Windows or OnGuard have software updates.

Lenel software requires certain security adjustments to the operating system to function more securely. These security adjustments are listed when Setup Assistant runs. Click [Release Notes] to review a description of the changes made by the Security Utility. Upon agreeing to this disclaimer, the user assumes responsibility for any security issues that might occur due to these adjustments. The Security Utility then makes the changes automatically.

The Security Utility automatically adds the following to the Firewall Exception list:

- File and Printer Sharing groups
- All OnGuard and Video Recording applications that can receive unsolicited calls
- RPC Port 135 for Lenel NVR, IVS, and IVAS installations
- UDP Port 5000 for Lenel NVR failover
- Allow incoming echo requests
- Allows remote clients for RPC; changes RPC restrictions from High(2) to Default (1)
- Machine-wide remote and local activation and access rights to Anonymous Logon and Everyone users
- Message Broker Ports 5671 and 5672
- Web Services Port 8080
- Lenel® OpenAccess Port 8048
- Web Event Bridge Port 8049
- Site Publication Server Port 8032 (for Enterprise Installations)

The Security Utility does not open the following ports:

- SQL Port 1433
- Oracle Port 1521 TCP/IP
- SNMPv1 Ports 161 and 162

Notes: By default, the Security Utility enables all ports that are necessary for OnGuard to operate and adds them to the Firewall Exception list. Certain ports for Lenel NVR, IVS, IVAS and Remote Monitor are also opened by default. To ensure the OnGuard environment is properly hardened, all unused ports must be manually disabled.

For a single-machine installation, where the client and server are housed on the same machine and with no video recording hardware used, the Security Utility is not needed for OnGuard to function.

The Security Utility grants Anonymous Logon user remote access and activation rights in DCOM settings. To avoid this from occurring, do not authenticate remote callers as Anonymous Logon users.

To manually adjust or remove certain security exceptions in the Security Utility, changes must be made to the **sp2.xml** file. Refer to the release notes supplied with the Security Utility for more information.

Unquoted Service Paths

If an application does not correctly store execution paths in the system's registry, a user with enough permissions on the file system could insert an executable into the execution path. This vulnerability could allow a user the ability to place malicious code with a creative naming convention and gain control prior to the legitimate service.

Use the following steps to identify any unquoted paths for OnGuard services and resolve them.

1. On the workstation where the OnGuard application server is installed, open the Registry Editor.
2. Navigate to the following registry hive: ***HKEY_LOCAL_MACHINE > System > CurrentControlSet > services***.
3. Scroll to the section with the OnGuard services. The naming convention used is **LS*.exe**.

Note: The ImagePath value for the **LpsSearchSvc** service must also be updated. This service does not follow the naming convention used by other OnGuard services. It will require a separate search.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LpsSearchSvc

4. Click on the service and review the **ImagePath** row.

   If the path displayed in the **Data** column is not enclosed inside double quotation marks (“quotes”):

   a. Right-click **ImagePath**.
   b. Select **Modify**.
   c. Enclose the path displayed in the **Value** data field in double quotation marks.
   d. Click **OK**.
5. Repeat Step 4 for all other OnGuard services.
6. Save the changes made to the registry.
7. Close the Registry Editor.

OnGuard Applications

Lenel OpenAccess

When using an application built on the OpenAccess platform, there are several system-wide inactivity and timeout properties that will have the same timeout settings applied to every client of the OpenAccess server. In an Enterprise system, these properties can be configured at each region to support local usage and regulation of the applications. These properties can be configured in the **openaccess.ini** file. For more information on these properties and the **openaccess.ini** file, refer to the "OpenAccess Custom Configuration" section in the OpenAccess User Guide (DOC-1057-EN-US).

Note: It is important that the right balance is struck to optimize productivity and to minimize the exposure time period, in which an attacker can launch attacks over active sessions and hijack them. Idle and absolute timeout values are highly dependent upon whether and to what degree the application and its data are critical to the customer. Common idle timeouts ranges are 2-5 minutes for high-value applications and 15- 30 minutes for low risk applications.

Accounts and Passwords

To properly harden the OnGuard system, all default passwords must be changed to passwords that comply, at a minimum, with the password standards detailed in this hardening guide.

Default Accounts and Passwords

During initial installation of the OnGuard software, default accounts and passwords are created, which include:

Description	User name	Password	How to change the password
Default system administrator account. This is the account that is used initially to log into the main OnGuard applications, such as System Administration.	SA	SA	Refer to “Change the System Administrator Password for the Database” in the OnGuard Installation Guide (DOC-110).
OnGuard database. This is the actual OnGuard SQL Server Desktop Engine, SQL Server, or Oracle database. By default, the login name for the Lenel database is “Lenel.” It is recommended to change this at installation to change the default login name. Make sure to update or create a corresponding user account in your database.	LENEL	Secur1ty#	Refer to “Change the Database Password” in the OnGuard Installation Guide (DOC-110).
License Administration account. This is the account that is used initially to log into the License Administration application.	ADMIN	ADMIN	Refer to “Changing Administrator Properties for License Administration” in the OnGuard Installation Guide (DOC-110).

In order to properly harden the OnGuard system, the default passwords must be changed.

Note: The default accounts can be removed. The exception to this is the system administrator account (“SA”). By definition this account has permission to do anything in the system. A user with system access has unlimited access to the application. You cannot delete or change the system account except to modify the password, which you are strongly encouraged to do as soon as possible to discourage unauthorized use.

OnGuard “SA” (System Administrator) Account

By definition, this account has permission to do anything in the OnGuard system, and is intended to be used during system commissioning and management. Some advanced OnGuard features, such as adding an Enterprise region, require the OnGuard SA password. This password may also be valuable when engaging with a system integrator or Lenel Technical Support. This account and its password should not be used for general operation or shared with multiple users.

IMPORTANT: As with other mission-critical systems, it is paramount that your OnGuard SA account password be carefully safeguarded and stored in a secure location. In the event that further assistance is needed, contact Lenel Technical Support at (800) 631-6046.

Strong Password Enforcement

OnGuard includes optional strong password enforcement, which checks the user's password against the OnGuard password standards. This functionality is designed to enhance password security. If directory-based or single sign-on (automatic or manual) is used, then the password enforcement used is based within the directory configuration.

Strong password enforcement is enabled/disabled in System Administration or ID CredentialCenter. For more information, refer to the System Administration User Guide (DOC-200) or the ID CredentialCenter User Guide (DOC-300).

When creating a strong password, keep the following standards, requirements, and recommendations in mind.

OnGuard Password Standards

The following standards are in effect when strong password enforcement is enabled in OnGuard:

- Passwords cannot be the same as the username (for example, "SA" and "SA")
- Passwords cannot be Lenel keywords
- Passwords cannot be blank
- OnGuard passwords must be between 1 (weak) and 127 (strong) characters

Password Requirements

Whether or not strong password enforcement is enabled in OnGuard, the following requirements are in effect:

- OnGuard user passwords are not case-sensitive
- Database passwords must conform to the rules of the specific database being used; passwords in SQL Server and Oracle 12c are case-sensitive

Password Recommendations

The following list consists of good practices when creating passwords.

- Always consult with your company's password policies. Depending on password policies, it may be required to create passwords that contain numbers, letters, and symbols.
- Do not reuse passwords; each password should be unique to each service.
- Passwords should not contain the username or parts of the user's full name, such as the first name.
- A strong password should always be greater than eight (8) characters and preferably longer than 12 characters. Consider setting a stricter requirement for administrators or those with privileged roles to be a minimum of 12 characters.
- It is strongly advised to use long passphrases. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against dictionary attacks.

CHAPTER 4

Device Communication Hardening

Overview

This section provides hardening guidelines for communication between OnGuard and the Lenel Access Series controllers and downstream interface modules, including identifying critical information on features, options that should be enabled, and best practices for using the controller.

For a list of hardware devices supported by this hardening guide, refer to Hardware Scope on page 15.

Protection Levels

Depending on the system size and needs, there are different protection levels. Each level assumes the recommendation of the previous level.

Protection Level	Recommendation	Procedures
Basic	Minimum protection. Small businesses or office installations where the operator is also the administrator.	1. **Installation:** Place product on a private network, in a secured enclosure, with updated firmware and normal DIP switch settings. 2. **Embedded Web Server:** Enable HTTPS. 3. **User Accounts:** Remove the default user login and create a unique user account with a strong password. 4. **Equipment Replacement:** Perform the bulk erase procedure on the Intelligent System Controller, and clear the EEPROM on the Interface Modules.

Protection Level	Recommendation	Procedures
Intermediate	Corporations that have a dedicated system administrator.	5. **Embedded Web Server:** Add authorized IP addresses. 6. **Information Services:** Disable discovery and SNMP services. 7. **Encrypted and Authenticated Communication:** Enable AES or TLS encryption.
Enterprise	Large networks with an IT/IS department. Intended for integration into an enterprise network infrastructure.	8. **Information Services:** Enable SNMPv3 (LNL-4420). 9. **Encrypted and Authenticated Communication:** Generate and load customized peer certificates and enable TLS. 10. **Port-Based Network Access Control:** Enable 802.1X.

Installation

The following recommendations for installation of the controller and downstream interface modules include private networks, securing the enclosure, ensuring the latest firmware and normal operation.

Private Network

Do not install any Ethernet products on the public Intranet.

Securing the Enclosure

Install the hardware in a secure enclosure and use a cabinet tamper to generate notifications when the enclosure is opened.

Ensuring the Latest Firmware

Check for the latest firmware. Update all controllers and downstream interface modules to the latest version of firmware to ensure the latest changes and security improvements are installed.

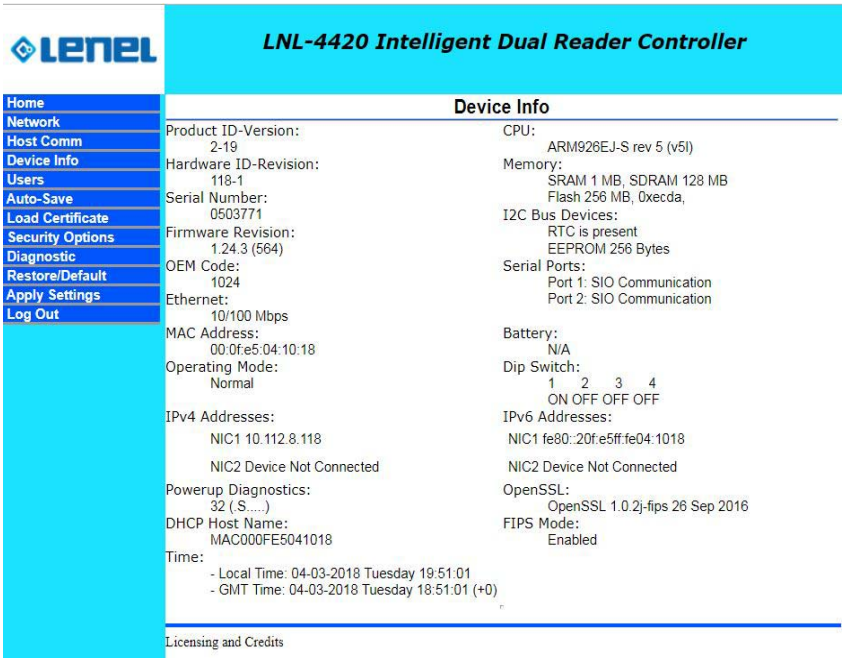
Normal Operation

For normal operation, set all DIP switches to OFF.

Embedded Web Server

To reduce risk, modify the HTTPS, session timer, and authorized IP addresses.

Device Information



HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a protocol for securing communication over a network. HTTPS is a combination of HTTP and TLS/SSL protocols. It is used to provide encrypted communication with the web server. Always enable HTTPS as the default.

To enable HTTPS, set DIP Switch 3 to the OFF position.

Note: The LNL-4420 does not support HTTP. Any HTTP request is redirected to HTTPS.

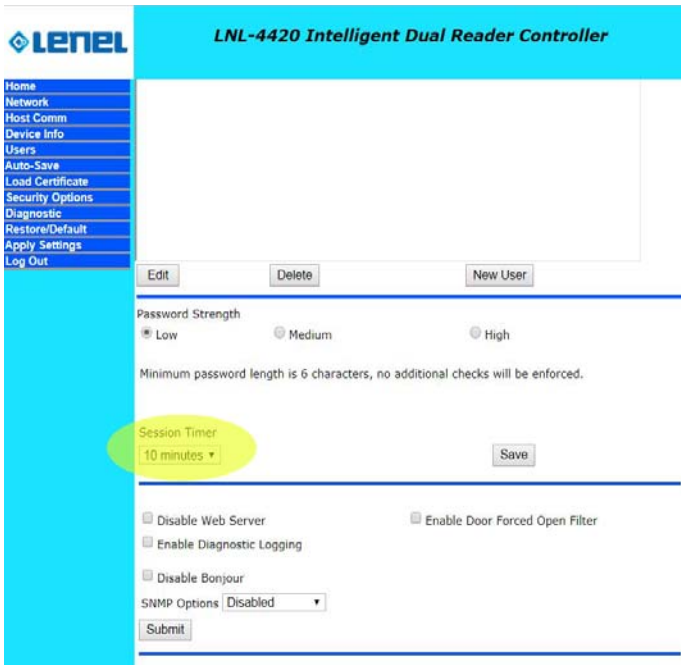
Session Timer

The session timer logs off a user after a certain period of time.

To minimize the risk when an attacker can access active sessions, set the session timer to five (5) minutes. Values from five minutes to 60 minutes in five-minute increments are allowed.

The session timer is available on the Users page of the embedded web server.

Users



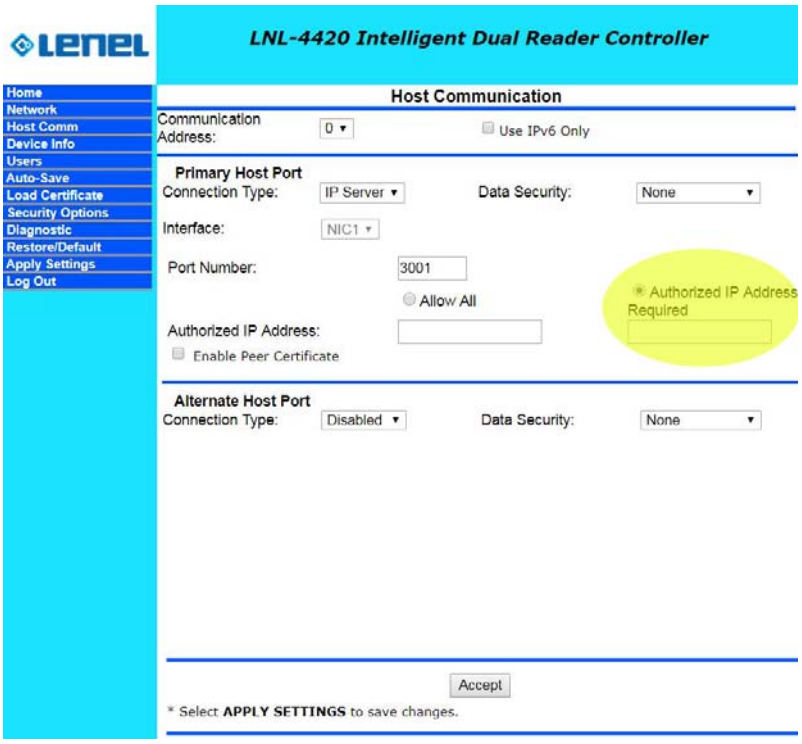
Authorized IP Addresses

Restrict access to the host communication port on the controller.

When there are only one or two IP addresses accessing the host communication port on the controller, you can restrict where this connection originates. This filter applies to the communication port established by OnGuard configured in IP Server (OnGuard-initiated connection) mode. In an IP Client (controller- initiated connection) mode, the authorized IP addresses are programmed into the controller by OnGuard.

From the Host Communication page, select **Authorized IP Address Required** and specify the permitted address or addresses.

Authorized IP Addresses



User Accounts

Modifying user account information is paramount to the security of the controller.

Default User Login

The default user login and password for the controllers is as follows:

- **Username:** admin
- **Password:** password

The default user credentials are the same for all Lenel Access Series controllers. To prevent unauthorized use, disable the default user.

- **For Firmware 1.25.6 or later:** Permanently disable the default user account by clicking the **Disable Default User** check box from the Users page.
- **For Firmware 1.19.4, build 0415 or later:** Temporarily enable the default user account with the following steps (only if the default user was not permanently disabled):
    1) Enable the default user by moving DIP switch 1 from OFF to ON. The user then has five minutes to log into the embedded web server.
    2) A single login within the five minutes, or rebooting the controller disables the ability to use the default login account until another transition of DIP switch 1 is performed.
- **For Firmware before 1.19.4 build 0415:** Ensure DIP switch 1 is OFF and at least one unique user account is created.

Unique User Accounts

Create at least one unique user the first time you log into the embedded web server. This user should use a unique username and password. Each person accessing the embedded web server should have their own unique account for audit purposes.

Password Strengths

User accounts have three levels of password strengths (Low, Medium and High).

Password Level	Criteria
High	• Eight-character minimum • Must not contain the username • Meets all three criteria points (see Password Criteria on page 44)
Medium	• Eight-character minimum • Meets two criteria points (see Password Criteria on page 44)
Low	Six-character minimum

Maximize password security by ensuring the password is a high level strength.

Password Criteria

Passwords must meet three of the four criteria as follows:

- Uppercase alphabet characters (A-Z)
- Lowercase alphabet characters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (!, $, #, or %)

Information Services

Prevent discovery services by implementing the following guidelines.

Disable Discovery

By default, the controllers support device discovery utilizing Zeroconf through services on Windows® and Linux like Apple® Bonjour® and mDNSResponder. Once the controller is installed and configured, it is recommended to turn discovery off. This prevents someone with access to the same network from discovering the controller.

Disable Zeroconf Discovery through the Users page in the embedded web server. For more information, refer to Users on page 42.

Disable SNMP

By default, SNMP is disabled. If SNMP is not used, leave this setting disabled. Disable SNMP through the Users page in the embedded web server. For more information, refer to Users on page 42.

Encrypted and Authenticated Communication

Use the following settings to improve encryption and authentication methods.

Encryption between OnGuard and the Lenel Access Series Controller

The controller supports AES and TLS encryption for communication between OnGuard and the controller. Use one of these methods to encrypt the data being transferred to and from the controller.

TLS is recommended for data security over AES. For more information on TLS, refer to “TLS Configuration” in the Encryption for Controllers User Guide (DOC-1200).

Note: The Encryption for Controllers User Guide is available on the Lenel Web Site: https://partner.lenel.com/downloads/onguard/user-guides. (You will need your Lenel login to gain access to this site.) When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

AES

Enable AES encryption by configuring both the controller and OnGuard. Load the encryption keys on both sides before enabling AES.

TLS

By default, unique certificates are loaded into each controller at production time. Use these certificates to encrypt communication between the controller and OnGuard. Enable TLS encryption through the embedded web server on the controller, or OnGuard, if implemented.

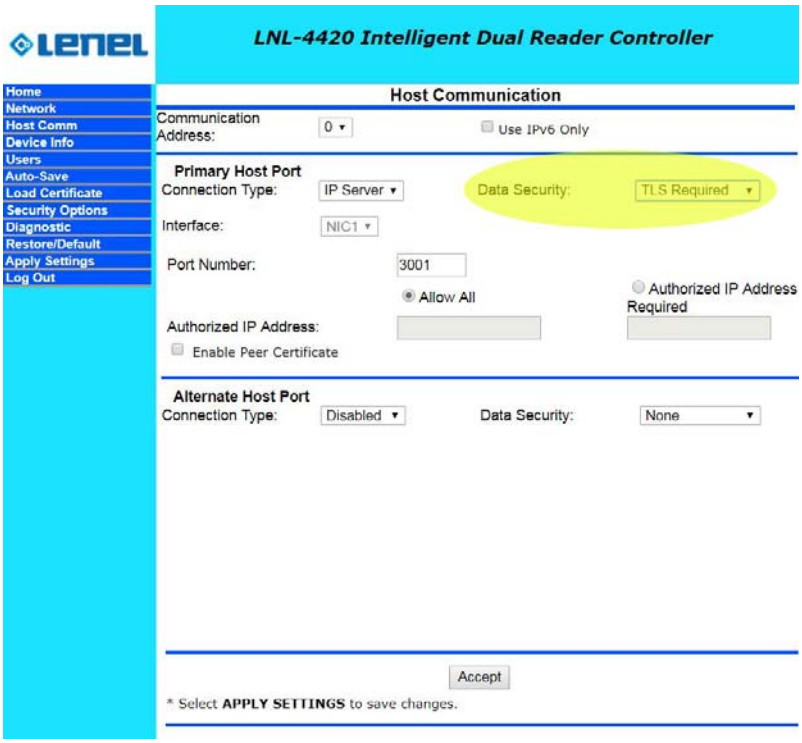
The Data Security menu provides the following options:

- **TLS if Available:** Enable **TLS if Available** locally at the controller without changes in OnGuard and the default will be TLS, if possible.
- **TLS Required:** Enable **TLS Required** indicates only encrypted connections are established and requires TLS configuration in OnGuard. TLS Required is more secure.

Notes: The LNL-2210, LNL-2220, and LNL-3300 only support TLS 1.1.

The LNL-4420 supports TLS 1.2.

Host Authentication



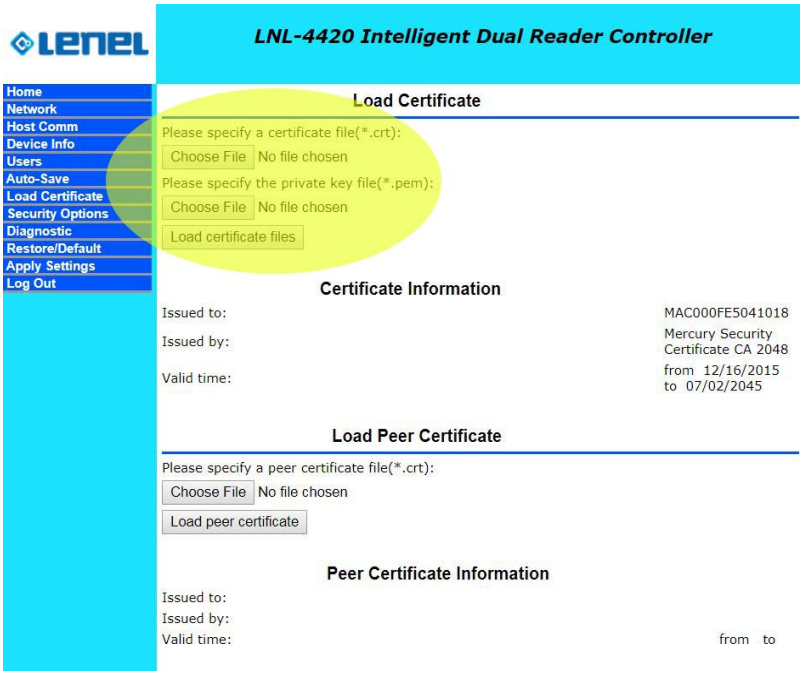
Authentication between the Lenel Access Series Controller and OnGuard

Use certificates to authenticate the validity of the controller and OnGuard. One limitation of factory loaded certificates is they cannot be customized to the location where the controller is deployed. By loading customized peer certificates on the controller and OnGuard, a TLS connection proves the validity of OnGuard and controller.

For more information on installing the TLS certificate on the OnGuard Communication Server and enabling TLS encryption in OnGuard System Administration and the controller, refer to the chapter on TLS Configuration in the Encryption for Controllers User Guide (DOC-1200).

Note: The Encryption for Controllers User Guide is available on the Lenel Web Site: https://partner.lenel.com/downloads/onguard/user-guides. (You will need your Lenel login to gain access to this site.) When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

Load Certificate



- The LNL-4420 supports larger key sizes and higher SHA size.
  - RSA Key Size: 4096-bit maximum (factory default is 2048-bit)
  - SHA Size: sha384 maximum (factory default is sha256)
  - Host and SIO Communication TLS Ciphers: FIPS 140 cipher suite
  - Webpage HTTPS/TLS Ciphers:
    EECDH+AESGCM
    EDH+AESGCM
- LNL-2210, LNL-2220, and LNL-3300 controllers support:
  - RSA Key Size: 1024-bit
  - SHA Size: sha1
  - Host, SIO Communication and Webpage HTTPS/TLS Ciphers:
    TLS_RSA_WITH_AES_256_CBC_SHA
    TLS_RSA_WITH_AES_128_CBC_SHA

Notes: Performance is degraded when values chosen or implemented are below those recommended above.

For more information on certificate verification (both server and controller), refer to the chapter on TLS Configuration in the Encryption for Controllers User Guide (DOC-1200).

Lenel Access Series Controller-to-Downstream Device Communication

Enable encryption between the controller and downstream devices by following the guidance provided below.

Downstream Device	Description
Series 2: LNL-1100, LNL-1200, LNL-1300, LNL-1320	• Only supports AES128 encryption • Must be configured and enabled
Series 3: LNL-1100, LNL-1200, LNL-1300, LNL-1320	• Supports AES128 and AES256 • For LNL-2210, LNL-2220, LNL-3300, and LNL-4420 controllers, AES128 is available and must be configured and enabled
LNL-1300e	Only supports AES128 encryption. Enabled by default.

Downstream encryption allows Series-2 controllers to securely communicate to Series-2 downstream interface modules. All Series-3 modules are automatically encrypted with AES-256.

To properly support downstream encryption, all Series-2 modules must use a version of firmware that is supported by the version of OnGuard that is currently installed.

After enabling encryption, a custom encryption master key can be set and downloaded to the downstream interface modules using OnGuard Alarm Monitoring.

After making any change to encryption, verify in the Alarm Monitoring System Tree that all modules return to the online state.

For more information on enabling the controller for host encryption, refer to the section for the specific controller in ***Access Control > Access Panels Folder*** in the System Administration User Guide (DOC-200).

Reader Communication

Use OSDP secure channel (V2) for reader communications. This bi-directional protocol is secured using symmetric keys shared between the reader and controller, and is a more secure communication method.

For more information on enabling secure channel communication, refer to ***Access Control > Readers and Doors Folder > General Form*** in the System Administration User Guide (DOC-200).

Note: OSDP secure channel encryption is not available on the LNL-1100, LNL-1200, LNL-1300, and LNL-1320 downstream interface modules.

Port-Based Network Access Control

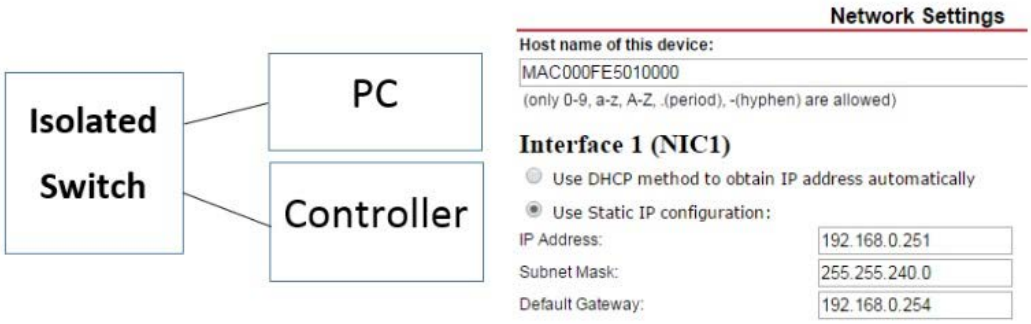
802.1x Authentication

Note: This feature is only supported on the LNL-4420 (Firmware 1.24.1).

As an added layer of local area network security, add 802.1x authentication to prevent unwanted access to a given network. A supplicant, or device intending to connect to the network, must first

agree on a type of Extensible Authentication Protocol (EAP) with the authentication server that is linked to the desired network. The supplicant is required to pass a series of challenges passed from the middle-man authenticator in order to communicate with the network connected to the authentication server. EAP's can range from something as simple as a combination of username/password, to requiring a certificate over Transport Layer Security (TLS), and requiring both certificate over TLS and the username/password. By doing so, the authentication server can prevent access to any supplicant who does not properly authenticate.

To activate, install the controller on an isolated network (or direct connect to host), configure with a static IP and connect through the embedded web server.



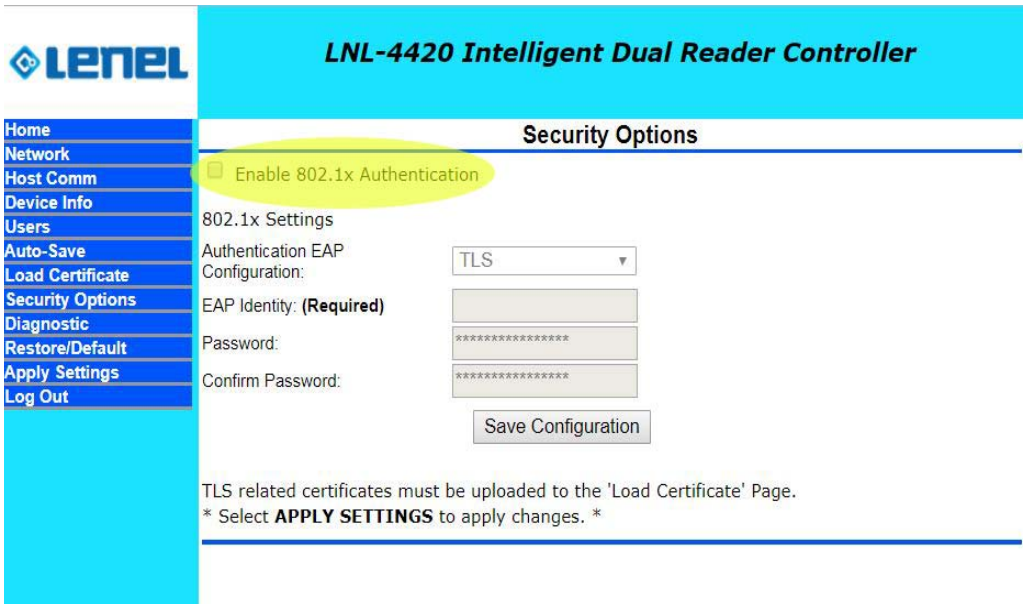
If you are using TLS, ensure that the certificates for the controller are signed by the same root certificate used by the authentication server. For more information on loading certificates, refer to Security Options on page 50.

When the controller is able to communicate using a web browser:

1. Select **Security Options**.
2. Check **Enable 802.1x Authentication**.
3. Enter the EAP login and password (based on the authentication server configuration).
4. Restart the controller.
5. Connect to the desired network.

   The controller is now authenticated using 802.1x.

Security Options



Equipment Replacement

When replacing a board, clear data if the hardware is capable.

Lenel Access Series Controllers

To sanitize the controller, use the following steps to perform the bulk erase procedure.

Bulk Erase Procedure

IMPORTANT: Do not remove power during Steps 1-4.

1. Set S1 DIP switches:
   - Switches 1 and 2: ON
   - Switches 3 and 4: OFF
2. Apply power to the controller.
3. Watch for LEDs 1 and 2, and 3 and 4, to alternately flash at a 0.5 second rate.

   If these switches are not changed, the controller powers up using the OEM default communication parameters.
4. Within 10 seconds of powering up, change Switches 1 or 2 to OFF.

   LED 2 flashes, indicating that the configuration memory is being erased.

   Full memory erase takes up to 60 seconds.

   When complete, LEDs 1 and 4 flash for eight seconds.

   The controller reboots eight seconds after LEDs 1 and 4 stop flashing (LEDs are off during this time).

Interface Modules

On the interface module, clear the EEPROM.

Clearing the EEPROM Procedure

Note: This procedure does not work with the LNL-1300e.

Perform the following steps to clear the configuration stored in EEPROM.

1. Set all DIP switches to OFF on the interface module.
2. Cycle power.
3. Within three seconds of applying power, set DIP switch 8 to the ON position.
4. After the interface module completes its power-up sequence, set the DIP switches to the correct state.

Network Ports

The default port for the Mercury Host Protocol (MSP2) is 3001. To help maintain a secure state for the OnGuard environment, this port should be changed.

For more information on changing the host port, refer to the section for the specific controller in ***Access Control > Access Panels Folder > Primary Connection Sub-tab*** and ***Secondary Connection Sub-tab*** in the System Administration User Guide (DOC-200).

Ports used by the LNL-2210, LNL-2220, and LNL-3300

Port	Port Type	Usage	Disable
67	UDP	DHCPS	No
68	UDP	DHCPC	No
80	TCP	HTTP	Yes: Use Disable Web Server from the Users web configuration page.
161	UDP	SNMP	Yes: Use Disable SNMP Server from the Users web configuration page.
443	TCP	HTTPS	Yes: Use Disable Web Server from the Users web configuration page.
3001	TCP	Mercury Host Protocol (MSP2)	Yes: Set the Connection Type from the Host Comm page to an option other than IP.
4001	TCP	PSIA	
5353	UDP	Zeroconf (Discovery)	Yes: Use Disable Bonjour option from the Users web configuration page.

Note: Configure the Mercury Host Protocol (MSP2) to use a different port. The default port is 3001.

Ports used by the LNL-4420

Port	Port Type	Usage	Disable
67	UDP	DHCPS	No
68	UDP	DHCPC	No
80	TCP	HTTP	Yes: Use Disable Web Server from the Users web configuration page.
161	UDP	SNMP	Yes: Use Disable SNMP Server from the Users web configuration page.
443	TCP	HTTPS	Yes: Use Disable Web Server from the Users web configuration page.
3001	TCP	Mercury Host Protocol (MSP2)	Yes: Set the Connection Type from the Host Comm page to an option other than IP.
4001	TCP	PSIA	
5353	UDP	Zeroconf (Discovery)	Yes: Use Disable Bonjour option from the Users web configuration page.
47808	TCP	BACnet™	Yes: BACnet is disabled by default.
47307	UDP	OTIS®	Yes: Not required for OTIS integration in OnGuard.
48307	UDP	OTIS	Yes: Not required for OTIS integration in OnGuard.
45303	UDP	OTIS	Yes: Not required for OTIS integration in OnGuard.
46303	UDP	OTIS	Yes: Not required for OTIS integration in OnGuard.
46308	UDP	OTIS	Yes: Not required for OTIS integration in OnGuard.
45308	UDP	OTIS	Yes: Not required for OTIS integration in OnGuard.
10200	TCP	pivCLASS® Embedded	Yes: Configure through the pivCLASS embedded web configuration page.

Note: OnGuard OTIS integration does not require the use of Ports 47307 - 45308 at this time.

Ports used by the LNL-1300e

Port	Port Type	Usage	Disable
3001	TCP	Mercury SIO Communication Protocol (MSP1)	No

CHAPTER 5

OnGuard Client Hardening

Overview

This section provides hardening guidelines applicable to browser-based applications.

HTTP Response Headers

HTTP caching allows a web browser to store local copies of web resources for faster retrieval the next time the resource is required. Client side caching occurs when these web resources are stored in a folder on the local computer system as determined by the browser. An attacker who gains access to the system may be able to read sensitive information, such as passwords, and potentially impersonate a user for malicious activities.

To harden websites and browser-based applications against malicious activity, client side caching should be disabled, and a combination of the following headers should be used:

- **x-frame-options:** This header helps protect visitors to a website against clickjacking attacks by not allowing the rendering of a page in a frame. The recommended configuration is to set this header to `sameorigin`, which directs the page to be loaded in a frame on the same origin as the page itself.
- **x-xss-protection:** This header is designed to enable the cross-site scripting (XSS) filter built into modern web browsers. This is usually enabled by default, but using it will enforce it. It is supported by Microsoft® Internet Explorer®8+, Google Chrome™, and Apple Safari®. The recommended configuration is to set this header to `1; mode=block`, which will enable the XSS protection and instruct the browser to block the response in the event that a malicious script has been inserted from user input.
- **x-content-type-options:** This response header is a marker used by the server to indicate that MIME (Multipurpose Internet Mail Extensions) types advertised in the `content-type` headers should not be changed or followed. This header was introduced by Microsoft in Internet Explorer 8 to allow webmasters to block content sniffing from occurring. The recommended configuration is to set this header to `nosniff`.

- **cache-control:** This header controls who caches the response, under what conditions, and for how long. The recommended configuration is to set this header to `no-store`, which disallows browsers and all intermediate caches from storing any versions of returned responses.
- **pragma:** This HTTP/1.0 general header is an implementation-specific header that may have various effects along with the request-response chain. It is used for backward compatibility with HTTP/1.0 caches where the `cache-control` HTTP/1.1 header is not yet present. The recommended configuration is to set this header to `no-cache`.

The OnGuard web applications are installed on the client side. Modifications made to the configuration (**.conf**) files for the web applications can reduce the chance an attacker compromises the OnGuard system by gaining access via cached information on the client side. Use the steps below to modify the **.conf** files for the following web applications:

- Lenel Console
- OnGuard Access Manager
- OnGuard Cardholder Self Service
- OnGuard Credentials
- OnGuard Monitor

1. On the system where OnGuard is installed, go to ***C:\ProgramData\Lnl\nginx\conf\modules***.
2. Locate the following **.conf** files and open in a text editor:
   - **AccessManager.conf** (OnGuard Access Manager)
   - **cardholder_self_service.conf** (OnGuard Cardholder Self Service)
   - **credentials.conf** (OnGuard Credentials)
   - **monitor.conf** (OnGuard Monitor)
   - **console.conf** (Lenel Console)
3. In each **.conf** file, add the HTTP headers (bold) at each `location` directive as shown in the following examples:

   AccessManager.conf (OnGuard Access Manager):

```
#Access Manager
location /accessmanager {
   add_header X-Frame-Options sameorigin;
   add_header X-XSS-Protection "1; mode=block";
   add_header X-Content-Type-Options nosniff;
   add_header Cache-Control no-store;
   add_header Pragma no-cache;
   alias  "C:/Program Files (x86)/OnGuard/AccessManager/";
   index  index.html index.htm;
}
```

   cardholder_self_service.conf (OnGuard Cardholder Self Service):

```
#CSS API
location /api {
    proxy_set_header Host $host;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
```

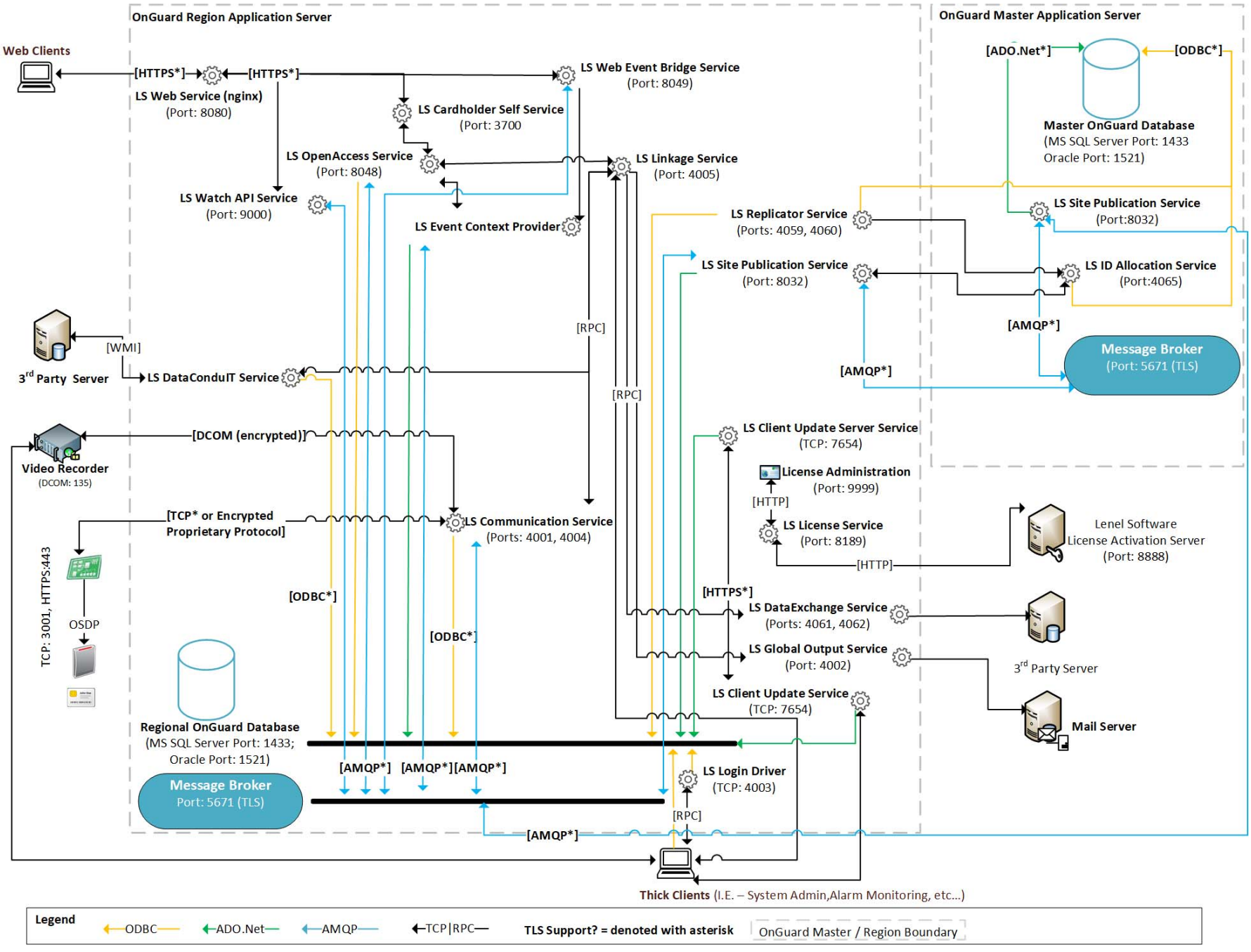
```
        proxy_pass http://localhost:3700;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
    }
    #Cardholder Self-Service
    location /css {
       add_header X-Frame-Options sameorigin;
       add_header X-XSS-Protection "1; mode=block";
       add_header X-Content-Type-Options nosniff;
       add_header Cache-Control no-store;
       add_header Pragma no-cache;
       alias  "C:/Program Files (x86)/OnGuard/CSS/frontend/bin/";
       index  index.html index.htm;
    }
    #CSS Admin App
    location /cssadminapp {
       add_header X-Frame-Options sameorigin;
       add_header X-XSS-Protection "1; mode=block";
       add_header X-Content-Type-Options nosniff;
       add_header Cache-Control no-store;
       add_header Pragma no-cache;
       alias  "C:/Program Files (x86)/OnGuard/CSS/CSSAdminApp/";
       index  index.html index.htm;
    }
```

4. Save the changes made to the first .**conf** file you edit and close the file.
5. Repeat these steps for the remaining **.conf** files.

APPENDIX A

System Diagram

The following system diagram depicts the installation of OnGuard in a hardened environment. For additional, optional, port configurations, refer to Ports and Endpoints on page 59.


OnGuard Region Application Server
OnGuard Master Application Server
Web Clients
[HTTPS*]
[HTTPS*]
LS Web Service (nginx)
(Port: 8080)
LS Web Event Bridge Service
(Port: 8049)
LS Cardholder Self Service
(Port: 3700
LS OpenAccess Service
(Port: 8048)
LS Linkage Service
(Port: 4005)
LS Watch API Service
(Port: 9000)
LS Event Context Provider
[ADO.Net*]
[ODBC*]
Master OnGuard Database
(MS SQL Server Port: 1433
Oracle Port: 1521)
LS Site Publication Service
(Port:8032)
LS Replicator Service
(Ports: 4059, 4060)
LS Site Publication Service
(Port: 8032)
LS ID Allocation Service
(Port:4065)
[AMQP*]
Message Broker
(Port: 5671 (TLS)
[RPC]
[WMI]
3rd Party Server
LS DataConduIT Service
[AMQP*]
[RPC]
[DCOM (encrypted)]
Video Recorder
(DCOM: 135)
LS Client Update Server Service
(TCP: 7654)
License Administration
(Port: 9999)
[HTTP]
LS License Service
(Port: 8189)
[HTTP]
Lenel Software
License Activation Server
(Port: 8888)
[TCP* or Encrypted
Proprietary Protocol]
LS Communication Service
(Ports: 4001, 4004)
TCP: 3001, HTTPS:443
OSDP
[ODBC*]
[ODBC*]
[HTTPS*]
LS DataExchange Service
(Ports: 4061, 4062)
LS Global Output Service
(Port: 4002)
3rd Party Server
LS Client Update Service
(TCP: 7654)
Regional OnGuard Database
(MS SQL Server Port: 1433;
Oracle Port: 1521)
Mail Server
[AMQP*]
[AMQP*][AMQP*]
LS Login Driver
(TCP: 4003)
Message Broker
Port: 5671 (TLS)
[RPC]
[AMQP*]
Thick Clients (I.E. – System Admin,Alarm Monitoring, etc...)
Legend
ODBC
ADO.Net
AMQP
TCP|RPC
TLS Support? = denoted with asterisk
OnGuard Master / Region Boundary

APPENDIX B

Ports and Endpoints

When adapting OnGuard permissions to corporate policies regarding the segregation or limitation of privileges on servers and associated user accounts, refer to this section to understand the process that manages server sockets and their associated operating system privileges.

Ports Used by OnGuard

Port	Protocol	Encrypted	Function	From (client)	To (server)	OnGuard Version	Port Change
80	SSL/HTTP	No	IIS Web Server	Web	IIS	≥ 5.12	See IIS configuration
135	DCOM	Yes	DCOM DCE endpoint resolution	Everywhere	OG, LNVR	All	No
161	UDP SNMP	No	SNMPv1 Messaging	DCM	Everywhere		See Windows SNMP configuration
162	UDP SNMP	No	SNMPv1 Traps	Everywhere	CS		See Windows SNMP configuration
443	SSL/HTTP	TLS	IIS Web Server	Web	IIS	≥ 5.12	See IIS configuration
1433	MS-SQL-S	Optional	SQL Server	Everywhere	DB	All	See SQL Server configuration
1434	UDP SSRP	No	SQL Server Browser Service	Everywhere	DB	All	
1521	Oracle	Optional	Oracle Database	Everywhere	DB	All	See Oracle configuration
3001	Mercury	TLS 1.1, 1.2	Mercury Controllers	CS	MC	≥ 5.0	See System Administration
3700			OnGuard Cardholder Self Service	NX	CSS		
4001	MSRPC		Communication Server RPC	AAM, AM, CDS, DC, DE, LS, RS	CS	All	ACS.INI [Service] DriverRpcPort
4002			Global Output Server RPC	LS	GOS	≥ 5.0	ACS.INI [Service] GosRpcPort
4003	MSRPC		Login Driver RPC	Everywhere	LD	≥ 5.0	ACS.INI [Service] LoginRpcPort

Port	Protocol	Encrypted	Function	From (client)	To (server)	OnGuard Version	Port Change
4004			Communication Server Events	AM, LS	CS	All	ACS.INI [Service] DriverSocketPort
4005	MSRPC		Linkage Server RPC	SA	CS	All	ACS.INI [Service] DriverSocketPort
4006			Video Server RPC	LS, SA	ARC	All	ACS.INI [Service] DriverSocketPort
4009-4057			Alarm Monitoring RPC	CS	AM	≥ 5.9	ACS.INI [Service] AcsmntrRpcMinPort, AcsmntrRpcMaxPort
4059			Replicator Data	RA, RS	RS	≥ 5.9	ACS.INI [Service] ReplicatorSocketPort
4060			Replicator RPC	RA, RS	RS	≥ 5.9	ACS.INI [Service] ReplicatorRpcPort
4061			Lenel® DataExchange Data	LS	DE	≥ 5.9	ACS.INI [Service] DESocketPort
4062			Lenel DataExchange RPC	LS	DE	≥ 5.9	ACS.INI [Service] DERpcPort
4065			Replicator	RA, RE	IA	≥ 6.3	No
4070			HID Edge Devices	CS	HE	≥ 6.1	ACS.INI [HID VertX] ListeningPort
5671	AMQP	TLS 1.1, 1.2	LS Message Broker (QPID)	Everywhere	MB	≥ 7.0	Security Utility
5672	AMQP	None	LS Message Broker (QPID)	Everywhere	MB	≥ 7.0	Security Utility
7007-7008			SkyPoint® Base Server	CS	SKY	≥ 7.0	No

Port	Protocol	Encrypted	Function	From (client)	To (server)	OnGuard Version	Port Change
7654			LS Client Update Server	CU	CU	≥ 7.0	System Administration
8032			Site Publication Server	SP	SP	≥ 7.0	Security Utility
8048	SSL/HTTP	TLS	OpenAccess REST Proxy	RP	NX	≥ 7.1	No
8049			LS Web Event Bridge	WB	Everywhere	≥ 7.2	No
8080	SSL/HTTP	TLS 1.1, 1.2	OpenAccess NGINX	Everywhere	NX	≥ 7.1	Security Utility
8080	SSL/HTTP	TLS 1.1, 1.2	NGINX: NetDVMS	ND	OS	≥ 7.1	Security Utility
8189			License Sever	Everywhere	LIC	≥ 5.7	Configuration Editor + LicenseServerConfig\Server.properties
8888			FLEXnet Licensing®	FN	Customer	≥ 6.1	No
9000			WATCH API Service	NX	WA		
9111	MS-NRTP	None	Application Server	Web	AS	≥ 5.12	No
9999			License Administration	Web	LIC	≥ 5.7	Configuration Editor + LicenseServerConfig\Server.properties
10001			Galaxy® Ethernet Module	CS	GP	≥ 5.11	No
45303	UDP/OTIS		Elevator Terminal Online Status	CS	OE	≥ 5.12	ACS.INI [Otis] SSOnlineStatusPort

Port	Protocol	Encrypted	Function	From (client)	To (server)	OnGuard Version	Port Change
45307	UDP/OTIS		Elevator Dispatching Heartbeat	OE	CS	≥ 5.12	ACS.INI [Otis] SSHeartbeatPort
46308	UDP/OTIS		Elevator Terminal Command	CS	OE	≥ 5.12	ACS.INI [Otis] SSDECCommandPort

Endpoints in OnGuard

Abbreviation	Description	Service Name	Service Principle	Process File Name
AAM	Area Access Manager			
AM	Alarm Monitoring			
ARC	Archive Server			
AS	Application Server	LS Application Service	,\<user>	Lnl.OG.ApplicationServer.Service.exe
CDS	Config Download Service	Ls Config Download Service	Local System	LnlConfigDownloadService.exe
CS	Communication Server	LS Communication Server	Local System	Lnlcomsrvr.exe
CSS	Cardholder Self Service			
CU	Client Update Service	LS Client Update Server	,\<user>	Lnl.OG.AutoUpgrade.Server.ServiceHost.exe
DB	Database Server			
DC	Lenel® DataConduIT	LS DataConduIT Service	Local System	WMIService.exe

Abbreviation	Description	Service Name	Service Principle	Process File Name
DCM	Lenel DataConduIT Message Queue	LS DataConduIT Message Queue Server	Local System	DataConduITQueueServer.exe
DD	Device Discovery	LS Device Discovery Service	Local System	Lnl.Discovery.DeviceDiscoveryService.exe
DE	DataExchange	LS DataExchange Server	Local System	DataExchangeService.exe
EC	Event Context Provider	LS Event Context Provider	Local System	Lnl.OG.EventContextProvider.exe
FN	FLEXnet Public License Site			
GOS	Global Output Server	LS Global Output Server	Local System	GOSServer.exe
GP	Galaxy Panels			
HE	HID Edge Devices			
IA	ID Allocation Service	LS ID Allocation	Local System	IDAllocationServiceu.exe
IIS	IIS Web Server			
LD	Login Driver	LS Login Driver	Local System	logindrvr.exe
LIC	License Server	LS License Server	Local System	LicenseServer.exe
LS	Linkage Server	LS Linkage Server	Local System	LSLServer.exe
MB	Message Broker	LS Message Broker	Local System	qpidd.exe
MC	Mercury Controllers			
ND	NetDVMS			
NX	NGINX Web Server	LS Web Service	Local System	NginxService.exe (wrapper)
OC	OnGuard Client			

Abbreviation	Description	Service Name	Service Principle	Process File Name
OE	OTIS Elevator Dispatching System			
OS	OnGuard Server			
RA	Replication Administration			
RP	OpenAccess REST Proxy	LS OpenAccess	Local System	Lnl.OG.LsOpenAccess.exe
RS	LS Replicator Service	LS Replicator	Local System	Replicator.exe
SA	System Administration			
SKY	SkyPoint Base Server			
SP	Site Publication Server	LS Site Publication Server	,\<user>	Lnl.OG.Replicator.Service.exe
WA	WATCH API Service			
WB	Web Event Bridge Service	LS Web Event Bridge	Local System	Lnl.OG.WebEventBridgeService.exe
Web	Web Browser			

APPENDIX C

Scope of OnGuard Features for a Highly Secured Environment

This section lists the features that are not included in this document for the hardening of an OnGuard system in a highly secured environment. If your installation requires these additional features, refer to the appropriate installation documentation for assistance.

OnGuard features not included for hardening in a highly secure environment

Feature	Description
Area Access Manager (Browser-based Client)	Area Access Manager has a lite client application that can run from an Internet browser on any computer with or without OnGuard installed.
VideoViewer (Browser-based Client)	VideoViewer has a lite client application that can run from an Internet browser on any computer with or without OnGuard installed. The primary purpose of the VideoViewer browser-based client is live and recorded video monitoring.
Visitor Management Administration	Visitor Management Administration is a browser-based application used to configure settings such as sign-in locations and devices for other browser-based applications such as Visitor Management Front Desk, Visitor Management Host, and Visitor Self Service. This application allows users to log into the visitor management system from any computer using the Internet Explorer browser.
Visitor Management Front Desk	Visitor Management Front Desk is a browser-based application used by front desk attendants to search for visitors, sign visitors in or out, capture information, determine status, and have email notifications sent to the hosts and visitors. Front desk attendants can also view upcoming visits. This application allows users to log into the visitor management system from any computer using the Internet Explorer browser.
Visitor Management Front Host	Visitor Management Host is a browser-based application that allows the hosting party to schedule a visit and add visitors. This application allows users to log into the visitor management system from any computer using the Internet Explorer browser.
LS Application Service	Required to support legacy IIS web-based applications.

Index

U

V

UTC Fire & Security Americas Corporation, Inc.
1212 Pittsford-Victor Road
Pittsford, New York 14534 USA
Tel 866.788.5095 Fax 585.248.9185
www.lenel.com
docfeedback@lenel.com