



## OnGuard 8.0 Hardening Guide



**© 2021 Carrier. All Rights Reserved. All trademarks are the property of their respective owners. LenelS2 is a part of Carrier.**

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the prior express written permission of Carrier Fire & Security Americas Corporation, which such permission may have been granted in a separate agreement (i.e., end user license agreement or software license agreement for the particular application).

Non-English versions of LenelS2 documents are offered as a service to our global audiences. We have attempted to provide an accurate translation of the text, but the official text is the English text, and any differences in the translation are not binding and have no legal effect.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that agreement.

SAP® Crystal Reports® is the registered trademark of SAP SE or its affiliates in Germany and in several other countries.

Integral and FlashPoint are trademarks of Integral Technologies, Inc.

Portions of this product were created using LEADTOOLS ©1991-2011, LEAD Technologies, Inc. ALL RIGHTS RESERVED.

Active Directory, Microsoft, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NEC, ExpressCluster and ExpressCluster X are registered trademarks or trademarks of NEC Corporation in the United States and other countries.

Oracle is a registered trademark of Oracle International Corporation.

Amazon Web Services and the "Powered by AWS" logo are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

Other product names mentioned may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

### **Product Disclaimers and Warnings**

THESE PRODUCTS ARE INTENDED FOR SALE TO, AND INSTALLATION BY, AN EXPERIENCED SECURITY PROFESSIONAL. LENELS2 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.

LENELS2 DOES NOT REPRESENT THAT SOFTWARE, HARDWARE OR RELATED SERVICES MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED. LENELS2 DOES NOT WARRANT THAT SOFTWARE, HARDWARE OR RELATED SERVICES WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS AND DOES NOT WARRANT ANY SOFTWARE, HARDWARE OR RELATED SERVICES AGAINST HARMFUL ELECTROMAGNETIC INTERFERENCE INDUCTION OR RADIATION (EMI, RFI, ETC.) EMITTED FROM EXTERNAL SOURCES. THE ABILITY OF SOFTWARE, HARDWARE AND RELATED SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH LENELS2 HAS NO CONTROL INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND RELATED OPERATING SYSTEM COMPATABILITY; OR PROPER INSTALLATION, CONFIGURATION AND MAINTENANCE OF AUTHORIZED HARDWARE AND OTHER SOFTWARE.

LENELS2 MAY MAKE CERTAIN BIOMETRIC CAPABILITIES (E.G., FINGERPRINT, VOICE PRINT, FACIAL RECOGNITION, ETC.), DATA RECORDING CAPABILITIES (E.G., VOICE RECORDING), AND/OR DATA/INFORMATION RECOGNITION AND TRANSLATION CAPABILITIES AVAILABLE IN PRODUCTS LENELS2 MANUFACTURES AND/OR RESELLS. LENELS2 DOES NOT CONTROL THE CONDITIONS AND METHODS OF USE OF PRODUCTS IT MANUFACTURES AND/OR RESELLS. THE END-USER AND/OR INSTALLER AND/OR RESELLER/DISTRIBUTOR ACT AS CONTROLLER OF THE DATA RESULTING FROM USE OF THESE PRODUCTS, INCLUDING ANY RESULTING PERSONALLY IDENTIFIABLE INFORMATION OR PRIVATE DATA, AND ARE SOLELY RESPONSIBLE TO ENSURE THAT ANY PARTICULAR INSTALLATION AND USE OF PRODUCTS COMPLY WITH ALL APPLICABLE PRIVACY AND OTHER

LAWS, INCLUDING ANY REQUIREMENT TO OBTAIN CONSENT. THE CAPABILITY OR USE OF ANY PRODUCTS MANUFACTURED OR SOLD BY LENEL S2 TO RECORD CONSENT SHALL NOT BE SUBSTITUTED FOR THE CONTROLLER'S OBLIGATION TO INDEPENDENTLY DETERMINE WHETHER CONSENT IS REQUIRED, NOR SHALL SUCH CAPABILITY OR USE SHIFT ANY OBLIGATION TO OBTAIN ANY REQUIRED CONSENT TO LENEL S2.

For more information on warranty disclaimers and product safety information, please check <https://firesecurityproducts.com/en/policy/product-warning> or scan the following code:



# Table of Contents

Chapter 1 : 8.0_Hardening Guide Introduction .....	10
Scope of this Guide .....	10
Chapter 1: Introduction .....	10
Chapter 2: Hardening Fundamentals.....	10
Chapter 3: OnGuard Application Server Hardening .....	10
Chapter 4: Device Communication Hardening.....	10
Chapter 5: OnGuard Client Hardening .....	10
Appendices .....	10
System Diagrams .....	10
Ports and Endpoints .....	11
Scope of OnGuard Features in a Highly Secured Environment .....	11
8.0_Acronyms Used in this Guide.....	11
A .....	11
C .....	11
D .....	11
E .....	11
F.....	11
H.....	12
I .....	12
L.....	12
M.....	12
N.....	12
O.....	12
P.....	12
Q.....	12
R.....	12
S .....	13
T .....	13
V .....	13
X .....	13

8.0_Hardening Overview .....	13
8.0_Prerequisite Skills .....	14
8.0_Recommended Industry Tools .....	14
8.0_Steps to Hardening Your OnGuard System.....	15
8.0_Secure by Default .....	15
8.0_Industry Accepted Guidelines.....	16
8.0_Architectural Assumptions of Scope .....	16
8.0_Hardware Scope.....	17
8.0_Software Scope .....	17
8.0_OnGuard Thick Client Applications .....	17
8.0_OnGuard Thin Client Applications.....	18
8.0_OnGuard Servers and Services .....	18
8.0_Deployment of OnGuard in a Highly Secure Environment .....	19
<b>Chapter 2 : 8.0_Hardening Fundamentals.....</b>	<b>20</b>
8.0_Protocols .....	20
8.0_Hardening TLS Against Man-in-the-Middle (MITM) Attacks .....	20
8.0_TLS .....	20
8.0_TLS and Cipher Configuration for RabbitMQ .....	20
8.0_Digital Certificates.....	21
8.0_Peer Certificates .....	21
OnGuard Message Broker and Client Applications .....	22
Requirements for Peer Certificate Verification.....	22
Video Peer Certificates.....	24
Prevent Automatic Redirects.....	24
8.0_Service Accounts .....	25
8.0_OnGuard Services.....	25
8.0_Registry Keys for OnGuard Services .....	26
8.0_Resources for OnGuard Services .....	29
8.0_HTTP Endpoints for OnGuard Services .....	30
8.0_OnGuard WATCH Services .....	31
8.0_RabbitMQ Service Account .....	32
8.0_OnGuard Policies.....	33

8.0_Unnecessary Services and Files.....	33
8.0_Microsoft Customer Experience Improvement Program (CEIP) .....	34
8.0_Printer Security .....	34
Hardening best practices for networked printers .....	34
8.0_Client-side Protections .....	35
<b>Chapter 3 : 8.0_OnGuard Application Server Hardening .....</b>	<b>38</b>
8.0_Isolating the OnGuard Resources within a VLAN .....	38
8.0_Hardening the Databases .....	38
8.0_Encrypting the Database .....	38
8.0_Enabling TLS/SSL Encryption for an Instance of SQL Server .....	39
8.0_SQL Server Database Roles.....	39
8.0_LenelS2 Installation Packages.....	40
8.0_OnGuard Servers, Services, and Utilities .....	45
8.0_License Server .....	45
8.0_NGINX Web Service.....	46
8.0_Login Driver .....	47
8.0_OnGuard Security Utility.....	47
8.0_OnGuard Applications.....	48
8.0_OpenAccess Session Management.....	48
8.0_Accounts and Passwords .....	49
8.0_Default Accounts and Passwords.....	49
8.0_OnGuard "SA" (System Administrator) Account .....	50
Key Points for System Administrator Password Change .....	50
8.0_OnGuard "SA" Delegate User.....	50
8.0_OnGuard Passwords .....	51
8.0_Password Best Practices.....	51
8.0_Password Settings in OnGuard.....	51
8.0_Logon Authorization Warning .....	52
8.0_RabbitMQ Management Plugin .....	52
<b>Chapter 4 : 8.0_Device Communication Hardening .....</b>	<b>53</b>
8.0_Protection Levels .....	53

8.0_Device Installation .....	54
8.0_Embedded Web Server .....	54
HTTPS .....	55
Session Timer .....	55
Authorized IP Addresses .....	56
8.0_User Accounts.....	57
Default User Login.....	57
Unique User Accounts.....	58
Password Strengths .....	58
Password Criteria .....	58
8.0_Information Services.....	58
Disable Discovery .....	59
Disable SNMP .....	59
8.0_Encrypted and Authenticated Communication .....	59
8.0_Encryption between OnGuard and the LenelS2 X-Series and Access Series Controllers .....	59
8.0_AES Encryption.....	59
8.0_TLS Encryption .....	59
8.0_Authentication between the LenelS2 X-Series and Access Series Controllers and OnGuard .....	60
8.0_LenelS2 X-Series and Access Series Controller-to-Downstream Device Communication .....	62
8.0_Reader Communication.....	62
8.0_Data at Rest Encryption .....	63
8.0_Protection Against Replay Attacks on IP Networks.....	63
8.0_Host/Controller Communication .....	63
8.0_Controller/IP-Based Downstream Module Communication.....	64
8.0_Port-Based Network Access Control .....	64
802.1x Authentication .....	64
8.0_Equipment Replacement.....	65
8.0_LenelS2 X-Series and Access Series Intelligent System Controllers .....	65
8.0_Bulk Erase Procedure.....	65
8.0_Interface Modules .....	66
8.0_Clearing the EEPROM .....	66
8.0_LNL-1324e Bulk Erase .....	66

8.0_Network Ports .....	66
8.0_Ports Used by the LNL-2210, LNL-2220, and LNL-3300 .....	67
8.0_Ports Used by the LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 .....	67
8.0_Ports Used by the LNL-1300e.....	68
8.0_Ports Used by the LNL-1324e.....	68
8.0_OSDP Readers.....	69
8.0_Prerequisites .....	69
8.0_OSDP Secure Channel Communication .....	70
8.0_Enable OSDP Secure Channel Mode in OnGuard .....	70
8.0_Configure Readers for OSDP Secure Channel Mode.....	70
8.0_Configure OnGuard for OSDP Secure Channel Support.....	70
8.0_Set Reader Configuration to Support OSDP Biometrics .....	70
8.0_Initiate Secure Connection with the Connected Reader.....	71
<b>Chapter 5 : 8.0_OnGuard Client Hardening .....</b>	<b>73</b>
8.0_HTTP Response Headers.....	73
8.0_Removing a Wildcard Directive from the Content-Security-Policy Header .....	74
8.0_Required Services for OnGuard Thin Client (Browser-based) Applications.....	74
<b>Chapter 6 : 8.0_Appendices .....</b>	<b>76</b>
8.0_Protocol Hardening Guide .....	76
Overview .....	76
A Primer on Cipher Suites .....	76
Why Not Just Say TLS 1.x ? .....	77
Policies for 2020 .....	77
TLS 1.3 Strong Ciphers.....	77
TLS 1.2 Strong Ciphers.....	77
LenelS2 X-Series and Access Series Controllers .....	79
8.0_System Diagrams .....	79
8.0_OnGuard System Diagram .....	80
8.0_OnGuard WATCH System Diagram .....	81
8.0_Ports and Endpoints .....	81
8.0_Ports Used by OnGuard .....	82
8.0_Endpoints in OnGuard .....	87



8.0_Scope of OnGuard Features for a Highly Secured Environment.....	89
---	----

# Chapter 1 : 8.0\_Hardening Guide 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.

### Chapter 5: OnGuard Client Hardening

This section provides hardening guidelines applicable to specific clients, including removing services, closing ports, and reviewing default configurations.

## Appendices

### System Diagrams

This section consists of system diagrams that depict the installation of OnGuard in a hardened environment.

## Ports and Endpoints

This section identifies and defines the server sockets and associated operating system privileges that pertain to an OnGuard system.

## Scope of OnGuard Features in 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.

## 8.0\_Acronyms Used in this Guide

### A

- AES: Advanced Encryption Standard

### C

- CEIP: Customer Experience Improvement Program (Microsoft®)
- CN: Common Name
- CIS: Center of Internet Security®
- CSRF: Cross-site Request Forgery

### D

- DIP: Dual In-line Package
- DCOM: Distributed Component Object Model (Microsoft®)
- DDOS: Distributed Denial of Service
- DEK: Database Encryption Key
- DMZ: Demilitarized Zone
- DNS: Domain Name Service
- DOS: Denial of Service

### E

- EAP: Extensible Authentication Protocol
- EEPROM: Electrically Erasable Programmable Read-Only Memory
- EKM: Encryption Key Manager

### F

- FQDN: Fully Qualified Domain Name

## H

- HTTP: Hypertext Transfer Protocol
- HTTPS: Hypertext Transfer Protocol Secure

## I

- IIS: Internet Information Services (Microsoft®)
- IP: Internet Protocol
- ISO: International Organization for Standardization
- IT: Information Technology

## L

- LED: Light Emitting Diode
- LS: Lenel Service

## M

- MIME: Multipurpose Internet Email Extensions

## N

- NIC: Network Interface Card
- NIST: National Institute of Standards and Technology
- NVR: Network Video Recorder (Lenel)

## O

- OEM: Original Equipment Manufacturer
- OSDP: Open Supervised Device Protocol™ (access control)
- OWASP: Open Web Application Security Project

## P

- PII: Personally-Identifiable Information

## Q

- QPID: Qwest Protected Internet Delivery (data transport interface)

## R

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

## S

- SANS: SysAdmin, Audit, Network and Security Institute
- SHA: Secure Hash Algorithm
- SIA: Security Industry Association
- SNMP: Simple Network Management Protocol
- SSL: Secure Sockets Layer

## T

- TDE: Transparent Data Encryption
- TLS: Transport Layer Security

## V


- VLAN: Virtual Local Area Network

## X

- XSS: Cross-site Scripting

## 8.0\_Hardening 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).

 Each 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
- Lock 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 is 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 the 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.

## 8.0\_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 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, and Microsoft® Exchange Server.
- Basic knowledge of enabling or disabling protocols, ciphers, hashes, and key exchange algorithms.

 For a complete list of supported firmware, operating systems, database software, and other third-party components, refer to the version information in the OnGuard Release Notes (DOC-10120-EN-US), or the compatibility charts on the LenelS2 web site: <https://partner.lenel.com/downloads/onguard/software>. Once there, select **Compatibility Charts** from the **Choose type of download** menu.

## 8.0\_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.

 These tools should be considered as examples only and are neither provided nor supported by LenelS2. 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.

## 8.0\_Steps to Hardening Your OnGuard System

Hardening your OnGuard applications is only one step in securing your environment. Following the hardening steps below 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.
12. Do not:
  - Run any other programs on OnGuard servers. These servers should be dedicated to the OnGuard system.
  - Run any uncertified third-party integrations on the OnGuard system.
  - Modify the database schema or store third-party data in the OnGuard database.
  - Use group accounts or super accounts for integration access or for OnGuard Cardholder Self Service or OnGuard Policies.
  - Include unnecessary PII in the OnGuard database.

## 8.0\_Secure by Default

Several features are secure by default in order to align with industry best practices for new installations. System administrators should still review these defaults to ensure they align with corporate policies. For OnGuard upgrades, system administrators should review and align with these best practices as some settings may be retained during an upgrade.

The following features are now secure by default:

- TLS 1.2 is now in use by default. For more information, refer to:
  - [8.0\\_TLS](#)
  - [8.0\\_TLS and Cipher Configuration for RabbitMQ](#)
- The License Server is now configured to only operate from a local system. For more information, refer to [8.0\\_License Server](#).

- The License Server is now also configured for HTTPS protocol by default. To change this setting, or to use CA-signed certificates instead of the self-signed certificates provided by OnGuard, refer to "HTTPS Support for the License Server" in the OnGuard Installation Guide (DOC-110).
- Certain password policies and settings are now enabled by default. For more information, refer to:
  - [8.0\\_OnGuard Passwords](#)
  - [8.0\\_Password Best Practices](#)
  - [8.0\\_Password Settings in OnGuard](#)
- License Administration now requires you to create a username and password when it is run for the first time. License Administration is now only accessible by the local user. For more information, refer to "Log into License Administration" in the OnGuard Installation Guide (DOC-110).


## 8.0\_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](#)

## 8.0\_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.

 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 7.6. 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 [8.0\\_Hardware Scope](#).
  - For a list of applications considered in this guide, refer to [8.0\\_Software Scope](#).
  - For a list of legacy services exceptions excluded from hardening considerations, refer to [8.0\\_Deployment of OnGuard in a Highly Secure Environment](#).
- 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/](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).

## 8.0\_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, LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420
- **Series-3 Downstream Interface Modules:** LNL-1100-S3, LNL-1200-S3, LNL-1300-S3, LNL-1320-S3, LNL-1324e
- **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

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

## 8.0\_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 [8.0\\_System Diagrams](#) and [8.0\\_Ports and Endpoints](#).

## 8.0\_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

 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.

## 8.0\_OnGuard Thin Client Applications

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

- OnGuard Access Manager
- OnGuard Cardholder Self Service
- OnGuard Credentials
- OnGuard Monitor
- OnGuard Policies
- OnGuard Reports
- OnGuard Surveillance
- OnGuard Users
- OnGuard Visitor
- OnGuard WATCH

## 8.0\_OnGuard Servers and Services

The following servers and services are installed with OnGuard:

- LS Client Update Server
- LS Badge Printing Service
- 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 Lenel OpenAccess
- LS Replicator
- LS Reporting Server
- LS Site Publication Server
- LS Web Event Bridge
- LS Web Service
- RabbitMQ Service

The following servers and services are optional and only installed when optional browser-based modules (OnGuard Cardholder Self Service, OnGuard Policies, and OnGuard WATCH) are installed:

- LS Cardholder Self Service

- LS Policies Service
- OnGuard WATCH servers and services:
  - LS OGW Application Server Collector
  - LS OGW FastCGI Web Server
  - LS OGW Log File Collector
  - LS OGW Metrics Receiver
  - LS OGW Metrics Summarizer
  - LS OGW Resource Collector
  - LS OGW Threshold Processor

## 8.0\_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. LenelS2 continues to replace these applications in future releases of OnGuard. For a complete list of legacy web technologies, refer to [8.0\\_Scope of OnGuard Features for a Highly Secured Environment](#).

## Chapter 2 : 8.0\_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.

### 8.0\_Protocols

Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices, from servers and routers to endpoints, can communicate regardless of the differences in their underlying infrastructures, designs or standards. Network security protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data. This applies to virtually all data types regardless of the network medium used.


### 8.0\_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 deployed, 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>.

### 8.0\_TLS

For recommended best practices regarding TLS and cipher suites, refer to [8.0\\_Protocol Hardening Guide](#).

 As discussed in the Protocol Hardening Guide appendix, as of the publication of this hardening guide, Microsoft still has no public ETA for TLS 1.3. Since OnGuard was implemented primarily on a Microsoft technology stack, OnGuard cannot fully support TLS 1.3 until Microsoft releases support for standards that are compliant and interoperable with TLS 1.3 through their SChannel APIs.

### 8.0\_TLS and Cipher Configuration for RabbitMQ

By default, TLS communication with the RabbitMQ server is restricted to TLS v1.2. In addition, the supported set of ciphers are explicitly defined.

**i** If changes to the default configuration are made, restart the server, or run the following commands from the RabbitMQ command prompt:

```
rabbitmq-service stop
rabbitmq-service start
rabbitmqctl start_app
rabbitmqctl environment (repeats back configuration changes)
```

For more information, refer to the following websites:

- TLS Support: <https://www.rabbitmq.com/ssl.html>
- Troubleshooting TLS-enabled Connections: <https://www.rabbitmq.com/troubleshooting-ssl.html>

## 8.0\_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 Service) sub-section in “OnGuard and the Use of Certificates”

**i** The OnGuard Installation Guide is available on the LenelS2 Web Site: <https://partner.lenel.com/downloads/onguard/user-guides>. (You will need to 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) in the certificate 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.

## 8.0\_Peer Certificates

Peer verification is recommended in production environments where the identity needs verification that the user is authorized to access and use an application. For those sites that require strong security, it is highly recommend that self-signed certificates be replaced with commercial certificates for such validation.

## OnGuard Message Broker and Client Applications


Peer certificates can be used to provide mutual authentication between the message broker, which uses the RabbitMQ Message Broker software, and client applications. Before a connection between both the client application and host machine can be made, the client application and host machine must authenticate their identities to each other. A peer, X.509 certificate is used to represent the identity of the host machine.

By default, the RabbitMQ connections are encrypted via TLS, and use a traditional username and password combination for authentication. By verifying the identity of each machine via its trusted certificate, peer certificate validation strengthens the authentication mechanism between components.

Peer verification is highly recommended in production environments where some services do not reside on the same primary application server that contains the Message Broker. One such service that can benefit from peer certificate verification is the LS Badge Printing Service because it does not need to reside on the primary application server with the other services.

If an end user elects to enable peer verification, then all host machines where the OnGuard services reside must have a properly configured peer certificate.

For more information on setting up peer certificates, refer to “Performing Peer Verification on Clients Connecting to LS Message Broker Server” in the OnGuard Installation Guide (DOC-110).

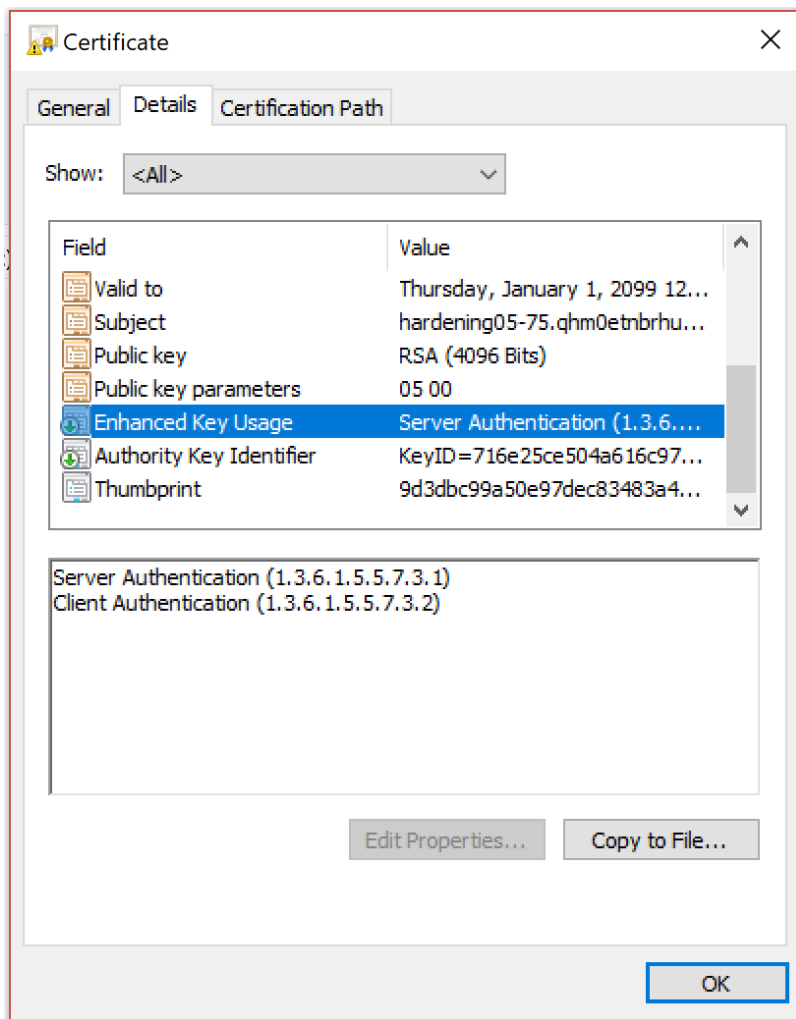
 If the certificate is protected with a passphrase, then peer certificates cannot be leveraged.

### Requirements for Peer Certificate Verification

The default certificates generated as part of the OnGuard installation do not support peer certificate verification. In order to use peer certificate verification, purchase certificates from a commercial certificate authority, or regenerate SSL certificates using an existing public key infrastructure (PKI).

If requesting a server certificate for your application server, ensure that it contains the following enhanced key usage object identifiers:

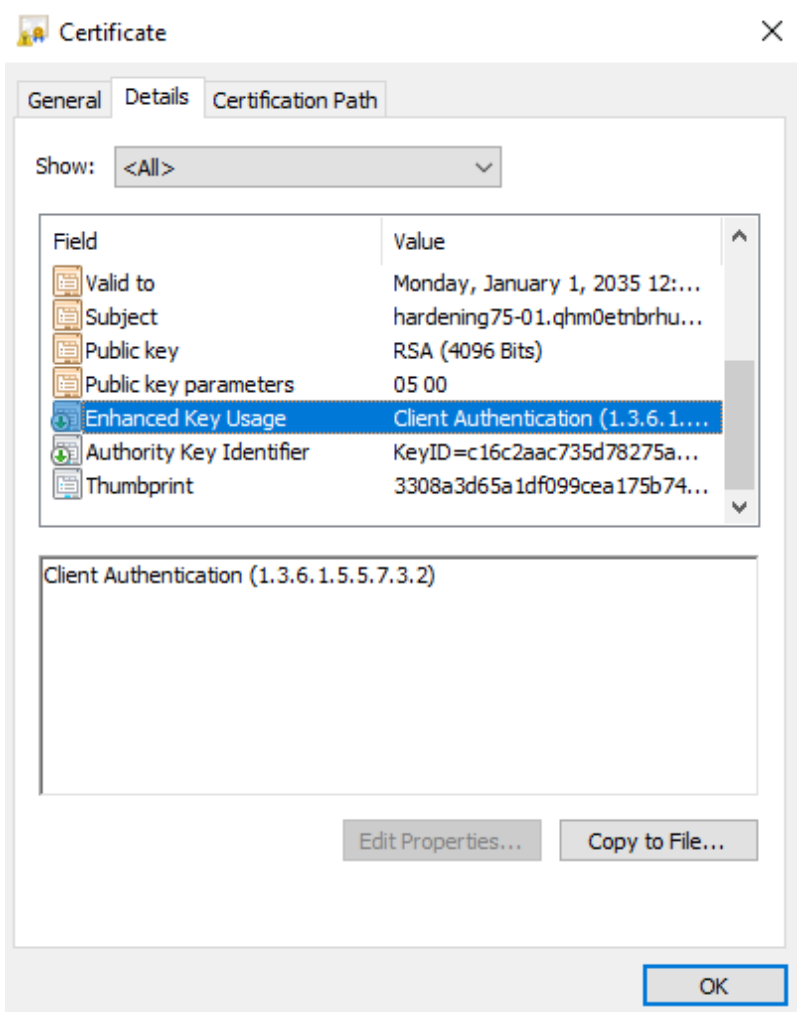
- 1.3.6.1.5.5.7.3.1-Server Authentication
- 1.3.6.1.5.5.7.3.2-Client Authentication



#### *Server Certificate with Server and Client Authentication Object Identifiers*

If requesting a client certificate for a badge printing station, for example, ensure that it contains the following enhanced key usage object identifier:

1.3.6.1.5.5.7.3.2-Client Authentication



*Client Certificate with Client Authentication Object Identifier*

## Video Peer Certificates

### Prevent Automatic Redirects

It is strongly recommended that the customer reconfigure the web server to prevent hackers from altering the intended URL to send users to destinations used for malicious intent such as collecting sensitive information or infecting with malware.

Preventing automatic redirects will ensure that only the intended URL is used. However, for those customers who do not install commercial certificates on their recorders after having prevented the automatic redirect, users will have to execute some manual steps to accept the self-signed certificate on their client systems. This is not recommended as it reduces the level of security protections and places additional burden on the user.

To ensure security of video connections, the customer should replace self-signed certificates with a valid certificate from a Certificate Authority (CA). With a valid certificate in place on the machine running Video Web Services, video from that recorder will be presented assuring proper trust between the recorder and OnGuard services.



If the customer replaces the self-signed certificate with a valid certificate from a CA and takes steps to prevent automatic redirects as recommended, no other action is needed. With a valid certificate in place, video from that recorder/OVWP is presented without the need to execute any manual steps.

To prevent automatic redirects:

1. Navigate to the NGINX\conf folder.
  - For Lenel NVR: **C:\Program Files (x86)\LNVSuite\nginx\conf.**
  - For UltraView and OVWP: **C:\Program Files (x86)\LenelS2 Video Web Services\nginx\conf.**
2. Open the **modules** folder.
3. Delete the **redirect.conf** file.

### If the Default Self-Signed Certificate is Not Replaced

When inserting a camera from one of these systems into a cell in the OnGuard Surveillance client, or launching video from one of these systems in the OnGuard Monitor client, video is not rendered and the user is prompted with a link to “Test security certificate.” Clicking on this link directs the browser to the recorder (or OVWP, as the case may be), and the user may follow the prompts to accept the self-signed certificate (for more information, refer to the “Connection Failed” topic in the Troubleshooting section of the online help in OnGuard Surveillance or OnGuard Monitor). Typically, after completing these steps to accept the self-signed certificate, the browser is automatically redirected back to the client application (OnGuard Surveillance or OnGuard Monitor). However, in this scenario, redirection is not automatic. As a result, the user must manually relaunch the client application (OnGuard Surveillance or OnGuard Monitor).

As an alternative to the above workflow, the user can proactively accept the certificate by opening the browser and navigating to the following URL: **https://<FQDN of video server>:<HTTPS port>/. From there, follow the prompts to accept the certificate.** The “video server” in the above example is the recorder or OVWP, as the case may be. The user can then launch the OnGuard client application, and video from that recorder/OVWP is presented without the need to follow any additional steps.


## 8.0\_Service Accounts


To increase security and reduce risk, service accounts for users should be configured following the principle of least privilege in which all users should log on with accounts that have only the absolute minimum permissions necessary to complete the tasks they need to complete while logged on.


### 8.0\_OnGuard Services

By default, OnGuard services are run as the Local System account or local administrator account. It is recommended that the logon user (the service account) be a low privilege account.

Follow the steps below to ensure that all OnGuard services are running securely. For a list of the OnGuard services, refer to [8.0\\_OnGuard Servers and Services](#).

 In the steps shown below, the user account identified as “Service Account” can be a local user account, an Active Directory account, or a virtual service account. For more information, refer to <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts>.

 These steps require changes made to the registry keys on the OnGuard system. It is highly recommended to make a backup copy of the registry keys before making any changes.

 The following list provides examples of utilities that can be used to manage system security. Consult with your IT administrator before using any utility to edit your system's registry.

- **icacls:** A Microsoft® Windows native command line utility capable of displaying and modifying the security descriptors on folders and files. An access control list is a list of permissions for securable object, such as a file or folder, that controls who can access it.
- **subinacl:** A command-line tool that enables administrators to obtain security information about files, registry keys, and services, and transfer this information from user to user, from local or global group to group, and from domain to domain.
- **Process Monitor:** An advanced monitoring tool for Microsoft® Windows that shows real-time file system, Registry and process/thread activity.

1. Identify the service account to use for the OnGuard services.
2. Assign service account ACL permissions for the registry keys listed in [8.0\\_Registry Keys for OnGuard Services](#).
3. Assign service account ACL permissions to the resources (for example, files and folders) listed in [8.0\\_Resources for OnGuard Services](#).
4. Assign service account ACL permissions for specific HTTP endpoints listed in [8.0\\_HTTP Endpoints for OnGuard Services](#).
5. Add an inbound firewall rule for Replicator (replicator.exe).

For example:

```
netsh advfirewall firewall add rule name="OnGuard Replicator Rule" profile=domain,private protocol=any enable=yes
DIR=in program="C:\Program Files (x86)\OnGuard\replicator.exe" Action=Allow
```

## 8.0\_Registry Keys for OnGuard Services

Assign service account ACL permissions for the registry keys listed below.

Registry Key	User Group/ Service Account	Permissions
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS Badge Printing Service  Alter keys and subkeys. Represents an OnGuard Windows service.	Service Account	Full Control (F)
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS Client Update Server  Alter keys and subkeys. Represents an OnGuard Windows service.		

Registry Key	User Group/ Service Account	Permissions
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS Communication Server  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS Config Download Service  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS DataConduit Message Queue  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS DataConduit Message Service  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS DataExchange Server  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS Global Output Server  Alter keys and subkeys. Represents an OnGuard Windows service.		

Registry Key	User Group/ Service Account	Permissions
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS ID Allocation  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS License Server  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS Linkage Server  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS Login Driver  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS Message Broker  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ LS Module Manager  Alter keys and subkeys. Represents an OnGuard Windows service.		

Registry Key	User Group/ Service Account	Permissions
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS OpenAccess  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS Web Service  Alter keys and subkeys. Represents an OnGuard Windows service.		
HKEY_CURRENT_USER\Software\Lenel  Alter keys and subkeys.		
HKEY_CURRENT_USER\Software\Policies\Microsoft\SystemCertificates  Alter keys and subkeys.		
HKLM:\SOFTWARE\Microsoft\EnterpriseCertificates  Alter keys and subkeys.		
HKLM:\SOFTWARE\WOW6432Node\Microsoft\WBEM\CIMOM  Alter keys and subkeys.		
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Lenel  Alter keys and subkeys.		

## 8.0\_Resources for OnGuard Services

Assign service account ACL permissions to the resources (for example, files and folders) listed below.

Resource	User Group/ Service Account	Permissions
C:\Program Files (x86)\OnGuard Alter folder, subfolders, and files.	Service Account	Full Control (F)
C:\ProgramData\Ln Alter folder, subfolders, and files.		
C:\ProgramData\Lenel Alter folder, subfolders, and files.		
C:\Windows\ACS.ini Alter files.		
C:\Windows\SysWow64\*.ssdl Alter files.		
C:\Windows\SysWow64\*.msl Alter files.		
C:\Windows\SysWow64\*.csdl Alter files.		

## 8.0\_HTTP Endpoints for OnGuard Services


Assign service account ACL permissions for specific HTTP endpoints.


HTTP Endpoint	User Group/ Service Account	Permissions
Web Event Bridge Add http://*:8049/ to urlacl	Service Account	Full Control (F)
NGINX/OpenAccess Web Service Add https://*:8080/ to urlacl		

## 8.0\_OnGuard WATCH Services

By default, OnGuard WATCH services are run as the Local System account or local administrator account. It is recommended that the logon user (the server account) be a low privilege account.

Follow the steps below to ensure that all OnGuard WATCH services are running securely. For a list of the OnGuard services, refer to [8.0\\_OnGuard Servers and Services](#).

 These steps are based on a built-in machine account, “Network Service,” but can also be used on an Active Directory account or a virtual service account.

 These steps require changes made to the registry keys on the OnGuard WATCH system. It is highly recommended to make a backup copy of the registry keys before making any changes.

1. Identify the service account to use for the OnGuard WATCH services.
2. Assign service account ACL permissions for the registry keys listed below.

Registry Key	User Group/ Service Account	Permissions
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS OGW Application Server Collector	Service Account	Full Control (F)
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LSOGWFASTCGIWEBSERVER		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS OGW Log File Collector		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS OGW Metrics Receiver		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS OGW Metrics Summarizer		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS OGW Resource Collector		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS OGW Threshold Processor		

## 8.0\_RabbitMQ Service Account

Use the following steps to ensure the RabbitMQ service account is a low privilege account.

1. Stop the RabbitMQ service.
2. Change the logon account for the RabbitMQ service to the <serviceaccount>.
3. Assign service account ACL permissions for the registry key listed below

Registry Key	User Group/ Service Account	Permissions
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RabbitMQ	Service Account	Full Control (F)

4. Assign service account ACL permissions to **C:\Program Files\erl10.4\erts-10.4\bin\erlsrv.exe**.  
The path above is the default erlang (RabbitMQ) installation path.
5. Assign service account ACL permissions to **C:\Users\<serviceaccount>\AppData\Roaming\RabbitMQ**.
6. Copy the erlang.cookie from **C:\Windows\System32\config\systemprofile\.erlang.cookie** to %userprofile%\erlang.cookie.  
The %userprofile% variable is associated with the <serviceaccount>.
7. Restart the RabbitMQ service.



8. Go to the RabbitMQ command prompt and type `rabbitmqctl status`.  
If there are any error messages in the command prompt output, refer to the diagnostics section for suggestions on resolving the errors.

## 8.0\_OnGuard Policies

By default, OnGuard Policies service runs as the Local System account or local administrator account. It is recommended that the logon user (the server account) be a low privilege account.

Follow the steps below to ensure that all OnGuard Policies services are running securely.

1. Stop the OnGuard Policies service.
2. Change the logon account for the OnGuard Policies service to the **<serviceaccount>**.
3. Assign the service account ACL permissions for the registry key listed below.

Registry Key	User Group/Service Account	Permissions
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LS Policies Service	Service Account	Full Control (F)

4. Assign service account ACL permissions to **C:\Program Files (x86)\OnGuard\Policies\LnI.APM.APIService.exe.config**.  
This path is the default installation path for OnGuard Policies.
5. Restart the OnGuard Policies Service.

## 8.0\_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.

## 8.0\_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.

## 8.0\_Printer Security


OnGuard 7.6 and higher allows badge printing on networked printers. When implementing security best practices, printers with network access should be treated like any other endpoint. Networked printers that are not treated as such can be targets of cyber attacks because they:

- Often fall out of focus for IT departments.
- Are more sophisticated and contain many more capabilities than their predecessors, such as the abilities to scan and fax.
- Possess operating systems and control capabilities similar to computers.
- Often go without hardening and patching that would be required of other such capable endpoints.
- Are shipped and installed with many open default ports, such as common TCP and UDP ports.

If networked printers are not hardened, an attacker can gain access through wireless access points, or from infected computers. Once an attacker has access, they can scan for exploitable systems and pivot to other connected machines on the internal network, and/or cause a DDOS. An attacker can also gain access to the printer's print spool, which may contain sensitive information.

## Hardening best practices for networked printers

- Inventory all printer endpoints and update them with the latest patches available.
- Change all default passwords and ensure that all passwords are encrypted.
- For more information, refer to [8.0\\_Accounts and Passwords](#).
- Disable any rarely used or extraneous services, such as File Transfer Protocol (FTP).
- Select management protocols that provide encryption (HTTPS or SSH).
- If possible, segment networked printers from enterprise systems by placing the printers on a VLAN, thus preventing printers from having access to the entire internal network.
- If possible, place the printer behind a firewall to limit access.

 OnGuard leverages the printer settings made in the workstation's operating system. For more information, refer to **Control Panel > Printers** in the operating system and the documentation for the printer.

## 8.0\_Client-side Protections

To protect against malicious attacks or vulnerabilities, it is important to ensure that the following best practices for client-side protections are in place.

- It is highly recommended that all clients are protected within your network and are actively monitored.
- Install only clients that are required on specific workstations, limiting the install base to the fewest number of workstations needed.
- Restrict physical access to workstations to authorized personnel only. It is not recommended that you have unattended workstations, but if they are required, then they should be reduced to only those that are absolutely necessary.
- Customers with workstation clients in exposed physical spaces, such as unmanned workstations, should consider the use of virtual terminal services to further protect such endpoints.
- The first line of defense is denying local administrator access to workstation users so an attacker cannot take advantage of user privileges in order to install malware or attack tools.
- Restrict users from being able to temporarily disable anti-virus protection and any additional protections provided by OnGuard Services. Consult your OnGuard Advanced Services project leader for such OnGuard Services.
- Ensure that users are aware of the dangers of clicking on unknown links and consenting to the installation of unauthorized software.
- Enact strong complex passwords.
- Conduct an examination of anti-virus solutions and ensure that:
  - Anti-virus monitoring is enabled on all workstations.
  - Rules are enacted to prevent installation of potentially unauthorized software.
  - Anti-virus solutions include protections for process memory injections and providing memory exploit mitigation. Note that most freeware anti-virus will not remove these tools that can be used for further memory exploits. This is important as Kernel malware circumvents this abstraction of privileges by running in kernel mode with direct access to all system services. In other words, it has complete control of the infected system. One attack vector is the installation of a malicious driver.
  - Anti-virus software does not whitelist kernel mode process tools such as 'process hacker.'
  - Leverage anti-virus heuristics for further protections.
- Disable all USB access to prevent loading of unapproved software that can be used to perform the attack. It is recommended to disable USB ports both through policy settings and physical port blockers.
- Implement firewalls on all workstations. Configure the firewall to block all incoming connections, from the Internet and the local area network, to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world. This can help prevent self-propagating infections from spreading.
- Implement a whitelist for all outbound connections.
- Implement a strong patch management process. Patching helps eliminate software flaws that can be used to inject malicious kernel code.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- If not required, turn off file sharing. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Enable SMB signing.
- Disable SMBv1.
- If not in use, disable Web Proxy Auto-detect.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.

- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

To protect against malicious attacks or vulnerabilities, it is important to ensure that the following best practices for client-side protections are in place.

- It is highly recommended that all clients are protected within your network and are actively monitored.
- Install only clients that are required on specific workstations, limiting the install base to the fewest number of workstations needed.
- Restrict physical access to workstations to authorized personnel only. It is not recommended that you have unattended workstations, but if they are required, then they should be reduced to only those that are absolutely necessary.
- Customers with workstation clients in exposed physical spaces, such as unmanned workstations, should consider the use of virtual terminal services to further protect such endpoints.
- The first line of defense is denying local administrator access to workstation users so an attacker cannot take advantage of user privileges in order to install malware or attack tools.
- Restrict users from being able to temporarily disable anti-virus protection and any additional protections provided by OnGuard Services. Consult your OnGuard Advanced Services project leader for such OnGuard Services.
- Ensure that users are aware of the dangers of clicking on unknown links and consenting to the installation of unauthorized software.
- Enact strong complex passwords.
- Conduct an examination of anti-virus and ensure that:
  - Anti-virus monitoring is enabled on all workstations.
  - Rules are enacted to prevent installation of potentially unauthorized software.
  - Anti-virus solution has protections for process memory injections and providing memory exploit mitigation. Note that most freeware anti-virus will not remove these tools that can be used for further memory exploits. This is important as Kernel malware circumvents this abstraction of privileges by running in kernel mode with direct access to all system services. In other words, it has complete control of the infected system. One attack vector is the installation of a malicious driver.
  - Anti-virus solutions do not whitelist kernel mode process tools such as 'process hacker.'
  - Leverage anti-virus heuristics for further protections.
- Disable all USB access to prevent loading of unapproved software that can be used to perform the attack. It is recommended to disable USB ports both through policy settings and physical port blockers.
- Implement firewalls on all workstations. Configure the firewall to block all incoming connections, from the Internet and from the local area network, to services that should not be publicly available. By default, all incoming connections should be denied access, and only services that are explicitly offered to the outside world, should be allowed access. This helps prevent self-propagating infections from spreading.
- Implement a strong patch management process. Patching helps eliminate software flaws that can be used to inject malicious kernel code.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- If not required, turn off file sharing. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Enable SMB signing.
- Disable SMBv1.
- If not in use, disable Web Proxy Auto-detect.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.

- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

## Chapter 3 : 8.0\_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.

To see how OnGuard is installed in a hardened environment, refer to [8.0\\_System Diagrams](#).

### 8.0\_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:

- 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 the clients, servers and network-attached devices to the VLAN.

### 8.0\_Hardening the Databases

Securing your databases helps to ensure data is not lost or leaked and unauthorized access is prevented.

#### 8.0\_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).

## 8.0\_Enabling TLS/SSL Encryption for an Instance of SQL Server

To support encryption of data in transit, 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>.

## 8.0\_SQL Server Database Roles

The database account used by the LenelS2 OnGuard, Windows®-based thick clients include 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 OnGuard database, but other databases residing on the same server.


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

 For general, everyday use of OnGuard, the LenelS2 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 created 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:
  - a. public
  - b. db\_datareader
  - c. db\_datawriter
  - d. db\_ddladmin
  - e. db\_executor

 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
```

8. Click OK to apply the changes made.

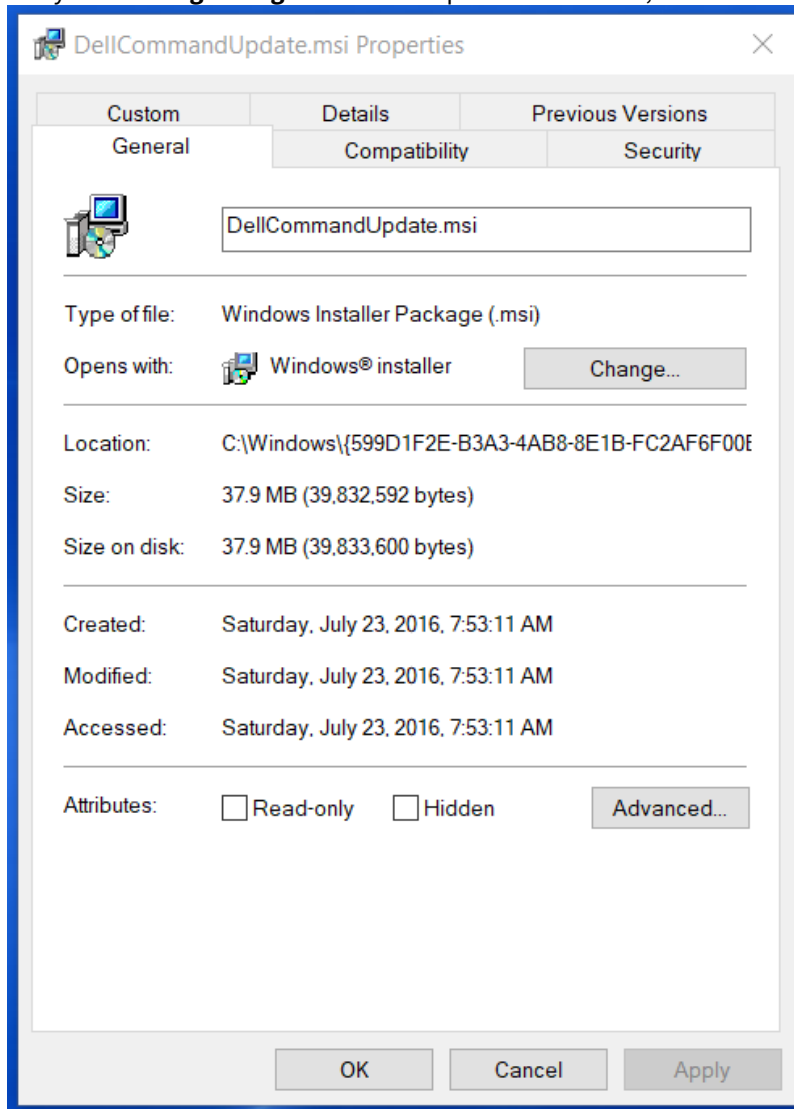
## 8.0\_LenelS2 Installation Packages

Use the following steps to verify that the certificate issued by VeriSign for a LenelS2 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**.

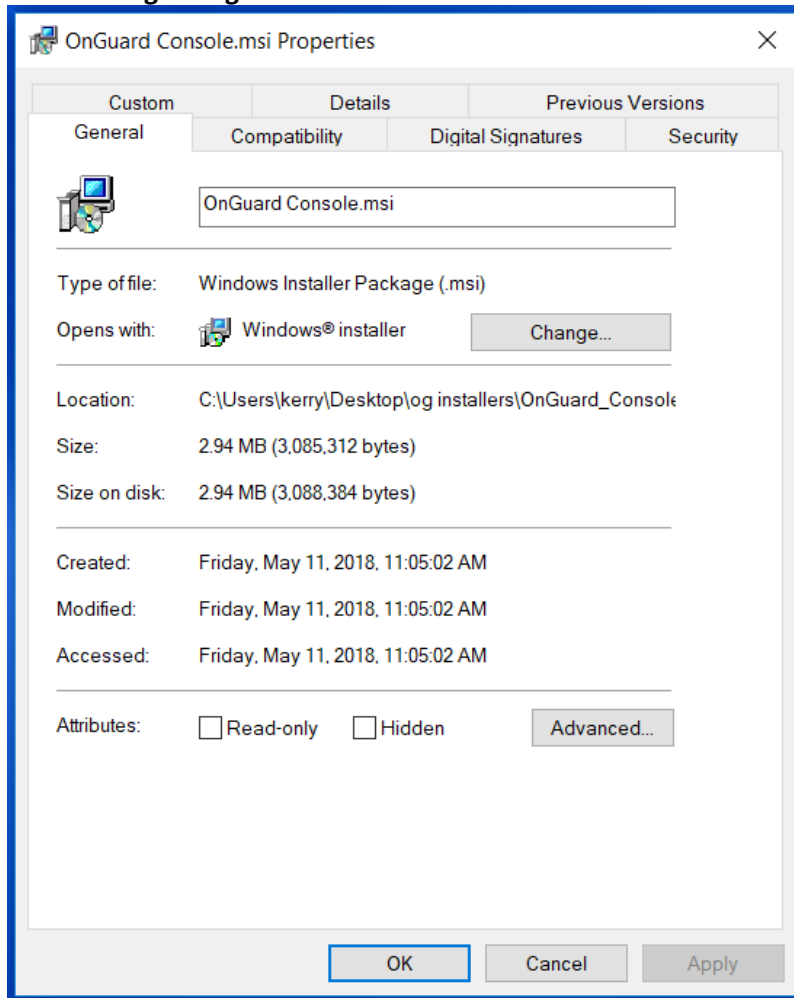


4. Verify that the **Digital Signatures** tab is present. If it is not, the installer is not signed and should not be trusted.



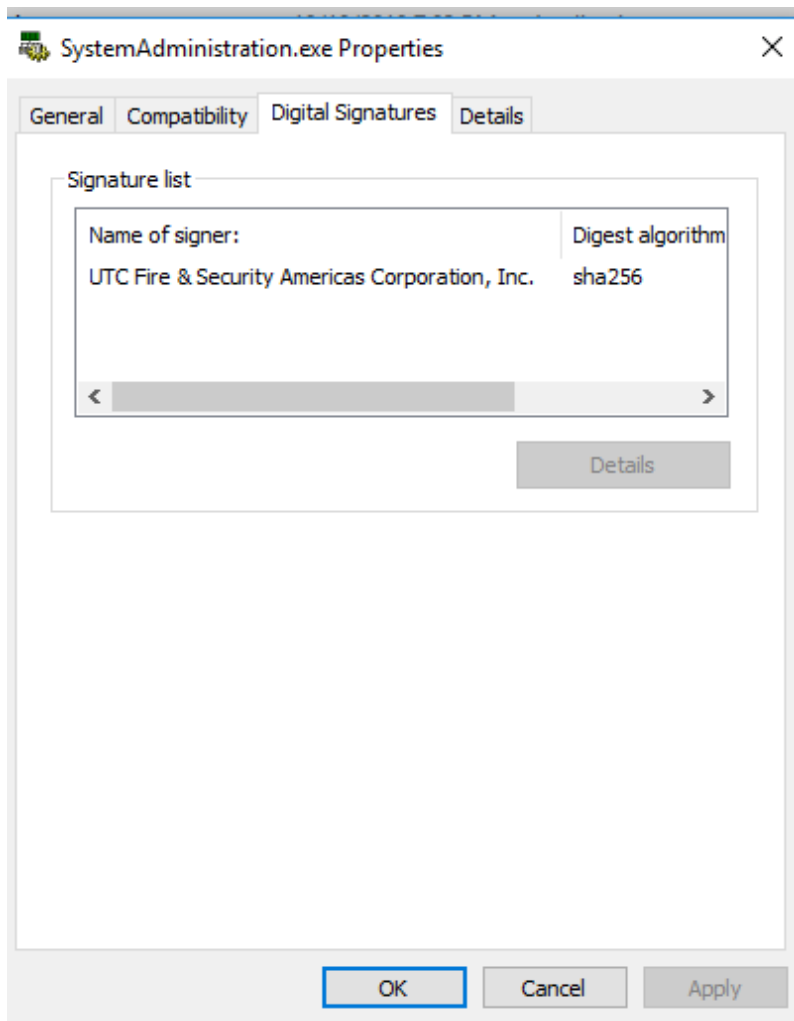
*Unsigned .MSI File*

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



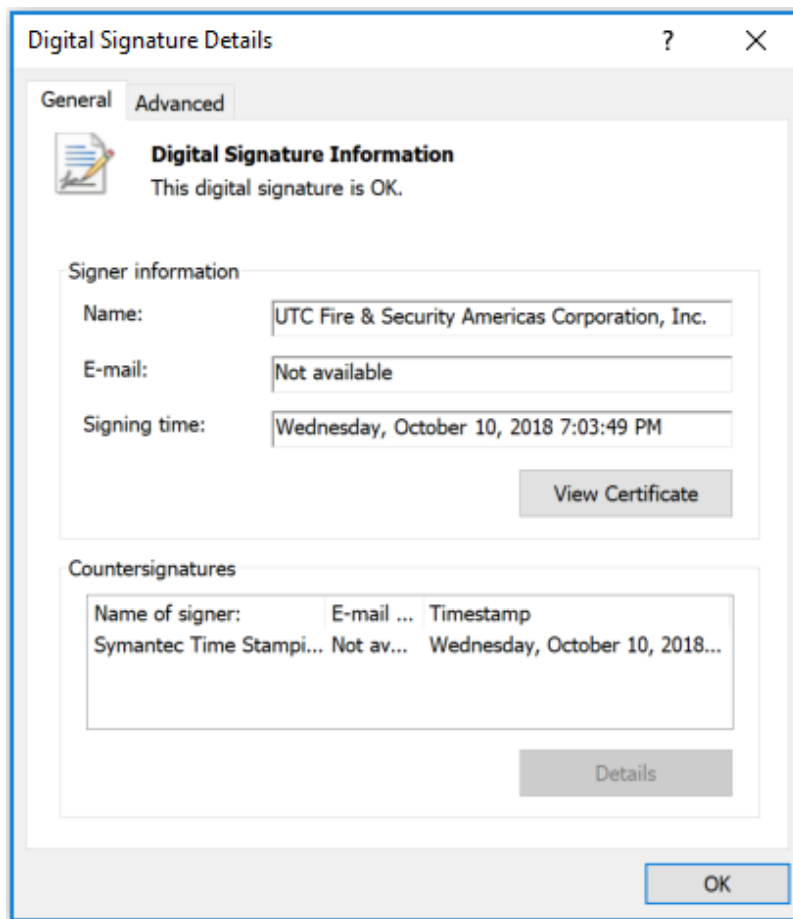
*Signed .MSI File*

6. Under **Signature list**, verify that an entry named “UTC Fire & Security Americas Corporation, Inc.” is present. If not, the installer was not signed by LenelS2 and should not be trusted.



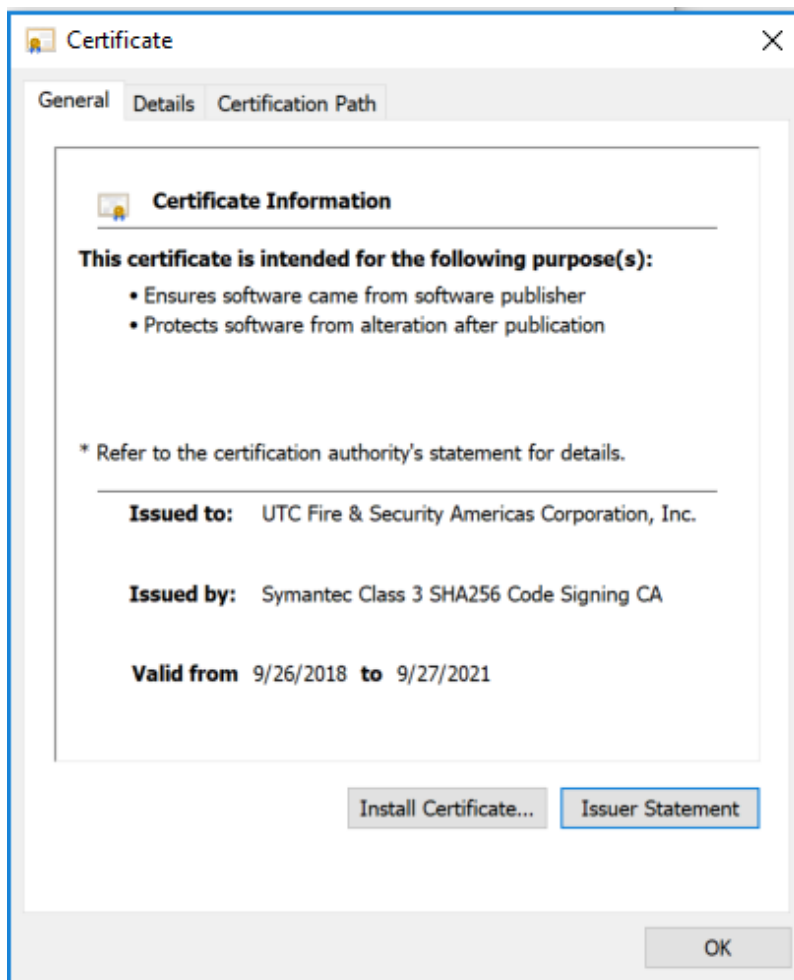
*Digital Signatures Tab*

7. Select the "UTC Fire & Security Americas Corporation, Inc." signature line and click **Details**.
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 states "Issued By: Symantec Class 3 SHA256 Code Signing CA" should be present. If not, then the certificate is not signed by the certification authority used by LenelS2 and should not be trusted.



*Certificate Information*

11. If the installation package from LenelS2 successfully passes each of these steps, it can be assumed that the certificate issued by Symantec to LenelS2 is valid and can be trusted.

## 8.0\_OnGuard Servers, Services, and Utilities

This section contains guidelines on how to harden servers, services, and utilities specific to the OnGuard system.

### 8.0\_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 8.0 > 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.

## 8.0\_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 100;
        limit_req zone=req_limit_per_ip burst=200 nodelay;
    }
}
```

 The above values of 100 for connection limit and limit per IP burst are default values. These values may need to be adjusted depending on the customer environment.

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_conn_module.html)
- [http://nginx.org/en/docs/http/ngx\\_http\\_limit\\_req\\_module.html](http://nginx.org/en/docs/http/ngx_http_limit_req_module.html)

## 8.0\_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 username 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 usernames. If the name is changed, make sure to update or create a corresponding user account in the database.

## 8.0\_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).

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.

LenelS2 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 Port 5657 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

**i** 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.

**i** Although Message Broker Port 5672 is opened by the OnGuard Security Utility, this port is no longer used by OnGuard and should be closed after the utility has been run unless the administrator determines there is a business need for Port 5672.

## 8.0\_OnGuard Applications

This section contains guidelines on how to harden applications specific to the OnGuard system.

### 8.0\_OpenAccess Session Management

When using an application built on the OpenAccess platform, such as an OnGuard thin client (browser-based) application (refer to [8.0\\_OnGuard Thin Client Applications](#)), the **authenticated\_token\_timeout** property and the inactivity timeout will have the same timeout settings applied to every client of the OpenAccess server. In an OnGuard Enterprise system, these properties can be configured at each region to support local usage and regulation of the applications.



The **authenticated\_token\_timeout** property 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).

The inactivity timeout can be configured in the OnGuard Users thin client (browser-based) application.

- i** 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 on 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.

## 8.0\_Accounts and Passwords

To properly harden the OnGuard system, all default passwords must be changed by the customer to passwords that comply, at a minimum, with the password standards detailed in this hardening guide. For more information, refer to [8.0\\_OnGuard Passwords](#).

### 8.0\_Default Accounts and Passwords

To optimize system security and system hardening, default passwords that are created during the installation of the OnGuard software must be changed by the customer. Refer to the following table for the default passwords created during installation.

Description	Username	Password	How to change the password
<p><b>Default system administrator account</b></p> <p>This is the account that is used initially to log into the main OnGuard applications, such as System Administration.</p> <div> <p><b>i</b> After logging into OnGuard, create an SA Delegate user with all permissions and as the SA Delegate user, disable the default system account user.</p> </div>	SA	SA	<p>Refer to "Change the System Administrator Password for the Database" in the OnGuard Installation Guide (DOC-110). The OnGuard Installation Guide is available on the LenelS2 Web Site: <a href="https://partner.lenel.com/downloads/onguard/user-guides">https://partner.lenel.com/downloads/onguard/user-guides</a>. (You will need to login to gain access to this site.) When accessing the Downloads section at <a href="https://partner.lenel.com">https://partner.lenel.com</a>, make sure to select the version of OnGuard that is currently installed.</p>

Description	Username	Password	How to change the password
<p><b>OnGuard database</b></p> <p>This is the actual OnGuard SQL Server Desktop Engine, SQL Server, or Oracle database.</p> <p>By default, the login name for the LenelS2 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.</p>	LENEL	Secur1ty#	Refer to "Change the Database Password" in the OnGuard Installation Guide (DOC-110).

## 8.0\_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 with LenelS2 OnGuard Technical Support. This account and its password should not be used for general operation or shared with multiple users.

### Key Points for System Administrator Password Change

- 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 LenelS2 OnGuard Technical Support at (800) 631-6046.

#### Other points to consider:

- This password is intended to be used during system commissioning and is not intended for daily system operations.
- Integrator and End-User should have a defined process for awareness of any password changes and access to the password when necessary.
- Creation of [SA Delegate accounts](#) assigned to specific users are recommended after commissioning.

## 8.0\_OnGuard "SA" Delegate User

A "SA" Delegate account can be created by the default system account user and assigned all permissions. Then the SA Delegate can disable the default system account to meet the needs for NO Default User Account Names.

- After logging into OnGuard, create an SA Delegate user with all permissions as the SA Delegate user, and then disable the default system account user.

For more information, refer to the OnGuard Installation Guide (DOC-110).

## 8.0\_OnGuard Passwords

The following standards are enabled by default in OnGuard:


- A password cannot be:
  - the same as the corresponding username (for example, “SA” and “SA”)
  - a prohibited keyword
  - blank
- OnGuard user passwords are case-sensitive
- Database passwords:
  - must conform to the rules of the specific database being used
  - are case-sensitive in Microsoft® SQL Server® and Oracle®12c

## 8.0\_Password Best Practices

- Always consult with your corporate password policies. Depending on your corporate 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 14 characters. Consider setting a stricter requirement for administrators or those with privileged roles to be a minimum of 14 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.

## 8.0\_Password Settings in OnGuard

An OnGuard system administrator can use OnGuard® Users, a browser-based application included with the OnGuard 8.0 platform, to configure and enforce password policies for internal accounts in OnGuard.

-  When user accounts are linked to domain (or directory) accounts to allow the use of single sign-on to the workstation and any OnGuard application, password policies these user accounts are configured outside of OnGuard. Password policy settings made in OnGuard Users do not apply to OnGuard user accounts linked to domain accounts.

The following settings represent current minimum recommendations, which can, and should, be adjusted to reflect corporate password policy settings associated with a given customer environment.

To optimize the security of your password settings in OnGuard:

1. From the Lenel Console, click the Users card to launch the OnGuard Users thin client (browser-based) application.
2. Click **Password Settings**.
3. In the **Expiration** section, update the password settings as follows:
  - a. Click the **Password expiration** check box.
  - b. Set the **Expiration time** to no more than 90 days.
4. In the **Complexity** section, update the password settings as follows:

- a. Click the **Minimum password length** check box.
  - b. Set the minimum number of password characters to 14.
  - c. Click the check boxes to require:
    - Numeric characters
    - Special (!@#\$%^&\*) characters
    - Uppercase and lowercase characters
  - d. Click the **History prevents reuse of recent password** check box.
  - e. Set the number of previous passwords to at least 3.
5. Save the changes made to the password settings and exit out of the OnGuard Users thin client (browser-based) application.

## 8.0\_Logon Authorization Warning

The Log on authorization warning in **System Administration > General System Options** form configures the text for the authorization warning that is displayed in an Authorization Notification window when logging into OnGuard.

It is highly recommended that Administrators inform users of possible legal implications of malicious actions carried out against the system. This can be accomplished by selecting either the standard warning message, or by creating a custom message. For more information, refer to the OnGuard System Administration User Guide (DOC-200).

## 8.0\_RabbitMQ Management Plugin

The RabbitMQ management plugin provides an HTTP-based API for management and monitoring of RabbitMQ nodes and clusters, along with a browser-based UI and a command line tool, **rabbitmqadmin**. This plugin allows anyone with admin privileges to access and change RabbitMQ configurations, including users and hosts.

To ensure your system is secured, remind system administrators of the following:

- Do not enable the RabbitMQ management plugin.
- Make sure that only trusted computers can connect to the RabbitMQ message broker.
- Do not allow untrusted software or personnel on the machines.

For more information on the RabbitMQ management plugin, refer to <https://www.rabbitmq.com/management.html>.

## Chapter 4 : 8.0\_Device Communication Hardening

This section provides hardening guidelines for communication between OnGuard and the LenelS2 X-Series and 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 [8.0\\_Hardware Scope](#).

### 8.0\_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.	<p><a href="#">8.0_Device Installation</a>: Place product on a private network, in a secured enclosure, with updated firmware and normal DIP switch settings.</p> <p><a href="#">8.0_Embedded Web Server</a>: Enable HTTPS.</p> <p><a href="#">8.0_User Accounts</a>: Remove the default user login and create a unique user account with a strong password.</p> <p><a href="#">8.0_Equipment Replacement</a>: Perform the bulk erase procedure on the controller and clear the EEPROM on the Interface Modules.</p>
Intermediate	Corporations that have a dedicated system administrator.	<p><a href="#">8.0_Embedded Web Server</a>: Add authorized IP addresses.</p> <p><a href="#">8.0_Information Services</a>: Disable discovery and SNMP services.</p> <p><a href="#">8.0_Encrypted and Authenticated Communication</a>: Enable AES or TLS encryption.</p>

Protection Level	Recommendation	Procedures
Enterprise	Large networks with an IT/IS department. Intended for integration into an enterprise network infrastructure.	<p><a href="#">8.0_Information Services</a>: Enable SNMPv3 (LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420, LNL-4420).</p> <p><a href="#">8.0_Encrypted and Authenticated Communication</a>: Generate and load customized peer certificates and enable TLS.</p> <p><a href="#">8.0_Port-Based Network Access Control</a>: Enable 802.1X.</p> <p><a href="#">8.0_Data at Rest Encryption</a>: Enable data encryption at rest (LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420, LNL-4420).</p>

## 8.0\_Device 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.

## 8.0\_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.

**i** The following controllers do not support HTTP: LNL-4420, LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420. 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

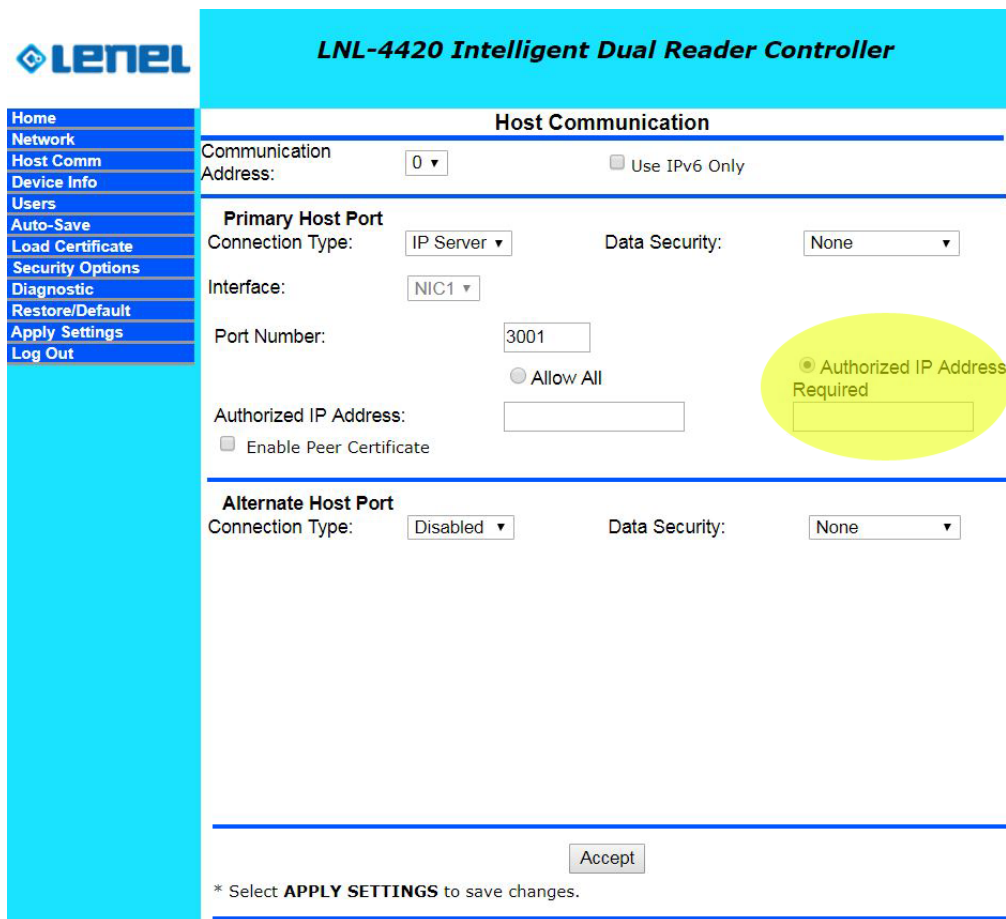
## Authorized IP Addresses

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.





**LENEL** **LNL-4420 Intelligent Dual Reader Controller**

**Host Communication**

Communication Address:  ☐ Use IPv6 Only

**Primary Host Port**

Connection Type:  Data Security:

Interface:

Port Number:

☐ Allow All ☒ Authorized IP Address Required

Authorized IP Address:

☐ Enable Peer Certificate

**Alternate Host Port**

Connection Type:  Data Security:

\* Select **APPLY SETTINGS** to save changes.

Authorized IP Addresses

## 8.0\_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 LenelS2 X-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):

- a. 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.
- b. 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	<ul style="list-style-type: none"> <li>• Eight-character minimum</li> <li>• Must not contain the username</li> <li>• Meets all three criteria points (see <a href="#">Password Criteria</a>)</li> </ul>
Medium	<ul style="list-style-type: none"> <li>• Eight-character minimum</li> <li>• Meets two criteria points (see <a href="#">Password Criteria</a>)</li> </ul>
Low	Six-character minimum

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

 The following controllers require a high strength password: LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420.

## 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 %)

## 8.0\_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 [Authorized IP Addresses](#).

## 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 [Authorized IP Addresses](#).


## 8.0\_Encrypted and Authenticated Communication

Use the following settings to improve encryption and authentication methods.

### 8.0\_Encryption between OnGuard and the LenelS2 X-Series and Access Series Controllers

The controllers support 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).

 The Encryption for Controllers User Guide is available on the LenelS2 Web Site: <https://partner.lenel.com/downloads/onguard/user-guides>. (You will need to 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.

### 8.0\_AES Encryption

Enable AES encryption by configuring both the controller and OnGuard. Load the encryption keys (128 or 256-bit) on both sides before enabling AES.

### 8.0\_TLS Encryption

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.

**i** The LNL-2210, LNL-2220, and LNL-3300 only support TLS 1.1.

The LNL-4420, LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 support TLS 1.2.

Starting with Firmware version 1.290, TLS is enabled by default for the LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 controllers. For more information, refer to:

- "Configuration via Web Page" in the Hardware Installation Guide (DOC-600)
- "TLS Configuration" in the Encryption for Controllers User Guide (DOC-1200)

**LENE** **LNL-4420 Intelligent Dual Reader Controller**

**Host Communication**

Communication Address: 0 ☐ Use IPv6 Only

**Primary Host Port**

Connection Type: IP Server **Data Security: TLS Required**

Interface: NIC1

Port Number: 3001

☒ Allow All ☐ Authorized IP Address Required

Authorized IP Address:

☐ Enable Peer Certificate

**Alternate Host Port**

Connection Type: Disabled Data Security: None

\* Select **APPLY SETTINGS** to save changes.

### Host Authentication

## 8.0\_Authentication between the LenelS2 X-Series and Access Series Controllers 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).

**i** The Encryption for Controllers User Guide is available on the LenelS2 Web Site: <https://partner.lenel.com/downloads/onguard/user-guides>. (You will need to 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 the controller, peer certificates are loaded through the Load Certificate page on the embedded web server, or, if implemented, through OnGuard. Likewise, the peer certificate of the controller must be loaded into the certificate store in OnGuard to mutually authenticate the validity of the controller.

### Load Certificate

- The LNL-4420, LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 controllers support larger key sizes and higher SHA size.
  - RSA Key Size:
    - 4096-bit maximum
    - Factory default is 2048 for the LNL-4420; 3072 for the LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 controllers
  - SHA Size: sha384 maximum (factory default is sha256)
  - Host and SIO Communication TLS Ciphers: FIPS 140 cipher suite
  - Webpage HTTPS/TLS Ciphers:
    - ECDH+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

 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).

## 8.0\_LenelS2 X-Series and Access Series Controller-to-Downstream Device Communication

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

Downstream Device	Description
<b>Series 2:</b> LNL-1100, LNL-1200, LNL-1300, LNL-1320	<ul style="list-style-type: none"> <li>Only supports AES128 encryption</li> <li>Must be configured and enabled</li> </ul>
<b>Series 3:</b> LNL-1100, LNL-1200, LNL-1300, LNL-1320	<ul style="list-style-type: none"> <li>Supports AES128 and AES256.</li> <li>For LNL- LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 controllers, AES256 encryption is enabled by default.</li> <li>For LNL-2210, LNL-2220, LNL-3300, and LNL-4420 controllers, AES128 is available and must be configured and enabled.</li> </ul>
LNL-1300e	Only supports AES128 encryption. Enabled by default.
LNL-1324e	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).

## 8.0\_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).

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

## 8.0\_Data at Rest Encryption

The ability to encrypt “data at rest” has been implemented to satisfy privacy concerns for end users in the field. The encryption allows the configuration and data files to be stored in an encrypted container such that the files will remain inaccessible if the correct procedure and password are not used.

To enable “data at rest” encryption, select **Enable Encryption Partition** on the Security Options page in the embedded web server.

The screenshot shows the web interface for the LNL-4420 Intelligent Single Door Controller. The left sidebar contains a navigation menu with options: Home, Network, Host Comm, Device Info, Advanced Networking, Users, Auto-Save, Load Certificate, OSDP File Transfer, Security Options (highlighted), Diagnostic, Restore/Default, Apply Settings, and Log Out. The main content area is titled 'Security Options' and contains the following settings:

- ☐ Enable 802.1x Authentication
- 802.1x Settings
  - Authentication EAP Configuration:
  - EAP Identity: (Required)
  - Password:
  - Confirm Password:
- TLS related certificates must be uploaded to the 'Load Certificate' Page.
- ☒ Enable Encrypted Partition (highlighted in yellow)
- 

\* Select **APPLY SETTINGS** to apply changes. \*

*Enable Encrypted Partition*

**i** This feature is only supported on the LNL-4420 (Firmware 1.24.1), LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 controllers.

## 8.0\_Protection Against Replay Attacks on IP Networks

### 8.0\_Host/Controller Communication

The LenelS2 X-Series and Access Series Controllers listed in [8.0\\_Hardware Scope](#) support AES and TLS encryption for host communication. These mechanisms are used to encrypt the data transferred to and from the controller. When using AES encryption (128 or 256-bit), both OnGuard and the controller are loaded with encryption keys set by OnGuard. When using TLS encryption, unique certificates are installed on every controller at the time of production and used to encrypt communication between OnGuard and the controller. Additionally, OnGuard or the embedded web server on the controller may be used to load customized peer certificates to the controller. Encryption and network specific mutual authentication can then be

realized by loading controller peer certificates on the OnGuard system. Different controller models support different key lengths and ciphers. When utilizing AES or TLS, each session is protected using session keys that are generated using a FIPS 140-2 approved (and certified on LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 controllers) random number generator. Additionally, only a single OnGuard connection to the controller is allowed, thus limiting the ability for rouge hosts to connect to the controller. Commands sent to the controller also utilize sequence numbers that reduce the ability to replay commands that are out of sequence.

## 8.0\_Controller/IP-Based Downstream Module Communication

By default, the LNL-1324e and LNL-1300e IP-enabled input/output modules support AES encryption (128-bit) between the controller and downstream module. Additionally, the LNL-1324e supports TLS specifically for the embedded web server. The AES encryption on the LNL-1324e and LNL-1300e is synchronized using a combination of random seed and RSA1024 private/public key pairs generated every time after reboot. When utilizing AES or TLS, each session is protected using session keys that are generated using an FIPS 140-2 approved random number generator. These security mechanisms help protect against replay command attacks.

## 8.0\_Port-Based Network Access Control

### 802.1x Authentication

**i** This feature is only supported on the LNL-4420 (Firmware 1.24.1), LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420 controllers.

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.



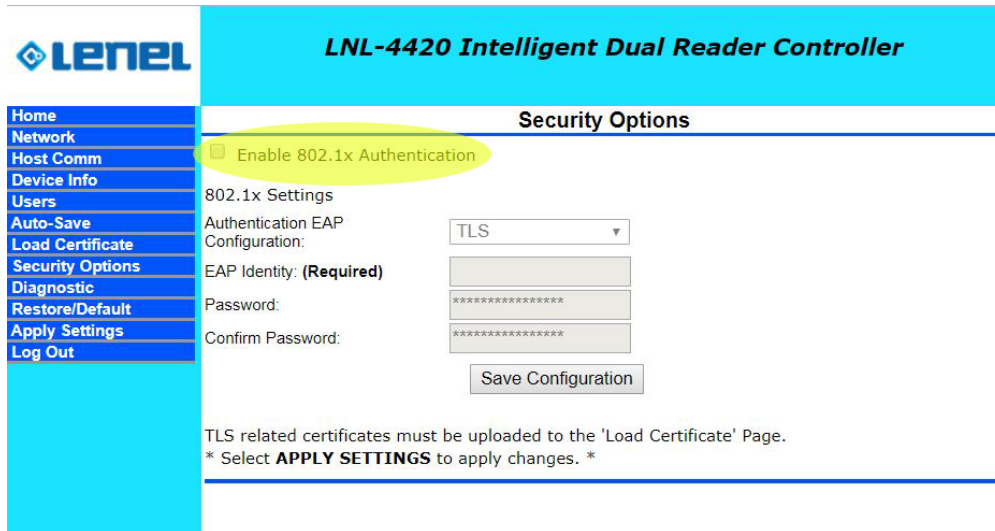


If you are using TLS, ensure that the certificates for the controller are signed by the same root certificate used by the authentication server.

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*

## 8.0\_Equipment Replacement

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

### 8.0\_LenelS2 X-Series and Access Series Intelligent System Controllers

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

#### 8.0\_Bulk Erase Procedure

**i** 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).

## 8.0\_Interface Modules

On the interface module, clear the EEPROM.


### 8.0\_Clearing the EEPROM

 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.

### 8.0\_LNL-1324e Bulk Erase

 Do not remove power during Steps 4-6.

1. Set S1 DIP switches:
  - Switches 1 and 2: ON
  - Switches 3 and 4: OFF
2. Apply power to the LNL-1324e.
3. Watch for LEDs 1 and 2, and 3 and 4, to alternately flash at a 0.5 second rate.
4. Within 10 seconds from applying power, change Switches 1 or 2 to OFF.  
If these switches are not changed, the LNL-1324e powers up using the OEM default communication parameters.
5. LEDs 1 and 2 alternately flash at a 0.5 second rate while the memory is erased.
6. Once the memory is erased, LED will turn on for approximately three seconds, and then the LNL-1324e will reboot.


## 8.0\_Network Ports

The default port for the Host Protocol 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).

## 8.0\_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	Host Protocol	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.

 Configure the Host Protocol to use a different port. The default port is 3001.

## 8.0\_Ports Used by the LNL-X2210, LNL-X2220, LNL-X3300, and LNL-X4420

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	Host Protocol	Yes: Set the Connection Type from the Host Comm page to an option other than IP.

Port	Port Type	Usage	Disable
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.

 The OnGuard integration for OTIS® systems does not require the use of Ports 47307 - 45308 at this time.

## 8.0\_Ports Used by the LNL-1300e

Port	Port Type	Usage	Disable
3001	TCP	SIO Communication Protocol	No

## 8.0\_Ports Used by the LNL-1324e

Port	Port Type	Usage	Disable
161	UDP	SNMP	Yes: Use Disable SNMP Server from the Users web configuration page.

Port	Port Type	Usage	Disable
443	TCP	HTTPS	Yes: Use Disable Web Server from the Users web configuration page.
3001	TCP	Host Protocol	Yes: Set the Connection Type from the Host Comm page to an option other than IP.
4001	TCP	Mercury SIO Communication Protocol (MSP1)	No
5353	UDP	Zeroconf (Discovery)	Yes: Use Disable Bonjour option from the Users web configuration page.

## 8.0\_OSDP Readers

Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP v2.1.7 is currently in-process to become a standard recognized by the American National Standards Institute (ANSI), and OSDP is in constant refinement to retain its industry-leading position. For more information, refer to <https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/>.

OnGuard provides support for OSDP readers. These readers use the SIA OSDP standard for reader communication. In the case of OSDP biometric readers, in addition to the standard access control data exchange, biometric templates are transferred from the controller to the reader when a credential is presented.

## 8.0\_Prerequisites

- Ensure the correct LenelS2 software and licenses are installed:
  - OnGuard 7.4 or higher for OSDP Secure Channel Encryption
- Use LenelS2 X-Series or Access Series controllers that support OSDP Secure Channel Mode for onboard readers or downstream door controllers:
  - LNL-2210 or LNL-X2210
  - LNL-2220 or LNL-X2220
  - LNL-3300 or LNL-X3300 (requires door controller)
  - LNL-4420 or LNL-X4420
- Use LenelS2 door controllers that support OSDP biometrics:
  - LNL-1300e-S2
  - LNL-1300e-S3
  - LNL-1300-S3
  - LNL-1320-S3
- Use supported LenelS2 firmware:
  - LenelS2 firmware for Intelligent System Controllers v1.267 or later
  - LenelS2 firmware for Door Controllers v3.21 or later
- Use OSDP readers that support Secure Channel Mode:
  - LenelS2 BlueDiamond™ Reader (all models)
  - Access control readers from third parties that support OSDP Secure Channel Mode

- Biometric access control readers from third parties that support OSDP Secure Channel Mode

## 8.0\_OSDP Secure Channel Communication

Many installations require secure communication between the controller and the reader. An authentication/encryption scheme called Secure Channel Mode is defined in the OSDP specification. Secure Channel Mode defines a method of implementing encryption, key management, and authentication on an OSDP connection. Using AES-128 encryption and CMAC chaining (see FIPS 197), this method allows relatively easy implementation in controllers and peripheral devices.

## 8.0\_Enable OSDP Secure Channel Mode in OnGuard

Separate documents are available for supported OSDP biometric readers that explain how they are configured for operation with OnGuard.

## 8.0\_Configure Readers for OSDP Secure Channel Mode

The OSDP Standard outlines requirements for establishing a connection between the controller and the reader. However, each reader manufacturer may implement their own process on how to prepare their reader for Secure Channel Connection.

The LenelS2 BlueDiamond™ reader automatically switches from Wiegand communication protocol to OSDP when the connected controller initiates an OSDP connection. Once the LenelS2 BlueDiamond reader is in OSDP mode, it is ready to switch to Secure Channel Mode when instructed by the controller.

If needed, to switch the LenelS2 BlueDiamond™ reader from OSDP Secure Channel to OSDP, or to move it from one reader port to another, the LenelS2 BlueDiamond reader must be reset using one of the available Configuration Cards: BDC-CSN or BDC-DESFIRE.

## 8.0\_Configure OnGuard for OSDP Secure Channel Support

Configuring OnGuard to support OSDP Secure Channel readers and initiate a connection consists of the following:

- [8.0\\_Set Reader Configuration to Support OSDP Biometrics](#)
- [8.0\\_Initiate Secure Connection with the Connected Reader](#)

### 8.0\_Set Reader Configuration to Support OSDP Biometrics

1. In System Administration, go to **Access Control > Readers and Doors**.
2. On the **General** tab, make the following changes:
  - a. Set **Output** to either **OSDP Protocol** or **OSDP Biometric**.
  - b. Check the **Secure channel** check box.
3. Save the changes.

Device	LNL	Interface	Protocol	Port	1	0		
Magnetic Reader	LNL 2220 (Primary)	Onboard Reader	Magnetic	Onboard	0	1		
Morpho Sigma Lite	LNL 2220 (Secondary)	Onboard Reader	OSDP Biometric	Onboard	0	0	0	
Morpho Sigma Lite Prox	LNL 3300	LNL-1320 (Dual Interface)	Wiegand / Prox	Port 2	1	1		
Morpho WR Sigma Prox	LNL 4420	Onboard Reader	OSDP Biometric	Onboard	0	0	0	
NDE Lock 0 GW_2	LNL 3300	Schlage Engage Gateway	Wiegand / Prox	Port 3	0	0		
NDE Lock 1 GW_2	LNL 3300	Schlage Engage Gateway	Wiegand / Prox	Port 3	0	1		
NDE Lock 2 GW_2	LNL 3300	Schlage Engage Gateway	Wiegand / Prox	Port 3	0	2		

General
Grouping
Settings
Controls
Aux Inputs
Aux Outputs
Anti-Passback
Command Programming
Notes

Name: Morpho Sigma Lite
Panel: LNL 2220 (Secondary)
Type: Onboard Reader
Output: OSDP Protocol
Port: Onboard
Address: 0
Gateway Address:
IP Port: 0
OSDP Baud rate: 9600
Address: 0
Primary Reader:
Reader number: 0

Held Open Time: 75
Extended Open: 75
Strike Time: 3
Extended Strike: 5
OSDP
Secure channel
Strike:
Cut off on Close
Do Not Activate Strike on REX
Keypad:
Allow User Commands
Allow Intrusion Commands

Card Format
Type
26 - bit IsoProx (fac code 1) Wiegand
26-bit IsoProx Wiegand
35-Bit IsoProx Wiegand
36-bit IsoProx Wiegand
DESFire CSN Wiegand
Magnetic Card Format Magnetic
SafeTrust Bluetooth Wiegand
Wiegand 35 Wiegand

Reader Modes
Online: Pin or Card
Offline: Pin or Card
Biometric Verify
Cipher
First Card Unlock
Authenticated reader

Encrypted Communications Mode:

System Administration > Access Control > Readers and Doors > General Tab Settings

## 8.0\_Initiate Secure Connection with the Connected Reader

With LenelS2 controllers, the OSDP secure channel connection must be established when the reader is connected to the reader port for the first time, or when it is moved from port to port.

1. In Alarm Monitoring, in the System Status Tree, right-click on the OSDP reader.
2. Select **Remote Link Mode**.
3. Click **Start**.

The screenshot displays the OnGuard 8.0 interface. The top section shows a tree view of system components, including LNL 2220 (Secondary), LNL 3300, and LNL 4420. A context menu is open over the LNL 2220 component, listing various actions such as Acknowledge..., Trace..., Update Hardware Status, and Remote Link Mode. The 'Remote Link Mode' option is highlighted, and a sub-dialog is open with 'Start' and 'Abort' buttons. The bottom section shows the 'Main Alarm Monitor' table, which lists alarm descriptions, time/date, and controllers.

Alarm Description	Time/Date	Controller
Reader Offline Restored	4:07 PM 1/31/2019	LNL 2220 (Secondary)
Reader Offline Restored	4:03 PM 1/31/2019	LNL 2220 (Secondary)
Door Held Open	3:48 PM 1/31/2019	LNL 3300
Door Forced Open	3:47 PM 1/31/2019	LNL 3300
Reader Mode Card Only	3:47 PM 1/31/2019	LNL 3300
Relay Contact Deactivated	3:47 PM 1/31/2019	LNL 3300
Relay Contact Deactivated	3:47 PM 1/31/2019	LNL 3300
Reader Offline Restored	3:47 PM 1/31/2019	LNL 2220 (Secondary)
Panel Download Completed	3:45 PM 1/31/2019	LNL 3300
Reader Mode Card Only	3:45 PM 1/31/2019	LNL 3300
Relay Contact Deactivated	3:45 PM 1/31/2019	LNL 3300
Relay Contact Deactivated	3:45 PM 1/31/2019	LNL 3300
Cabinet Tamper Restored	3:45 PM 1/31/2019	LNL 3300
Power Failure Restored	3:45 PM 1/31/2019	LNL 3300
Alarm Active	3:45 PM 1/31/2019	LNL 3300
Relay Contact Deactivated	3:45 PM 1/31/2019	LNL 3300

Alarm Monitoring > System Status Trees > Remote Link Mode



## Chapter 5 : 8.0\_OnGuard Client Hardening

This section provides hardening guidelines applicable to OnGuard thin client (browser-based) applications.

### 8.0\_HTTP Response Headers

HTTP security headers provide an additional layer of security by helping to mitigate attacks and security vulnerabilities. The settings for HTTP headers used in applications that are built on the OpenAccess platform are made in accordance with industry best practices and compatibility with OnGuard applications as default. Administrators should review the configuration (.conf) files for the OnGuard browser-based applications to ensure the settings align with their policies and procedures.

Header	Response
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 <b>sameorigin</b> , which allows the page to be loaded in a frame only if it has 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 <b>1; mode=block</b> , 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 <b>content-type</b> 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 <b>nosniff</b> .
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 <b>no-store</b> , 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 <b>cache-control</b> HTTP/1.1 header is not yet present. The recommended configuration is to set this header to <b>no-cache</b> .
HTTP strict transport security (HSTS)	This header states that the website must only be accessed over HTTPS protocol. If a user enters an address without including https://, the browser automatically requests https://. Doing so avoids a redirect and can improve website performance.

Header	Response
content security policy (CSP)	This header allows a website to whitelist the resources that are loaded by a website.

The configuration (.conf) files are located at **C:\ProgramData\Lenel\nginx\conf**.

- The **nginx.conf** file includes a reference to the **httpsecurity.conf** file.
- The **httpsecurity.conf** file contains the HTTP header setting configuration.

## 8.0\_Removing a Wildcard Directive from the Content-Security-Policy Header

The default **httpsecurity.conf** file allows websocket connection to any web server so that OnGuard Monitor and OnGuard Surveillance can connect to video recorders like Lenel NVR. It is recommended to replace a wildcard "wss:" directive with a list of video recorders so that only these servers can be approached by the browser.

This can be changed in the following section of **httpsecurity.conf**:

```
map $uri $connect_src {
    /monitor/index.html    "'self' wss:";
    /surveillance/index.html "'self' wss:";
    default                "'self'";
}
```

For example, in a system with a two Lenel NVR's available at servers VIDEORECORDER1 and VIDEORECORDER2 on Port 3001, this section would be:

```
map $uri $connect_src {
    /monitor/index.html    "'self' wss://VIDEORECORDER1:3001 wss://VIDEORECORDER2:3001";
    /surveillance/index.html "'self' wss://VIDEORECORDER1:3001 wss://VIDEORECORDER2:3001";
    default                "'self'";
}
```

After making the changes in the **httpsecurity.conf** file, restart the LS Web Service.

## 8.0\_Required Services for OnGuard Thin Client (Browser-based) Applications

The following matrix identifies the services that must be enabled in order for OnGuard thin client (browser-based) applications built on the OpenAccess platform to function as expected. If your system has services running that are not needed for any of the browser-based applications installed on your OnGuard system, disable them to reduce your system's attack surface.

	OnGuard Services							
Application	LS Message Broker	LS Web Service	LS OpenAccess	LS Event Context Provider	LS Communication Server	LS Web Event Bridge	LS Badge Printing Service	LS Reporting Service
OnGuard Access Manager	x	x	x		x			
OnGuard Cardholder Self Service	x	x	x		x			
OnGuard Credentials	x	x	x		x		x	
OnGuard Monitor	x	x	x	x	x	x		
OnGuard Policies	x	x	x					
OnGuard Reporting and Dashboards	x	x	x					x
OnGuard Surveillance	x	x	x		x			
OnGuard Users	x	x	x		x			
OnGuard Visitor	x	x	x	x	x	x	x	
OnGuard WATCH	x	x	x		x			

## Chapter 6 : 8.0\_Appendices

### 8.0\_Protocol Hardening Guide

#### Overview

Given the importance of maintaining the highest degree of reasonably achievable security in our products, securing the attack surface is especially critical. This section focuses on the configuration of cryptographic protocols, which are often the first line of defense against a remote attacker. While the majority of these protocols are built upon TLS, there are no widely accepted industry standards for the configuration of these components, and often the cryptographic settings are buried within application specific settings.

This section attempts to present cryptographic protocol best practices, which should be updated as security trends evolve. It also attempts to present a mapping of these best practices into specific configuration details for the various third-party and operating system components, while presenting a normalizing of vendor terminology to the terms used in academic security literature.

#### A Primer on Cipher Suites

In a simple world, a cryptographic protocol would use a single, standard set of algorithms to communicate between endpoints. In the real world, security threats and defenses are constantly evolving, so most long-lived cryptographic protocols are continually improved. These often include a communication step where the endpoints present a list of their available protocol variations with the goal of both sides agreeing to use the strongest mutually available configuration. This negotiation phase also exists to facilitate that various governments have at times outlawed the development or use of strong encryption within or across their borders, so the protocol also allows endpoints to agree on the strongest configuration they are allowed to use at that time.

Cryptographic protocol configuration can be quite complicated as these are complex systems built from several different algorithms serving different functions. These functions include:

- **Key Exchange:** How keys are securely agreed upon between the endpoints.
- **Cipher:** The cipher used to encrypt data, block or stream depending on application.
- **Mode:** How the cipher is used to encrypt data, such as the block mode and how it is initialized.
- **Padding:** How transmitted blocks are padded when less than a full block is sent.
- **Message Authentication:** How data is verified as not being modified between endpoints.

There are lists of algorithms available for each of these functions, each of which may have multiple configurations (such as ranges of key size), not all of which are compatible with each other across their entire range of possible settings.

A 'cipher suite', a term that came into widespread use in early SSL specifications, is a specification of the full set of cryptographic primitives that are used together in a protocol. For example, 'TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA' is a TLS protocol, using RSA for key exchange, the block cipher is 3DES that is used in Cipher Block Chaining mode using encrypt-decrypt-encrypt processing, and utilizing SHA (1) for message authentication.

## Why Not Just Say TLS 1.x ?

While it is true that newer TLS versions do add stronger algorithms, as well as remove algorithms that are known to contain critical weaknesses, TLS versions also contain a wide breadth of algorithms that range from the strongest generally available to the weakest deemed necessary for backward compatibility with systems that are less frequently patched. It is also not uncommon for organizations to include older cipher suites in order to support legacy systems. Because of these issues, it is highly desirable and often required to manage protocols at the cipher suite level rather than simply at the TLS level, and this section will cover them at that level.


## Policies for 2020

The following should no longer be used unless no alternative exists for a specific legacy requirement:

- **RSA key exchange:** no forward secrecy
- **DES ciphers:** replaced by AES
- **RC4 ciphers:** known insecure
- **MD5 or SHA-1 hashes:** known insecure
- **Any version of PCT:** deprecated
- **Any version of SSL:** deprecated
- **TLS v 1.0 or 1.1:** deprecated as of March 2020

The following are good guidelines:

- Use the smallest set of cipher suites possible to minimize attack surface against unknown vulnerabilities.
- Use TLS 1.3 perfect forward secrecy wherever possible (most non-Microsoft systems).
- Key exchange order of preference:
  - Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)
  - Diffie-Hellman Ephemeral (DHE)
- Enable TLS Session Resumption to provide performance improvements without compromising security.

 While TLS 1.3 has been generally available since 2018, as of mid-2020, Microsoft has not released TLS 1.3 support in any of their products except their re-branded Google Chrome browser, nor have they published a date when it may be expected. Additionally, the optional beta support available in recent versions of Windows 10 are incompatible with many other TLS 1.3 implementations. Therefore, as of mid-2020, in Microsoft-dependent products, the highest required level of security is TLS 1.2, although it is highly recommended to enable TLS 1.3 in any non-Microsoft subsystems so they can interoperate using higher security whenever possible.

## TLS 1.3 Strong Ciphers

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256
- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_128\_CCM\_8\_SHA256
- TLS\_AES\_128\_CCM\_SHA256

## TLS 1.2 Strong Ciphers

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305
- TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305

## NGINX TLS 1.2 Configuration

### NGINX TLS

```
# Enable TLSv1.2, disable SSLv3.0, TLSv1.0 and TLSv1.1
ssl_protocols TLSv1.2;

# Enable modern TLS cipher suites
ssl_ciphers
'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-
AES128-SHA256';

# The order of cipher suites matters
ssl_prefer_server_ciphers on;
```

## Apache TLS 1.2 Configuration

### Apache TLS Config

```
# Enable TLSv1.2, disable SSLv3.0, TLSv1.0 and TLSv1.1
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1

# Enable modern TLS cipher suites
SSLCipherSuite
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-
AES128-SHA256

# The order of cipher suites matters
SSLHonorCipherOrder on

# Disable TLS compression
SSLCompression off

# Necessary for Perfect Forward Secrecy (PFS)
SSLSessionTickets off
```

## LenelS2 X-Series and Access Series Controllers

In addition to the high security cipher suites, the following cipher suites should be enabled to support the strongest security currently available for the LenelS2 X-Series and 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.

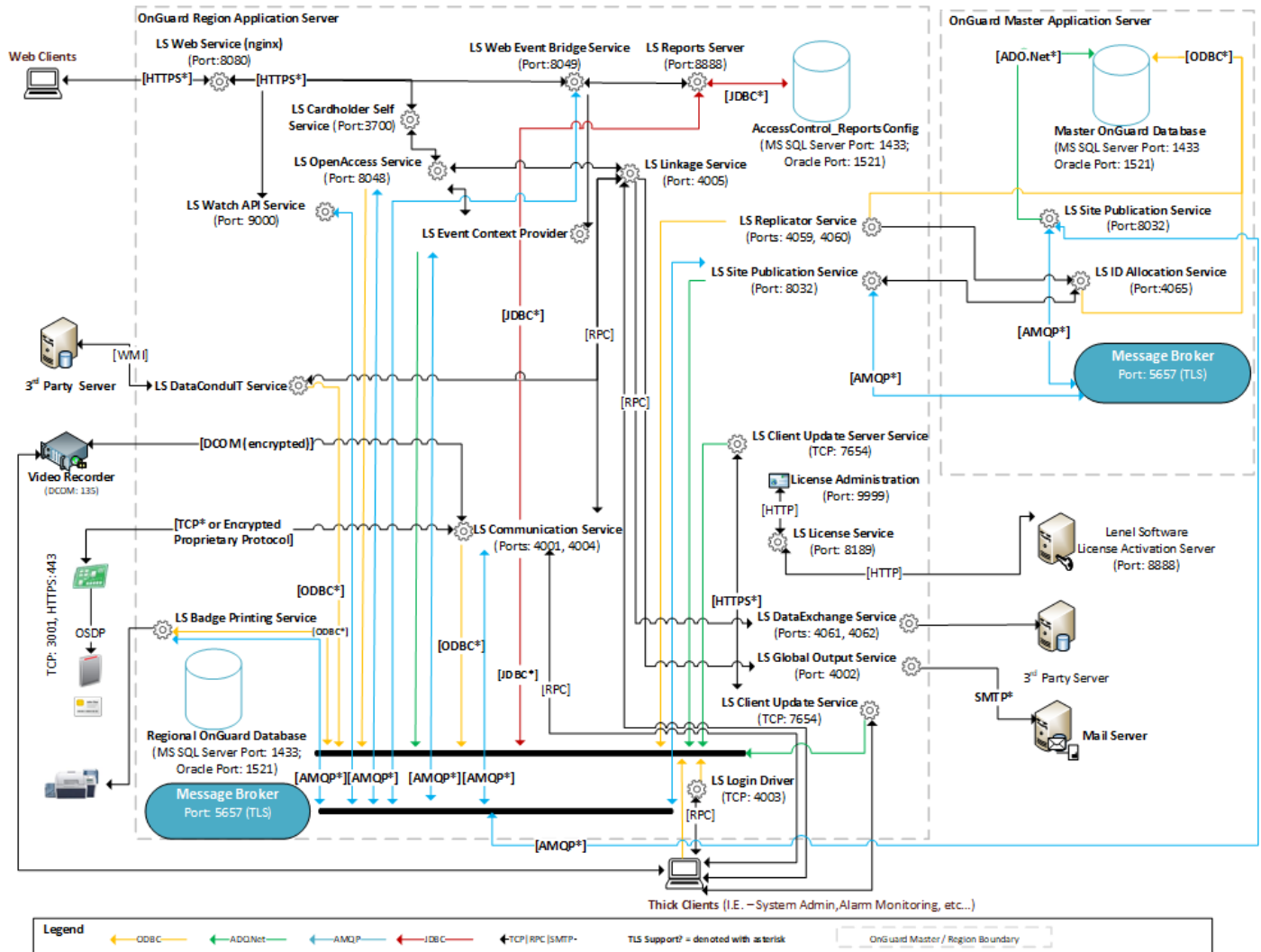
If you are using an LNL-4420, enable the TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 cipher suite.

If you are using any other LenelS2 X-Series or Access Series controller, enable the following cipher suites: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA and TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA.

## 8.0\_System Diagrams

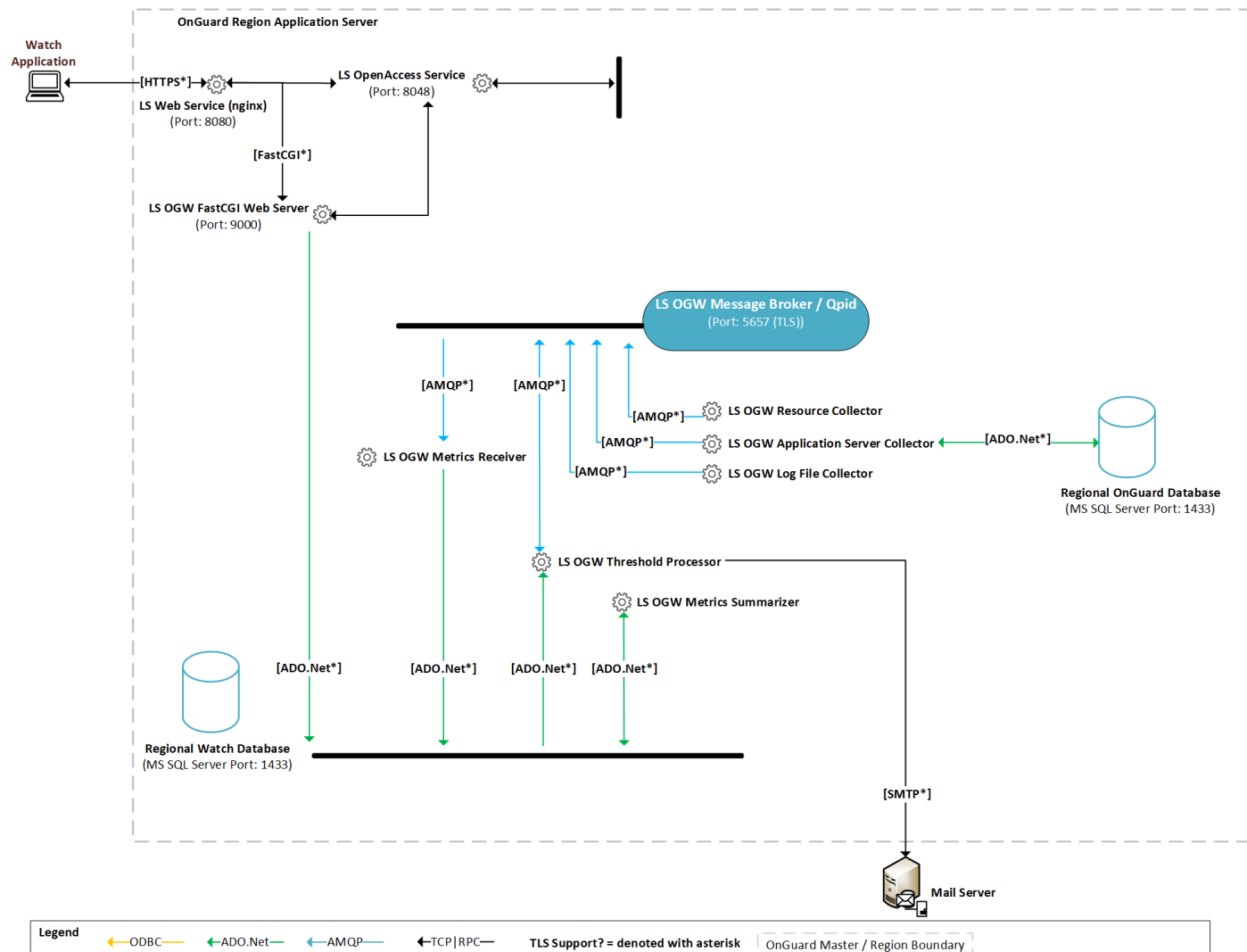
The following system diagram depicts the installation of OnGuard in a hardened environment. For additional, optional, port configurations, refer to [8.0\\_Ports and Endpoints](#).

## 8.0\_OnGuard System Diagram





## 8.0\_OnGuard WATCH System Diagram



## 8.0\_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.

## 8.0\_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	Host Protocol	TLS 1.1, 1.2	LenelS2 Controller	CS	MC	≥5.0	See System Administration
3700			OnGuard Cardholder Self Service	NX	CSS		
4001	MSRPC	No	Communication Server RPC	AAM, AM, CDS, DC, DE, LS, RS	CS	All	ACS.INI [Service] DriverRpcPort
4002		No	Global Output Server RPC	LS	GOS	≥5.0	ACS.INI [Service] GosRpcPort
4003	MSRPC	No	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	No	Linkage Server RPC	SA	CS	All	ACS.INI [Service] DriverSocketPort
4006	MSRPC	No	Video Server RPC	LS, SA	ARC	All	ACS.INI [Service] DriverSocketPort
4009-4057	MSRPC	No	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	MSRPC	No	Replicator RPC	RA, RS	RS	≥5.9	ACS.INI [Service] ReplicatorRpcPort
4061			Lenel® DataExchange Data	LS	DE	≥5.9	ACS.INI [Service] DESocketPort
4062	MSRPC	No	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
5657	AMQP	TLS 1.1, 1.2	LS Message Broker (RabbitMQ)	Everywhere	MB	≥7.0	Security Utility

Port	Protocol	Encrypted	Function	From (client)	To (server)	OnGuard Version	Port Change
5672	AMQP	None	<p>LS Message Broker (RabbitMQ)</p> <p><b>Note:</b> Port 5672 may be used for non-TLS encrypted traffic, if your LS Message Broker (RabbitMQ) service is so configured. By default, this port is not used. You are strongly advised to shut down this port in a production environment.</p>	Everywhere	MB	≥7.0	Security Utility
6071	AMQP	SSL	<p>LS OW Message Broker (QPID)</p> <p>This applies only to OnGuard WATCH 1.3. Starting with OnGuard WATCH 1.4, Ports 6071 and 6072 are not required.</p>	Everywhere	LS OW Message Broker	≥7.5	No

Port	Protocol	Encrypted	Function	From (client)	To (server)	OnGuard Version	Port Change
6072	AMQP	None	LS OW Message Broker (QPID)  <b>Note:</b> Port 6072 may be used for non-TLS encrypted traffic, if your LS OW Message Broker (QPID) is so configured for OnGuard. By default, this port is not used. You are strongly advised to shut down this port in a production environment. This applies only to OnGuard WATCH 1.3. Starting with OnGuard WATCH 1.4, Ports 6071 and 6072 are not required.	Everywhere	LS OW Message Broker	≥7.5	No
7007-7008			SkyPoint® Base Server	CS	SKY	≥7.0	No
7654			LS Client Update Server	CU	CU	≥7.0	System Administration
7702	Bosch Mode 1	No	Bosch® controller	CS	Bosch controller	≥7.5 Update 1	System Administration

Port	Protocol	Encrypted	Function	From (client)	To (server)	OnGuard Version	Port Change
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 Server	Everywhere	LIC	≥5.7	Configuration Editor + LicenseServerConfig\Server.properties
8888			FLEXnet Licensing®	FN	Customer	≥6.1	No
8888	HTTP	No	OnGuard Reports	NX	OR	≥8.0	NGINX config and OnGuard Reports config
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
	UDP/OTIS		Elevator Dispatching Heartbeat	OE	CS	≥5.12	ACS.INI [Otis] SSHHeartbeatPort
	UDP/OTIS		Elevator Terminal Command	CS	OE	≥5.12	ACS.INI [Otis] SSDECCommandPort

## 8.0\_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
DC	Lenel® DataConduIT	LS DataConduIT Service	Local System	WMIService.exe
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

Abbreviation	Description	Service Name	Service Principle	Process File Name
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	IDAllocationService.exe
IIS	IIS Web Server			
LD	Login Driver	LS Login Driver	Local System	logindr.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	MessageBrokerService.exe This file is a wrapper for the RabbitMQ service, which points to erlsrv.exe.
MC	LenelS2 Controllers			
ND	NetDVMS			
NX	NGINX Web Server	LS Web Service	Local System	NginxService.exe (wrapper)
OC	OnGuard Client			
OE	OTIS Elevator Dispatching System			
OR	OnGuard Reports			
OS	OnGuard Server			
RA	Replication Administration			



Abbreviation	Description	Service Name	Service Principle	Process File Name
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			

## 8.0\_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.

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.

Feature	Description
Visitor Management 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 the legacy IIS web-based applications listed above.

# Index

## 8

802.1x authentication [64](#)

## A

Accounts

- system administrator ("SA") [50](#)
- system administrator ("SA") delegate [50](#)

AES

- controller/downstream device communication
  - protection against replay attacks [64](#)
- encryption between OnGuard and controller [59](#)
- host/controller communication
  - protection against replay attacks [63](#)

Architectural assumptions of scope [16](#)

Authentication

- 802.1x [64](#)
- between controller and OnGuard [60](#)

## C

Center of Internet Security (CIS) [16](#)

Certificates

- digital [21](#)
- installation packages
  - verification of [40](#)
- peer
  - requirements for verification [22](#)
  - setup of [22](#)

Ciphers

- configuration for RabbitMQ [20](#)

Client

- protections [35](#), [36](#)

## D

Data at rest encryption [63](#)

Database

- encryption [38](#)

Databases

- Microsoft SQL Server
  - database roles [39](#)

Device communication hardening

- introduction [10](#)

Device discovery

- recommendations for [59](#)

## E

Encryption

- between OnGuard and controller
  - AES [59](#)
  - TLS [59](#)
- controller to downstream device [62](#)
- data at rest [63](#)
- database [38](#)

Endpoints

- introduction [11](#)

## G

Guidelines

- industry accepted [16](#)

## H

Hardening

- best practices for
  - login driver [47](#)
  - NGINX [46](#)
  - OnGuard security utility [47](#)
  - passwords [49](#)
- steps to [15](#)

Hardening fundamentals

- introduction [10](#)

Hardware

- Lenel Access Series
  - authentication between OnGuard and controller [60](#)
  - bulk erase procedure [65](#)
  - clear EEPROM [66](#)
  - encryption between controller and downstream device [62](#)
  - LNL-1324e bulk erase procedure [66](#)
  - protection levels [53](#)
- Lenel Access Series Controllers [17](#)
- Migration Bridge Controllers [17](#)
- scope [17](#)
- Series-2 Downstream Interface Modules [17](#)
- Series-3 Downstream Interface Modules [17](#)

Highly secured environment

- introduction [11](#)

HTTP

- response headers [73](#)

## I

Industry tools

- recommendations [14](#)

Installation package

- verification of [40](#)

International Organization for Standardization (ISO) [16](#)

## L

Lenel Access Series

- device installations
  - recommendations for [54](#)
- embedded web server
  - recommendations for [54](#)
- SNMP
  - recommendations for [59](#)
- user accounts
  - recommendations for [57](#)

LenelS2 X-Series and Access Series

- device discovery
  - recommendations for [59](#)

## License server

- local system
- operation [45](#)

## Login driver

- hardening
- best practices [47](#)

**M**

## Man-in-the-Middle Attacks

- hardening TLS against [20](#)

## Microsoft

- SQL Server
  - database encryption [38](#)
  - database roles [39](#)
  - TLS/SSL encryption [39](#)

**N**National Institute of Standards and Technology (NIST) [16](#)

## NGINX

- hardening
- best practices [46](#)

**O**

## OnGuard

- authentication with controller [60](#)
- browser-based apps
  - required services [74](#)
- controller encryption
  - AES [59](#)
  - TLS [59](#)
- database
  - encryption [39](#)
- deployment in highly secure environment [19](#)
- logging on
  - authorization warning [52](#)
- OSDP secure channel communication
  - configuration with [70](#)
- OSDP secure channel support
  - configuration for [70](#)
- resources
  - isolating with a VLAN [38](#)
- security utility
  - hardening best practices [47](#)
- servers and services [18](#)
- services [25](#)
- standards for
  - passwords [51](#)
- system administrator account [50](#)
- system administrator account delegate [50](#)
- thick client applications [17](#)
- thin client applications [18](#)
- Users (app)
  - password settings [51](#)
- WATCH
  - services [31](#)

## OnGuard application server hardening

- introduction [10](#)

## OnGuard client hardening

- introduction [10](#)

Open Web Application Security Project (OWASP) [16](#)

## OpenAccess

- session management [48](#)

## OSDP

- overview of [69](#)
- prerequisites [69](#)
- secure channel communication [70](#)
  - configuration with OnGuard [70](#)
- secure channel mode
  - reader configuration [70](#)
- secure channel support
  - OnGuard configuration [70](#)

## OSDP secure channel

- reader communication [62](#)

**P**

## Passwords

- best practices for [51](#)
- hardening
  - best practices [49](#)
- settings [51](#)
- standards for [51](#)

## Ports

- introduction [11](#)

## Printers

- hardening
  - best practices [34](#)

## Protections

- client-side [35, 36](#)

**R**

## RabbitMQ

- cipher configuration [20](#)
- service accounts [32](#)
- TLS configuration [20](#)

## Readers

- communication
  - OSDP secure channel [62](#)
- OSDP secure channel mode
  - configuration [70](#)

## Replay attacks

- protection against on IP networks
  - controller/downstream device communication [64](#)
  - host/controller communication [63](#)

**S**

## Security Utility

- hardening
  - best practices [47](#)

## Services

- OnGuard [25](#)
- OnGuard browser-based apps [74](#)
- OnGuard WATCH [31](#)
- RabbitMQ [32](#)
- unnecessary [33](#)

## Skills

- prerequisite [14](#)

## SNMP

- recommendations for [59](#)

## Software

- scope [17](#)

## SSL

- encryption
  - Microsoft SQL Server [39](#)

SysAdmin, Audit, Network and Security (SANS) Institute [16](#)

## System diagrams

- introduction [10](#)

**T**

## TLS

- configuration for RabbitMQ [20](#)
- controller/downstream device communication
  - protection against replay attacks [64](#)
- digital certificates [21](#)
- encryption
  - Microsoft SQL Server [39](#)
- encryption between OnGuard and controller [59](#)
- hardening against Man-in-the-Middle attacks [20](#)
- host/controller communication
  - protection against replay attacks [63](#)

Transparent Data Encryption (TDE) [38](#)

**V**

## VLAN

- isolating OnGuard resources [38](#)

**W**

## Warnings

- OnGuard
  - logon authorization [52](#)



1212 Pittsford-Victor Road  
Pittsford, New York 14534 USA  
Tel 866.788.5095 Fax 585.248.9185  
[www.LenelS2.com](http://www.LenelS2.com)

