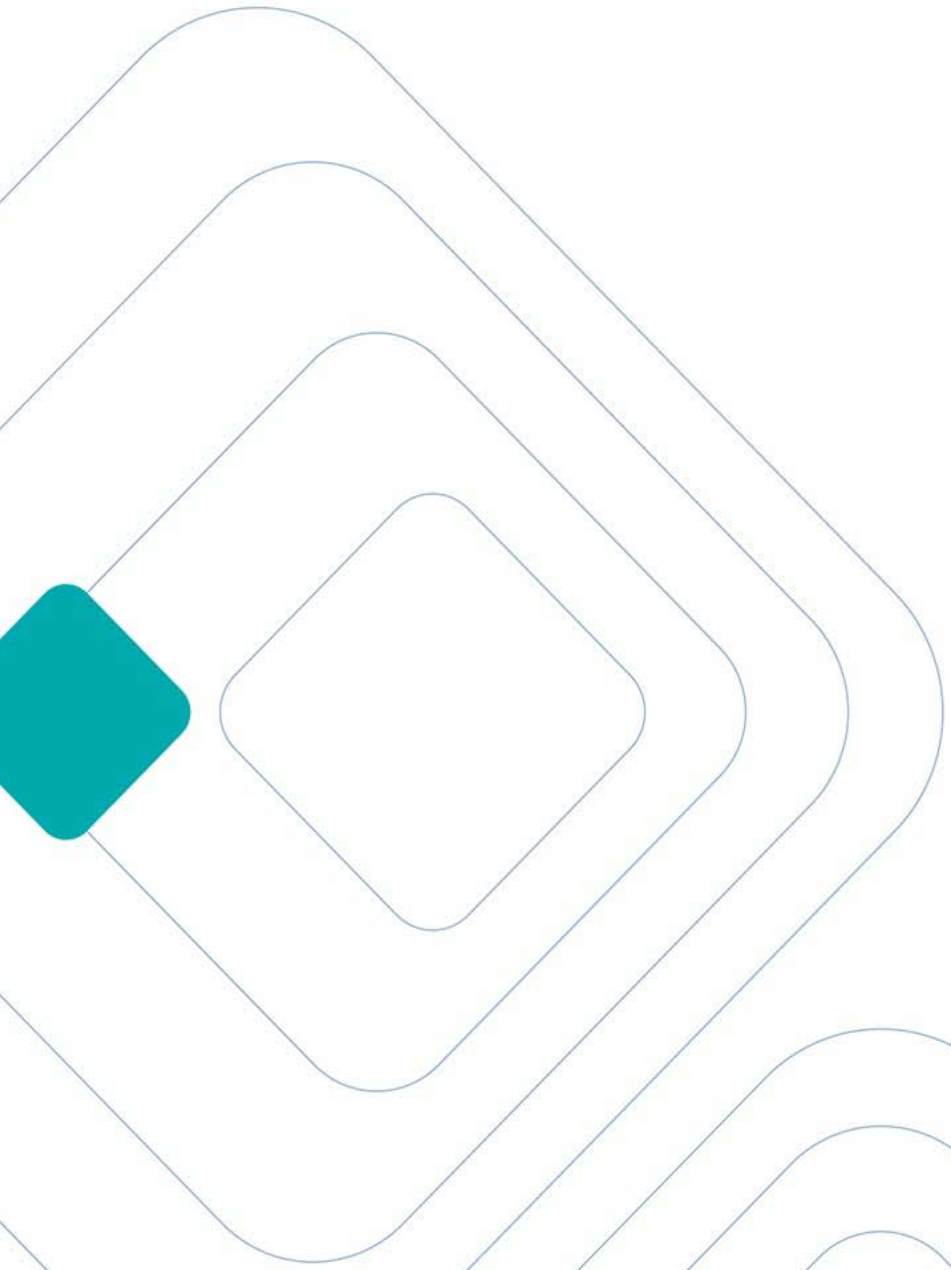
LENEL·S2

OnGuard®

Installation Guide



LenelS2 OnGuard® 8.3 Installation Guide
This guide is item number DOC-110, revision 14.023, September 2024.
©2024 Honeywell International Inc. All Rights Reserved. All trademarks are the property of their respective owners. LenelS2 is a part of Honeywell.

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 Honeywell Security Americas LLC (“LenelS2”), 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 separate 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.

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 in this document may be trademarks or registered trademarks of their respective owners 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 LENELS2 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 LENELS2.

FOR MORE INFORMATION ON PRODUCT WARNINGS AND DISCLAIMERS, SEE THE "LENELS2 PRODUCT WARNINGS AND DISCLAIMERS" KNOWLEDGE BASE ARTICLE IN THE LENELS2 KNOWLEDGE BASE. THIS INFORMATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Table of Contents

CHAPTER 1

About This Guide

The following table describes the different installation guides available.

Advanced Installation Topics. DOC-100. A guide that encompasses a variety of advanced topics including Oracle installation and configuration.

Installation Guide. DOC-110. A comprehensive guide that includes instructions for installing the OnGuard software. This guide also includes information on all supported SQL Server database systems and the browser-based client applications.

Upgrade Guide. DOC-120. A short and sequential guide on upgrading and configuring OnGuard to utilize SQL Server or SQL Server Express.

Enterprise Setup & Configuration User Guide. DOC-500. A guide that includes instructions for installing database software, the OnGuard Enterprise software, and how to setup complex Enterprise systems.

Vocabulary Used

Database System

Refers to the database program that you are using. SQL Server databases can be found in this document. For Oracle installation procedures, refer to the *Advanced Installation Topics* guide.

Server

The computer that your database is stored on. Commonly the most powerful computer on the network.

Client

Refers to the computer(s) that connect to the server.

Workstation

Any computer where OnGuard software is installed.

Hardware Key

Commonly referred to as a “dongle.” It is used on the server as part of the license.

Software License

A license that works without the need for a hardware dongle. When using a software license you are able to use License Administration to activate, return, or repair your license.

CHAPTER 2

Introduction

Installing OnGuard requires you to complete different steps depending on whether you are installing on a server or client machine.

If installing on a server, you must do four things: install your database system, install the OnGuard software, install your license, and set up your database.

If you are installing on a client, you only need to install the OnGuard software and verify that the license has been installed for the system.

Before beginning the installation process you must first check and see that your computer meets the minimum requirements. Specific hardware, operating system, database system, and Web browser requirements must be met prior to the OnGuard installation. Refer to the release notes for those requirements, which are located in the **Program Files\OnGuard\doc\en-US** directory of the OnGuard installation media.

IMPORTANT: LenelS2 software requires certain security adjustments to the operating system to function more securely. If needed, the Security Utility runs during installation. Please review the Security Utility release notes provided prior to running this utility, which then makes these adjustments automatically. Upon agreeing to this disclaimer, the user is assuming responsibility for any security issues that may occur due to these adjustments.

Required Installations and Configurations

The following must be installed and configured before installing OnGuard:

- When installing OnGuard servers or clients, the user account running the installation is required to have Unrestricted Local Administrative Privileges. The user must also have full read and write permissions to the Temp directory (commonly **%USERPROFILE%\AppData\Local\Temp**), as well as the Windows and Program Files directories, with no remapping of home or local drives.
- User Account Control (UAC) must be set to **Never Notify**.
- After mounting the OnGuard ISO file, right-click on **setup.exe** and select **Run as administrator**.

- If installing OnGuard directly on a non-default drive (X), the following setting needs to be added to the **ACS.ini** file so the License Server can locate the JRE:

  ```
  [LicenseServer]
  JAVA_HOME=<X>:\OnGuard\JRE
  ```

  For example, if installing on E drive:

  ```
  [LicenseServer]
  JAVA_HOME=E:\OnGuard\JRE
  ```

- All prerequisite software, on the Supplemental Materials media, must be installed.
- Each OnGuard server/workstation computer, as well as the SQL Server, must be configured for the TCP/IP network protocol prior to installation of the OnGuard software.
- Use of SQL Server with OnGuard Reporting and Dashboards (8.0 and forward), requires SQL Server Configuration to have TCP/IP network protocol as ENABLED prior to installation of the OnGuard software.
- Windows Service Packs should be installed and up to date, but are not provided on the Supplemental Materials media. See the Release Notes for this installation to confirm which service packs are supported.
- All database systems must be a supported version with the latest approved service pack and updates. Refer to the release notes for this installation to confirm which service packs are supported.
- Install the latest approved drivers required for any video capture devices and printers you have installed on workstations.
- LenelS2 Digital Video recorders should be upgraded to the supported version prior to upgrading the OnGuard software. Installation can be found on the Supplemental Materials media.
- Any third-party applications you are using, such as Crystal Reports, must be purchased and upgraded separately. See the Release Notes for this installation to confirm which versions are supported.
- Adobe Reader is not required but is highly recommended as it is needed to read the OnGuard documentation.
- OnGuard servers hosting web applications should be running a supported server operating system. Windows client operating systems have limitations with the number of allowed connections that could impact your licensed functionality.
- Most Windows operating systems limit the hostname to 15 characters. Therefore, the OnGuard installer trims the hostname to 15 characters. If you are installing OnGuard on a workstation running a Windows operating systems that allow hostnames longer than 15 characters, the installation will succeed but the hostname will be trimmed to 15 characters.

Steps for Installing OnGuard

The following steps will take you through OnGuard installation process. Use the following list as a guide while working through the installation process. Installations can be performed by a member of the Administrators Group.

Installing OnGuard with SQL Server

1. Make sure you have the proper hardware requirements.

2. Install and configure SQL Server or SQL Server Desktop Engine. For more information, refer to Chapter 5: Microsoft SQL Server on page 27.
3. Install prerequisites from the Supplemental Materials media. For more information, refer to OnGuard 8.3 Installation Prerequisites on page 41.
4. If your installation will use a hardware license key, refer to Configure a USB Hardware Key on page 42.
5. Install the OnGuard software. For more information, refer to Install the OnGuard 8.3 Software on page 43.
6. Setup Assistant runs automatically. For more information, refer to Setup Assistant on page 45. Setup Assistant performs the following steps:
   a. **Security Utility:** For more information, refer to Security Utility on page 45.
   b. **Configuration Editor:** For more information, refer to Configuration Editor on page 45.
   c. **System License** (License Administration)**:** For more information, refer to System License on page 47.
   d. **Service Log On:** For more information, refer to Service Log On on page 47.
   e. **Database Installation** (for new server installations with SQL Express)**:** For more information, refer to Database Installation on page 47.
   f. **Database Installation (Archival):** For more information, refer to Database Installation (Archival) on page 47.
   g. **Database Backup** (if upgrading an existing installation)**:** For more information, refer to Database Backup on page 47.
   h. **Database Backup (Archival)** (if upgrading an existing installation that archives to an Archival database instead of to text files)**:** For more information, refer to Database Backup (Archival) on page 48.
   i. **Database Setup** (for server installations)**:** For more information, refer to Database Setup and Encryption on page 48.
   j. **Database Setup (Archival):** For more information, refer to Database Setup (Archival) on page 48.
   k. **LS Message Broker Service:** For more information, refer to LS Message Broker Service on page 48.
   l. **Service Startup:** For more information, refer to Setup Assistant then starts all product services configured to start automatically. Setup Assistant lists all services that will be started, each service's status, and provides a progress bar. on page 49.
   m. **Universal Time Conversion Utility** (if upgrading a server running a version of OnGuard earlier than 6.3): For more information, refer to Finished on page 49.

CHAPTER 3

Database Backup and Restoration

You can back up your database using any of the following methods:

- Backing up to a file on a hard drive or network connection.
- Backing up to a CD or DVD.

The chapter also deals with how to restore the backup if needed. The procedures are broken into sections based on the backup option and the type of database you are using. Consult your Database Administrator for the preferred backup method.

Notes: Some of the procedures in this chapter require the use of SQL Server Management Studio. Beginning with Supplemental Materials media revision 16, the SQL Server Management Tools are no longer included. SQL Server Management Tools for Microsoft SQL Server Express are included with Microsoft SQL Server Management Studio Express, and are available at www.microsoft.com. If using a full version of SQL Server, SQL Server Management Studio is included in the full version.

To back up a SQL database with Transparent Data Encryption, refer to the *Backing up a TDE Protected Database* section in the *Advanced Installation Guide*.

Backing Up Your Database to File

This section includes information on how to:

- Automatic Back Up to a File on SQL Server Database on page 18
- One-Time Back Up to a File with SQL Server Express Edition on page 19

In addition to backing up the OnGuard access control database, include the following files to ensure that the database, report history, and custom reports for OnGuard Reporting and Dashboards can be properly restored on a new server:

- **AccessControl_ReportConfig**

  The naming convention for the ReportsConfig database is ***<Live OnGuard database name>*_ReportsConfig**. Since the default name of the Live OnGuard database is *AccessControl*, the default name of the ReportsConfig database is **AccessControl_ReportsConfig**. But if you manually changed the name of your Live OnGuard database to *AccCtrl*, for example, then your ReportsConfig database would be named **AccCtrl_ReportsConfig**.

- ***C:\Program Files\JReport\Server\history***
- ***C:\Program Files\JReport\Server\realm\defaultRealm***

Automatic Back Up to a File on SQL Server Database

The following section will show you how to back up your SQL Server database to a file.

Configure Microsoft SQL Server for Automatic Database Backup to a File

1. From Windows, open the SQL Server Management Studio.
2. Log into SQL Server Management Studio.
3. Navigate to the SQL Server Agent in the Object Explorer.
   a. Right-click the SQL Server Agent and select **Start**.
   b. You will be asked whether you are sure that you want to start the service, click [Yes].
   c. Right-click the SQL Server Agent and select **Properties**.
4. The SQL Server Agent Properties window is shown.
   a. Select the **Auto restart SQL Server if it stops unexpectedly** and **Auto restart SQL Server Agent if it stops unexpectedly** check boxes.
   b. Click [OK].

   Expand the Management folder in the Object Explorer.
5. Right-click on the Maintenance Plans folder and select **Maintenance Plan Wizard**.
6. The SQL Server Maintenance Plan Wizard is shown. Click [Next].
7. On the Select Plan Properties window:
   a. In the **Name** field, enter a name for the maintenance plan.
   b. Click [Change].
8. The New Job Schedule window is shown.
   a. For **Name**, enter a name for the schedule.
   b. Set the frequency for the backup to occur.
   c. Click [OK].
   d. Click [Next] in the Select Plan Properties window.
9. On the Select Maintenance Tasks window, select the **Back Up Database (Full)** check box. Click [Next].

10. On the Select Maintenance Task Order window, click [Next].
11. In the Define Back Up Database (Full) Task window, click the Databases drop-down.
12. In the Databases drop-down popup:
    a. Select the check box for the OnGuard database.
    b. Click [OK].
13. In the Define Back Up Database (Full) Task window:
    a. On the General tab, select the database you want to back up from the **Database(s)** drop-down menu.
    b. On the Destination tab, select the **Back up databases across one or more files** radio button.
    c. From the **If backup files exist** drop-down, select "Overwrite".
    d. Click [Add].
14. In the Select Backup Destination window, click [...].
15. In the Locate Database Files window:
    a. Enter a file location and name for the backup in the **File name** field.
    b. Click [OK] in the Select Backup Destination window.
    c. Click [Next] in the Define Back Up Database (Full) Task window.
16. On the Select Report Options window, click [Next].
17. On the Complete the Wizard window, click [Finish].
18. Once the Maintenance Plan Wizard Progress has completed, click [Close].
19. In the Administrative Tools section of Control Panel, open Services. Right-click the SQL Server Agent (MSSQLSERVER) service and select **Properties**.
20. The SQL Server Agent (MSSQLSERVER) Properties window is displayed.
    a. In the **Startup type** drop-down, select "Automatic."
    b. Click [OK].

One-Time Back Up to a File with SQL Server Express Edition

If you did not already have SQL Server Management Studio when OnGuard was installed, then you can install the Express Edition from the Supplemental Materials media. Once you have installed Express Edition, perform the following steps to create a one-time back up of the SQL Server database file.

Note: SQL Server Management Studio Express Edition provides limited functionality when compared to the full version of Management Studio. For example, Express Edition does not allow automatic database backups.

1. From Windows, open the SQL Server Management Studio.
2. Log into SQL Server Management Studio.
3. Expand the **Databases** folder in the Object Explorer.
4. Right-click on the OnGuard database and select ***Tasks > Back Up***.
5. On the **General** page of the **Back Up Database** window:
    a. In the **Backup type** field, select **Full**.
    b. Under **Backup component**, make sure **Database** is selected.
    c. In the **Name** field, enter a name for the backup set.
    d. In the **Description** field, enter a description for the backup set.

e. Under **Destination**, confirm that the path is as desired. If not, remove the default path and add a new path.

6. On the **Options** page of the **Back Up Database** window:
   a. Select **Back up to the existing backup set**, and then select **Overwrite all existing backup sets**.

Restoring Databases

To restore a SQL Server database from a file on either a network connection, CD, or DVD, restore the file to the database via the SQL Server Management Studio. For more information, refer to Restore Microsoft SQL Server Database from a File on page 20.

In addition to restoring the OnGuard access control database, include the following files to ensure that the database, report history, and custom reports for OnGuard Reporting and Dashboards can be properly restored on a new server:

- **AccessControl_ReportConfig**

  The naming convention for the ReportsConfig database is ***<Live OnGuard database name>*_ReportsConfig**. Since the default name of the Live OnGuard database is *AccessControl*, the default name of the ReportsConfig database is **AccessControl_ReportsConfig**. But if you manually changed the name of your Live OnGuard database to *AccCtrl*, for example, then your ReportsConfig database would be named **AccCtrl_ReportsConfig**.

- ***C:\Program Files\JReport\Server\history***
- ***C:\Program Files\JReport\Server\realm\defaultRealm***

By default, OnGuard Reporting and Dashboards is installed on the same machine that OnGuard and OpenAccess are installed on. To run OnGuard Reporting and Dashboards from a server other than the server already running OnGuard and OpenAccess, refer to Running OnGuard Reporting and Dashboards from an Alternate Server on page 115.

Restore Microsoft SQL Server Database from a File

1. From Windows, open SQL Server Management Studio.
2. The SQL Server Management Studio window is shown.
   a. Navigate to the OnGuard database.
   b. Right-click on the OnGuard database and select ***Tasks > Restore > Files and Filegroups***.
3. The Restore Files and Filegroups window is shown.
   a. In the **To database** drop-down, select the OnGuard database.
   b. In the **From database** drop-down, select the OnGuard database.
   c. If the **From database** is from another file, specify the file location in the **From device** drop-down, and select the desired backup set to restore.
   d. Click the Options page from the Select a page list view.
4. The Options page is shown.
   a. Select the **Overwrite the existing database** check box.
   b. Click [OK].
5. A success message is displayed. Click [OK].

Restore Microsoft SQL Server Database Onto a Different Server

Perform the following steps if you want to restore the Microsoft SQL Server Database onto a different OnGuard Server:

Note: If the new server is part of a cluster environment, you must failover to the second node in the cluster and then repeat steps 2 through 7 on that node.

1. Restore the database on the new server. For more information, refer to Restore Microsoft SQL Server Database from a File on page 20.
2. Synchronize the encryption key for the new server:
   a. In Task Manager, end the **Lenel OnGuard Login Server > LS Login Driver** process.
   b. Run the Login Driver as an application.
   c. Accept the error warning about the encryption key mismatch.
   d. In the Login Driver, select the **Edit > Manage Encryption Key** option.
   e. The ODBC dialog opens. Confirm the data source.
   f. Enter the password for the LENEL database login on the new server, then click [OK].
   g. Enter the encryption key for the new server, or load it from a file.
3. Run Setup Assistant, providing the login credentials from the restored database.
   a. In Setup Assistant, change the host for the LS Message Broker service to the new server.

Note: Setup Assistant can fail the Login Driver verification step because the LS Login Driver is not ready.

4. Run Setup Assistant, providing the login credentials from the restored database (ignore the OpenAccess warning).
5. In System Options, change the service's hosts to the new server.
6. (Optional) Change the LenelRabbitLD password on the new server:
   a. Open the **C:\Program Files\RabbitMQ Server\rabbitmq_server-<version>\sbin** folder.
   b. Open a **cmd** prompt for this folder location.
   c. Run the command: `rabbitmqctl change_password` **`LenelRabbitLD`** `<new_password>`
   d. View the Login Driver application again.
   e. Select the **Edit > Set RabbitMQ LD credentials** option.
   f. The ODBC dialog might open. Confirm the data source.
   g. Enter the password for the LENEL database login on the new server, then click [OK].
   h. The dialog for setting the RabbitMQ LD credentials opens. Enter the RabbitMQ LD password, then click [Apply].
   i. Restart the workstation.
7. Synchronize the LenelRabbit password:
   a. Open the **C:\Program Files\RabbitMQ Server\rabbitmq_server-<version>\sbin** folder.
   b. Open a **cmd** prompt for this folder location.
   c. Run the command: `rabbitmqctl change_password` **`LenelRabbit`** `<new_password>`
   d. Run System Administration (ignore the OpenAccess warning).
   e. In System Options, change the password for RabbitMQ to the new RabbitMQ password.
8. Run Setup Assistant, providing the login credentials from the restored database.

Restore OnGuard Reporting and Dashboards to an Alternate Server

Perform the following steps if you want to restore OnGuard Reporting and Dashboards to an alternate server (referred to as "Server 2" below) other than the server (host) named in the database backup:

1. On Server 1 that was in use when creating the backup, stop the LS Reporting service if it was not already stopped.
2. On Server 2:
   a. In System Administration, go to ***Administration > System Options > General System Options***. In the **Reports and Dashboards Server Host** field, browse to the location of the new server host, or enter its fully qualified domain name (FQDN).

      Make sure that it matches the OpenAccess Host location. If this is not the case, then refer to Running OnGuard Reporting and Dashboards from an Alternate Server on page 115.
   b. Run Setup Assistant.
   c. Confirm that the LS Reporting service starts as expected. If it does not start, restart Server 2, wait approximately five (5) minutes after the restart, and check the status of the LS Reporting service again.
3. To continue using any custom reports that existed on Server 1, copy the ***C:\Program Files\JReport\Server\history*** and ***C:\Program Files\JReport\Server\realm\defaultRealm*** directories and its contents from Server 1 to the same location on Server 2.

CHAPTER 4

Transfer a SQL Server Desktop Engine Database

You may wish to transfer a SQL Server Desktop Engine database for any number of reasons, although the most common reason is to upgrade to a new server.

Steps to Transfer a SQL Server Express Database

To transfer a SQL Server Desktop Engine database to a new server, complete the following procedures in the order listed:

- Back up the SQL Server Desktop Engine database. Refer to One-Time Back Up to a File with SQL Server Express Edition on page 19.
- Ensure Minimum Server Requirements are Met on page 23.
- Stop the SQL Server Service on page 23.
- Copy Files from the Old Server to the New Server on page 24.
- Restart the SQL Server Service on page 24.
- Attaching the AccessControl Database on page 24.
- Verify the Database Transfer was Successful on page 25.

Ensure Minimum Server Requirements are Met

Make sure that the new server meets the specifications that are listed in the current release notes. Although the server MUST meet the minimum specifications listed, your system will perform much better if the server also meets the recommended specifications.

Stop the SQL Server Service

Note: This procedure describes stopping the SQL Server service on a Windows machine.

The SQL Server (MSSQLSERVER) service must be stopped on both the old server and the new server before proceeding. To do this:

1. On the old server, click Start and then select ***Control Panel***.

2. Double-click **Administrative Tools**.
3. Double-click **Services**.
4. In the Services window, right-click on SQL Server (MSSQLSERVER) and select **Stop**.
5. Repeat steps 1–4 on the new server as well.

Copy Files from the Old Server to the New Server

Copy the **AccessControl.mdf** and **AccessControl_log.ldf** files on the old server to the new server, making sure to replace the files that might already exist on the new server. These files are located on the old server in **C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data**, and must be copied into the same location on the new server.

Restart the SQL Server Service

This procedure describes restarting the SQL Server service on a Windows machine.

1. On the new server, click Start and then select ***Control Panel***.
2. Double-click "Administrative Tools."
3. Double-click "Services."
4. In the Services window, right-click on SQL Server (MSSQLSERVER) and select **Start**.

Attaching the AccessControl Database

SQL Server Desktop Engine provides a user interface for accessing the database engine via the SQL Express Management Studio application. You can install the application from the Supplemental Materials media.

To attach the AccessControl database:

1. In the SQL Server Object Explorer pane, right-click on Databases.
2. Select Attach.
3. Click [Add].
4. Browse to the location of the AccessControl.mdf file, select the file, and then click [OK].
5. Click [OK] to close the Attach Databases window.

Change the Database Owner

Changing the database owner allows the lenel login to own the AccessControl database.

Note: You must already have a lenel login created. For more information, refer to Create a Login on page 33.

Change the Database Owner Using SQL Express Management Studio

1. In the Object Explorer pane of the SQL Server Management Studio, right-click on the AccessControl database and select **New Query**.
2. The Query tab is displayed.
   a. In the text window, type `sp_changedbowner lenel`
   b. Press <F5> to execute the command you typed.

c. The message “Command(s) completed successfully” is displayed in the Messages tab window.

3. Click the close (“X”) button to close the Query tab, then click [No] when prompted if you want to save the changes.

Verify the Database Transfer was Successful

Log into System Administration and verify that the database is indeed your old database.

CHAPTER 5

Microsoft SQL Server

Refer to the Compatibility Charts to determine which versions of SQL Server are compatible with OnGuard 8.3. Compatibility charts list currently supported OnGuard versions and components and are available on the LenelS2 Connect™ portal at: https://connect.lenels2.com/s/downloads.

To access OnGuard Compatibility Charts from the Web site:

1. Click the **Choose product or service** drop-down, select **OnGuard**.
2. Click the **Choose version** drop-down, select **OnGuard 8.3**.
3. Click the **Choose type of download** drop-down, select **Compatibility Charts**.

There are several editions of SQL Server; refer to the release notes for specific support information.

IMPORTANT: If you have SQL Server Express installed on your system, the database software will not be automatically upgraded during the OnGuard upgrade. If you want to upgrade your database software, instructions for upgrading to a supported version of SQL Server Express are provided in this chapter.

The following sections will show you how to install and upgrade SQL Server.

Prerequisites

The following prerequisites are required prior to installing SQL Server:

- Microsoft .NET Framework 4.8
- Microsoft Windows Installer 4.0 or later
- Microsoft Windows PowerShell

Note: Enable Windows PowerShell on supported operating systems.

SQL Server Express Edition

Notes: Some of the procedures in this chapter require the use of SQL Server Management Studio. Beginning with Supplemental Materials media revision 16, the SQL Server Management Tools are no longer included. SQL Server Management Tools for Microsoft SQL Server Express are included with Microsoft SQL Server Management Studio Express, and are available at www.microsoft.com. If using a full version of SQL Server, SQL Server Management Studio is included in the full version.

SQL Server Express installers are available on the Supplemental Materials media.

Installing or Upgrading SQL Server 2022 Express Edition

For information on installing SQL Server 2022 Express Edition, refer to https://learn.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server?view=sql-server-ver16.

For information on upgrading to SQL Server 2022 Express Edition, refer to https://learn.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-ver16.

Installing or Upgrading SQL Server 2019 Express Edition

For information on installing SQL Server 2019 Express Edition, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server?view=sql-server-ver15.

For information on upgrading to SQL Server 2019 Express Edition, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-ver15.

Installing or Upgrading SQL Server 2017 Express Edition

For information on installing SQL Server 2017 Express Edition, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/installation-for-sql-server?view=sql-server-2017.

For information on upgrading to SQL Server 2017 Express Edition, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-2017.

Installing SQL Server Management Tools

SQL Server Management Studio is required if the server intends to use Database Authentication or Windows single sign-on. The SQL Server Management Studio is available at www.microsoft.com.

Note: If using a full version of SQL Server, SQL Server Management Studio is already installed and should be used instead.

SQL Server Standard Edition

The instructions that follow are for the Standard edition. The installation and upgrade steps for SQL Server are very similar. Special considerations for upgrades are noted in the appropriate steps. When performing an upgrade, there should be nothing connected, that is: no clients logged on. There can be

no software connections to the database when the upgrade is performed, so all OnGuard LS and LPS services including the LS Communication Server must be stopped.

Note: Before upgrading SQL Server, be sure to back up your database.

Installation Steps

To perform the installation, complete the following steps:

1. Installing or Upgrading SQL Server 2019 on page 29.
2. Configuring SQL Server on page 31.
   a. Create the Database on page 31.
   b. Create a Login on page 33.
   c. Set Memory Usage on page 34.
   d. Truncate the Log File on page 34.
   e. Determine the Database Archive Plan on page 34.

Upgrade Steps

- SQL Server on page 29.
- Set Memory Usage on page 34.

SQL Server

Installing or Upgrading SQL Server 2022

For information on installing SQL Server 2022, refer to https://learn.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server?view=sql-server-ver16.

For information on upgrading to SQL Server 2022, refer to https://learn.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-ver16.

Installing or Upgrading SQL Server 2019

For information on installing SQL Server 2019, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server?view=sql-server-ver15.

For information on upgrading to SQL Server 2019, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-ver15.

Installing or Upgrading SQL Server 2017

For information on installing SQL Server 2017, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/installation-for-sql-server?view=sql-server-2017.

For information on upgrading to SQL Server 2017, refer to https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-2017.

Installing or Upgrading SQL Server 2016

Note: Before installing or upgrading SQL Server 2016, refer to Prerequisites on page 27. If you do not have these prerequisites prior to installing or upgrading SQL Server, the setup will prompt you before installing them.

1. Insert the SQL Server disc.

   If the SQL Server Installation Center does not automatically appear, open the Windows Run dialog and browse for **setup.exe** on the disc drive. Alternatively, you can run **setup.exe** from Windows Explorer.
2. The SQL Server Installation Center is shown. Click **Installation** from the left pane, then:
   - For new installations, click **New SQL Server stand-alone installation or add features to an existing installation**.
   - For upgrades, click **Upgrade from SQL Server**.
3. The Product Key window is shown. Enter your product key and click [Next].
4. In the License Terms window:
   a. If you agree with the license terms, select **I accept the license terms**.
   b. Click [Next].
5. The Microsoft Update window is shown. Select **Use Microsoft Update to check for updates (recommended)**, and then click [Next].
6. The Install Setup Files window is displayed. If an error is shown, click [Next]. If no error is shown, the installation will proceed to the next step automatically.
7. After the setup files have been installed in the Install Setup Files window, the Install Rules/ Upgrade Rules runs again to identify potential issues. You must resolve any failures before setup can continue. Once the check completes successfully, click [Next].
8. New installations only: The Setup Role step installs the SQL Server Feature configuration. Select **SQL Server Feature Installation**, and then click [Next].
9. Upgrade only: In the Select Instance window, select the **Instance to upgrade** from the drop-down and click [Next].
10. In the Select Features window, under Instance Features, select **Database Engine Services** and **Full-Text and Semantic Extractions for Search**. Then click [Next].

    Notes: For upgrades, these features may already be selected and it might not be possible to change the selections.

    In earlier SQL Server versions, you could install SQL Server Management Studio as part this installation process. The SQL Server 2016 installation does not include SQL Server Management Studio. Download and install SQL Server Management Studio separately from this installation procedure.
11. New installations only: In the Feature Rules window, click [Next] if an error is shown. If no error is shown, the installation will proceed to the next step automatically.
12. In the Instance Configuration window:
    - For new installations, select **Default instance**, and then click [Next].
    - For upgrades, the **Named instance** should already be selected. Click [Next].
13. The Server Configuration window is displayed.
    - For new installations:
      1) On the SQL Server Agent, click the drop-down menu under Account Name for the SQL Server Agent service.

2) Select Browse.
3) Click [Advanced].
4) Click [Find Now].
5) Select SYSTEM from the search results.
6) Click [OK].
7) On the SQL Server Agent, SYSTEM appears in the Object Name field. Click [OK]. You will see “NT AUTHORITY\SYSTEM” under Account Name.
8) Repeat these steps for the SQL Server Database Engine service.
9) Click [Next].

- For upgrades, click [Next].

14. New installation only: In the Database Engine Configuration window:
    a. Select the **Mixed Mode** radio button.
    b. Enter and confirm a password for the SQL Server system administrator account.
    c. Click [Add].
    d. In the Select Users or Groups window, click [Advanced].
    e. Change the **From this location** field to the local machine by clicking [Locations] and selecting the local machine from the list.
    f. Click [Find Now], then select Administrators from the Search results listing window.
    g. Click [OK], then click [OK] again to close the Select Users or Groups window.
    h. The BUILTIN\Administrators group should now appear in the Specify SQL Server administrators listing window. Click [Next].
15. Upgrade only: In the Full-text Upgrade window, select **Import**, and then click [Next].
16. In the Feature Configuration Rules/Feature Rules window, if any rules do no show a status of Passed, correct the issue and then click [Re-run]. Once all rules pass, click [Next].
17. In the Ready to Install or Ready to Upgrade window, click [Install] or [Upgrade] to begin the installation.
18. In the Complete window, click [Close].
19. Close the SQL Server Installation Center.
20. Reboot the computer, even if you are not prompted to do so. This completes the installation of SQL Server. You can now configure SQL Server. For more information, refer to Configuring SQL Server on page 31.

Configuring SQL Server

Create the Database

Notes: Unless otherwise indicated, the selections made during database creation are minimal options necessary for the operation of the OnGuard database. Your IT department might require that these selections are increased, but it is recommended they not be reduced.

In particular, the SQL Server selection for Recovery Model should be selected based on the expectation of data recovery in the event of database failure:

Recovery Model Simple - The database can be restored to the point of the last backup. This provides simple but effective protection.

Recovery Model Full - The database can be restored to last transaction prior to the failure. This requires more management, but also provides better protection than the Simple Recovery Model.

1. In Windows, open the ***SQL Server Management Studio***.
2. Select your method of authentication, provide credentials if required, and click [Connect].

Note: If using SQL authentication, use SA.

3. In the Object Explorer pane, expand the Databases folder. Right-click the Databases folder and select **New Database**.
4. The New Database window is displayed. On the General page:
   a. In the **Database name** field, type `ACCESSCONTROL` (this is case-insensitive).
   b. Set the Initial Size (MB) of the Data file to 50.
   c. Set the Initial Size (MB) of the Log file to 10.
   d. Scroll to the right in the Database files listing window and click the browse button in the Autogrowth/Maxsize column of the log file row.
   e. Under **Maximum File Size**, select the **Unlimited** radio button.
   f. Click [OK].
5. Select the Options page from the **Select a page** pane.
   a. In the **Recovery model** drop-down, select “Simple”.
   b. Verify that the **Compatibility level** drop-down is set to the proper compatibility level for your SQL Server version.
   c. In the **Other options** list view, set the **Auto Create Statistics**, **Auto Shrink**, **Auto Update Statistics**, and **Recursive Triggers Enabled** drop-downs to “True”.

Notes: Starting with OnGuard 8.1, the ACCESSCONTROL database’s encryption has changed. Because of this, you must not disable ANSI padding when running a SQL script by executing the **SET ANSI_PADDING OFF** SQL statement. To check your database for columns with ANSI padding set to OFF, run the following SQL script:

```
select t.name,c.name,c.is_ansi_padded from sys.columns c
join sys.tables AS t on t.object_id=c.object_id
where c.system_type_id = 165 and c.is_ansi_padded = 0
```

Switching ANSI padding from OFF to ON will not impact existing columns. To fix a database column with ANSI padding set to OFF, run the following SQL script (where **table_to_fix** is the name of the database table containing the column with ANSI padding set to OFF, and **column_to_fix** is the affected column in the table):

```
set ansi_padding on;
go
alter table table_to_fix alter column column_to_fix
varbinary(80);
```

```
go
```

In this example, **varbinary(80)** is the SQL type of the database column; you should use your column's actual SQL type.

d. Click [OK].

Create a Login

1. In the Object Explorer pane of the SQL Server Management Studio, expand the Security folder.
2. Right-click the Logins folder and select **New Login**.
3. In the General page of the Login window:
   a. In the **Login** name field, type `LENEL`.

Note: By default, the login name for the OnGuard database is "Lenel." This can now be customized as needed. If this name is changed, make sure to update or set up a corresponding user account in your database.

   b. Select the **SQL Server authentication** radio button.
      - For **Password**, type `Secur1ty#` (default password).
      - Retype the password in the text field to confirm it.

Note: The SQL Server password is case-sensitive.

   c. Deselect the **Enforce password policy, Enforce password expiration**, and **User must change password at next login** check boxes.

Note: If you choose to select the **Enforce password expiration** check box, you will be required by SQL Server to select a new login password at regular intervals. When the login password is changed by SQL Server, it must also be updated with the Login Driver. Failure to update the Login driver will cause OnGuard not to function properly.

4. In the Server Roles page of the Login window:
   - Most users should select the **dbcreator**, **public**, **serveradmin,** and **sysadmin** check boxes.
   - Advanced users should only select the **public** check box.
5. In the User Mapping page of the Login window:
   a. Select the master and tempdb check boxes.
   b. Click [OK].
6. Recommended settings for **lenel** account user:

Note: For advanced users who do not want the database owned by **lenel**, proceed to step 7.

   a. In the Object Explorer pane of SQL Server Management Studio, right-click on the OnGuard database and select **New Query**. A query tab is shown.
   b. In the text window, type `sp_changedbowner lenel`.
   c. Press <F5> to execute the command.
   d. The message **Command(s) completed successfully** is shown in the Messages tab.
   e. Click the close ("X") button to close the query tab, then click [No] when prompted if you want to save the changes.
   f. Proceed to Set Memory Usage on page 34.
7. For advanced users, the minimum required **lenel** user account settings are:

a. In the Object Explorer pane of SQL Server Management Studio, right-click on the OnGuard database you just created and select **New Query**. A query tab is shown.
b. In the text window, type:
   - `CREATE ROLE db_executor`
   - `GRANT EXECUTE TO db_executor`
c. Press <F5> to execute the command.
d. The message **Command(s) completed successfully** is displayed in the Messages tab.
e. Click the close ("X") button to close the query tab, then click [No] when prompted if you want to save the changes.
f. Select the **Login - New** dialog, which should already be open but might be hidden by another window.
g. Select **User Mapping** from the **Select a page** pane, and then select the `ACCESSCONTROL` database.
h. Select (check) the following roles:
   - public
   - db_datareader
   - db_datawriter
   - db_ddladmin
   - db_executor
i. Click [OK].
j. The new login appears in the **Logins** folder.

Note: At this point the **lenel** user account provides OnGuard functionality only. Any database level administration, such as backups and restores, must be performed by a different user with the appropriate permissions.

Set Memory Usage

1. In the Object Explorer pane of the SQL Server Management Studio, right-click on the database engine *<ServerName>* and select **Properties**.
2. Select the **Memory** option on the Select a page pane.
3. Set the **Maximum server memory (in MB)** option to be roughly one half of your system's actual memory. This will make sure that the database does not use your entire system's memory, which would needlessly slow down your system.
4. Click [OK].

Truncate the Log File

1. In the Object Explorer pane of the SQL Server Management Studio, right-click the OnGuard database, then select ***Tasks*** > ***Shrink*** > ***Files.***
2. The Shrink File window is displayed.
   a. In the **File type** drop-down, select "Log".
   b. Select the **Release unused space** radio button.
   c. Click [OK].

Determine the Database Archive Plan

In addition to creating the required Live database, OnGuard provides two options for archiving Events, Events Video Location, Alarm acknowledgments, User Transactions, Visits Records, and

specific event types from the Live database tables, as a way of keeping the database from growing so large over time that system performance is affected.

- Archive to text files
- Archive to an Archival database

If you plan to archive the Live database to an Archival database, then create the Archival database by performing the following steps.

Note: By default, OnGuard replicates all data that can be archived to the Global Server. For this reason, you might wish to Archive to database on the Global Server only.

1. Perform all of the previous steps to create the Live database.
2. Repeat the Create the Database on page 31 steps again to create the Archival database, changing the Database name to ACCESSCONTROL_ARCHIVAL.
3. Repeat step 1 from the Create a Login on page 33 procedure again.
4. Double-click on the existing **lenel** user account.
5. Select the User Mapping page.
6. Repeat steps 6a through 6e, or steps 7a through 7i, from the Create a Login on page 33 procedure again, depending on how you configured the Live database. The Archival database is now ready for use.

For detailed information about the Live and Archival databases, refer to the *Archives Folder* chapter in the *System Administration User Guide*.

Create ReportsConfig Database for OnGuard Reporting

Setup Assistant creates the ReportsConfig database automatically. For more information, refer to OnGuard Reports & Dashboards Database on page 49.

Notes: You must run Setup Assistant whenever you use **Configuration Editor** or **ODBC Data Source Administrator (32-bit)** to change database parameters, or whenever you change database parameters in the **application.config** or **ACS.ini** files. Setup Assistant will then modify the JReport configuration files (for example, **C:\Program Files\JReport\Server\bin\dbconfig.xml** and **C:\ProgramData\Lnl\reports.cat.xml**) on the reports host workstation to reflect your database parameter changes.

The naming convention for the ReportsConfig database is ***<Live OnGuard database name>*_ReportsConfig**. Since the default name of the Live OnGuard database is *AccessControl*, the default name of the ReportsConfig database is **AccessControl_ReportsConfig**. But if you manually changed the name of your Live OnGuard database to *AccCtrl*, for example, then your ReportsConfig database must be named **AccCtrl_ReportsConfig**.

If you want to configure the reports function in OnGuard manually, you must first create a separate database to support that function:

1. Create a new SQL database named **AccessControl_ReportsConfig**. Follow the process described in Create the Database on page 31 to create this database.
2. Assign a Windows authenticated user as described in Add the Windows user to SQL Server on page 65.

Note: Configure the User Mapping section as described in step 6, applying those selections to the new **AccessControl_ReportsConfig** database.

Configure SQL Server for OnGuard Reporting

To configure SQL Server to support OnGuard Reporting:

1. Open the **SQL Server Configuration Manager**.
2. Select **SQL Server Network Configuration > Protocols for MSSQLSERVER**.
3. Change the status of the **TCP/IP** protocol to **Enabled**.

Using Azure SQL Databases with OnGuard

Overview

Describe the concept of how OnGuard is used with Azure SQL, and highlight the considerations.

Considerations for using Azure SQL with OnGuard

Cost and sizing

For more information about the costs and sizing of using an Azure SQL database when configuring an OnGuard installation, refer to the *OnGuard Deployment Guide*, which can be downloaded from the LenelS2 Connect™ portal at: https://connect.lenels2.com/s/downloads.

Local and regional redundancy

Local and regional redundancy are important considerations when using Azure SQL to ensure high data availability and protection.

- **Local redundancy:** Local redundancy can be achieved by using Azure SQL's *automatic backups* and *point-in-time restore* features. These features ensure that you can restore data to a previous state if there is accidental data deletion or corruption. You can use options that do not change the operation of the database from OnGuard's point of view. You should consider performance changes that might be caused by the selected options, and follow the Azure SQL guidance on how these affect database usage.
- **Regional redundancy:** Regional redundancy can be achieved by using Azure SQL's *geo-replication* feature. This feature creates a secondary copy of the database in a different region, providing redundancy in the event of a regional outage.
- **High availability:** High database availability can be achieved by using Azure SQL's *failover groups* feature. This feature allows for automatic fail-over to a secondary database in the event of a primary database outage. You should evaluate cost and performance on a system-by-system basis, as these are a specific function of Azure SQL and the selected options.

Networking with Azure SQL

You should consider the network environment when using Azure SQL with OnGuard. The network environment should be decided by the end-user's IT department along with the system integrator. As with any OnGuard environment, connectivity of the systems, services, and clients must be available and maintained. Virtual Private Cloud, site-to-site VPN, and virtual networks might be required. LenelS2 does not provide IT services in support of this configuration.

References

Additional information from Microsoft:

- Provision an Azure SQL database to store application data
- Quickstart: Create a single database - Azure SQL Database

Prerequisites

- Using an Azure SQL database assumes that you know how to get to Azure SQL, an d have the ability to set up and configure a database in that platform
- You have an Azure SQL account
- Content from KB: Installing OnGuard on SQL Azure

Create the Azure SQL Server and Databases

Perform the following steps to create an Azure SQL server and the databases required to support OnGuard.

Create SQL Database - Basics

Perform the following steps to configure the basics for your Azure SQL server and databases:

Notes: The databases *must* be in the same region as OnGuard for expected performance.

You will use the same resource group for both the Azure SQL database and for the OnGuard server.

1. Log into your Microsoft Azure account.
2. Under **Azure services**, click **SQL databases** > **Create**. The **Create SQL Database - Basics** page opens.
3. In the **Subscription** drop-down, select your existing subscription.
4. Beneath the **Resource group** drop-down, click **Create new**.
5. Give the new resource group a **Name**, then click [OK].
6. In the **Database name** field, type `AccessControl`.
7. Beneath the **Server** drop-down, click **Create new**.
8. On the **Create SQL Database Server** page, type a name in the **Server name** field.
9. In the **Location** drop-down, select the same geographic location you will choose for your OnGuard server.
10. For **Authentication method**, select **Use both SQL and Azure AD authentication**.
11. Beneath **Set Azure AD admin**, click **Set admin**.
12. In the **Azure Active Directory** side panel, select your Azure Active Directory admin, then click [Select].
13. In the **Server admin login** field, type `SA`.
14. In the **Password** and **Confirm password** fields, type the administrator's password.
15. Click [OK].
16. For the **Want to use SQL elastic pool?** radio buttons, select either **Yes** or **No**.

Note: An elastic pool can help you better manage your workload so that the Azure SQL database can adapt automatically to peak and non-peak usage within your OnGuard system.

17. For the **Workload environment** radio buttons, select **Production** for a live OnGuard system. If you're creating an OnGuard system for testing purposes, select **Development**.

Note: You can select **Development** when you're initially configuring and testing your OnGuard system, then change it to **Production** when you're ready to use the system for actual business.

18. If you selected **Yes** for using an elastic pool, click **Create new** beneath **Elastic pool**, type the name of your elastic pool in the field, then click [OK].
19. If you selected **Yes** for using an elastic pool, beneath **Compute + storage**, click **Configure elastic pool**.
20. On the **Configure** page, in the **Service tier** drop-down, select **General Purpose (Scalable compute and storage options)**.
21. Beneath **Hardware Configuration**, click **Change configuration**, then select the configuration required to support your system usage. LenelS2 recommends **Standard-series (Gen5)**. Click [OK].
22. For the **Save money** radio buttons, select **Yes** if you want to use the Azure hybrid model. Otherwise, select **No**.

Note: Your choice of Azure SQL Licensing does not affect your OnGuard installation. Licensing is the responsibility of the end-user.

23. Use the slider to select the number of **vCores** (virtual cores) your system requires.
24. Use the slider to select the **Data max size (GB)** your system requires.
25. Under **Zone Redundancy**, select **Yes** if you want your OnGuard data to be replicated across multiple zones within the same region, and then make the appropriate configuration choices. Otherwise, select **No**.
26. Click [Apply].
27. Choose one of the **Backup storage redundancy** options.
    - Select **Locally-redundant backup storage** if you want your OnGuard data to be backed up on the same server as your active database's region.
    - Select **Zone-redundant backup storage** if you want your OnGuard data to be backed up in the same region as your active database's region.
    - Select **Geo-redundant backup storage** if you want your OnGuard data to be backed up in a different region than your active database's region.
28. Click [Next: Networking]. The **Create SQL Database - Networking** page opens.

Create SQL Database - Networking

Make choices in this section to establish network connectivity to your Azure SQL database according to your own requirements, and to ensure connectivity with your OnGuard environment.

Create SQL Database - Security

Make choices in this section to secure your Azure SQL database according to your own requirements. OnGuard does not require any of these security settings to perform normally. Either accept all of the defaults, or make your own configuration:

1. Under **Microsoft Defender for SQL**, select **Not now**.

2. Under **Ledger**, leave the configuration set to **Not configured**.
3. Under **Identity**, leave the configuration set to **Not configured**.
4. Under **Transparent data encryption**, leave the configuration set to **Service-managed key selected**.

Note: For more information about service-managed keys and customer-managed keys, refer to "Transparent Data Encryption" in the *Advanced Installation Guide*, or refer to the Microsoft article http://msdn.microsoft.com/en-us/library/bb934049.aspx.

5. Click [Next: Additional settings]. The **Create SQL Database - Additional settings** page opens.

Create SQL Database - Additional settings

Perform these steps to customize additional configuration parameters for your Azure SQL server:

1. Under **Data source**, select **None**.
2. Under **Database collation**, leave the default **SQL_Latin1_General_CP1_CI_AS**.
3. Under **Maintenance window**, leave the default **System default (5pm to 8am)**.
4. Click [Next: Tags]. The **Create SQL Database - Tags** page opens.

Create SQL Database - Tags

Perform these steps to configure how you categorize and view billing information for your Azure SQL server:

Note: OnGuard has no specific requirements for tagging, but the option is available to help you organize your installation.

1. Under **Name**, type a name into the field (for example, `Owner`).
2. Under **Value**, type a value into the field (for example, the name of the person in your Billing department responsible for the cost of your Azure SQL server).
3. Under **Resource**, use the drop-down to select the appropriate resources (for example, select the SQL Azure resources for which the named Owner will pay).
4. If you want more categories for billing and reporting purposes, create addition name/value pairs.
5. Click [Next: Review + create]. The **Create SQL Database - Review + create** page opens.

Create SQL Database - Review + create

Perform these steps to review and create your Azure SQL server:

1. Review the summary of your Azure SQL server and database.
2. If you want to modify a configuration, click [Previous] and make the necessary changes. Then return to this page.
3. Click [Create].

Note: Deploying the new server and database will take several minutes.

Create OnGuard Reports and Dashboards Database

Repeat the steps above to create the OnGuard Reports and Dashboards database.

Create Archiving Database

Repeat the steps above to create the archiving database.

Adding Clients

- Based on the network by the VAR - see above networking
- In this section, the VAR/IT must be able to provide for access to the Azure SQL database server for their OnGuard clients
- Potential list of 'clients' for OnGuard
  - OnGuard server
  - All service
  - All installed clients
  - OpenAccess
  - ODBC connectivity

Migrating an Existing OnGuard Database to SQL Azure

Microsoft provides several option to migrate an existing SQL database into an Azure SQL database. It is not possible to use your existing MDF files when migrating an existing OnGuard SQL database into Azure SQL.

Options for migrating an existing database into Azure SQL include:

- Export the database to SQL scripts, and then run the scripts in Azure SQL
- Export the database using Microsoft SQL Management Studio's built-in **Deploy Database to Windows Azure SQL Database** option.
- Export the database using Microsoft Data Migration Assistant.

For more information, refer to:
https://learn.microsoft.com/en-us/azure/azure-sql/migration-guides/database/sql-server-to-sql-database-guide?view=azuresql

CHAPTER 6

Installing OnGuard 8.3

This chapter describes the prerequisites and procedure for installing OnGuard 8.3.

OnGuard 8.3 Installation Prerequisites

Before you install OnGuard you must first install the third-party requirements from the OnGuard Supplemental Materials media. Windows Service Packs are also required but are not provided on the Supplemental Materials media. See the OnGuard release notes on the Installation media to see which service packs are required for your operating system.

1. Insert the OnGuard Supplemental Materials media into a computer running the Windows operating system.
2. Install Adobe Reader, which is required to read the OnGuard help documentation.

Note: Microsoft .NET Framework is installed automatically during the OnGuard installation.

3. Install your database system.
4. Restart your computer.

Notes: Any workstation that will be configured as a LenelS2 NVR 7.5 video client must have specific Windows features enabled for 360-degree camera support, depending on the workstation's operating system. If running Windows Server, enable **Media Foundation**.

Components of the OnGuard system require that Secure Socket Layer (SSL) is enabled, which is done by default using self-signed certificates that are created during installation. For more information on how to manage these certificates or to replace them, refer to refer to Appendix D: OnGuard and the Use of Certificates on page 105.

Installation Procedures

Attach the Hardware Key (License Server Only)

Note: If you are using a software license you do not need to configure a hardware key. For more information, refer to *Install Your OnGuard License* in the *Installation Guide*.

OnGuard software is protected by a hardware security key. USB hardware keys are available for use with the OnGuard software. Remember to physically attach the hardware key ("dongle" adapter) directly to the USB port on the computer that has License Server installed in order for the software to run properly.

A hardware key is only needed on the server running License Server. Each client computer running OnGuard 8.3 uses a software license instead of a hardware key.

Note: Parallel dongles are no longer supported. If you are using a parallel dongle, contact LenelS2 OnGuard Technical Support for a replacement USB dongle before installing the OnGuard software.

Configure a USB Hardware Key

If you are using a hardware key that attaches to the USB port, then you must install a driver in order for Windows to recognize the device.

IMPORTANT: You must install the driver for the hardware key BEFORE attaching the USB hardware key to the computer.

To configure a USB hardware key:

1. Install the SafeNet USB hardware key driver by doing the following:
   a. Navigate to the **SafeNet** directory on the Supplemental Materials media and then double-click the .exe file. This can be found by navigating through the following folders on the Supplemental Materials media: **/License Key Drivers/SafeNet**.
   b. The InstallShield Wizard starts. Click [Next].
   c. The wizard continues, and the License Agreement window opens. Select the **I accept the terms in the license agreement** radio button, and then click [Next].
   d. The wizard continues, and the Setup Type window opens. Select the **Custom** radio button, and then click [Next].
   e. The Custom Setup window opens. Make sure only the Parallel Driver and the USB System Driver get installed. You do not need to install any of the Sentinel Servers or Sentinel Security Runtime. Click on Sentinel Protection Server, Sentinel Keys Server, and Sentinel Security Runtime and select, "This feature will not be available." [Click Next].
   f. Click [Install].
   g. The wizard completes. Click [Finish] to exit.
2. Install the USB hardware key by doing the following:
   a. Attach the USB hardware key to any available USB port.
   b. The Found New Hardware wizard starts. Click [Next].
   c. The hardware is detected, and the Found New Hardware wizard completes. Click [Finish]. The hardware key is now configured and ready to be used.

3. Depending on your configuration, you may need to restart your computer so that License Administration recognizes the hardware key. Otherwise, you may receive an error in License Administration saying that the necessary hardware device was not found.

You are now ready to install the OnGuard software and license.

Install the OnGuard 8.3 Software

Note: When planning your OnGuard installation, make sure all OnGuard components installed in your environment are compatible with each other. Check the compatibility charts to confirm what component versions are necessary to support the installed version of the OnGuard software. Not using compatible components might cause unexpected system behavior. Compatibility charts are available on the LenelS2 Connect™ portal at: https://connect.lenels2.com/s/downloads.

Note: When performing a **Custom Install** of a client, and selecting the "DataConduIT" option, the installation may be successful but the DataConduIT service will not start, giving a WMI error. This occurs because the DataConduIT service is dependent on the same WMI Wrapper that is used by Open Access. (Not selecting the "Open Access" option causes the WMI error.) **To resolve:** Select both options "Open Access" and "DataConduIT" when performing a custom install of DataConduIT.

1. Insert the OnGuard 8.3 installation media into a USB port on a computer running the Windows operating system.
2. If the computer allows the OnGuard installer to run automatically, then the installer runs. Otherwise, double-click the **setup.exe** file.
3. The Microsoft .NET Framework 4.8 installation wizard begins. Click [Install] to begin installation. Microsoft .NET Framework 4.8 must be installed for some OnGuard features to work correctly.
4. When prompted, read the license agreement. If you agree to its terms:
   a. Select the **I accept the terms in the license agreement** radio button.
   b. Click [Next].
5. For Server System installations/upgrades only: Select the Preferred OnGuard System type you want to install:
   - Enterprise
   - Standard

   Select *Standard*, and then click [Next].
6. Next, you will be prompted to choose the system configuration you want to install:
   - Server System
   - Client System
   - Monitoring Client
   - Badging and Credential Client

Note: The **Server System** option will be disabled if you are installing a **Client System** from **OGClient.iso** introduced in OnGuard 8.2 Update 1.

7. If you selected **Server System** or **Client System**, you are given the option to **Add Milestone Support**. Select the checkbox if your OnGuard system includes Milestone XProtect recorders. Then click [Next].

8. Depending on your System Configuration choice, you will have different system options to select:
   - If you selected **Server System**, configure the following options:
     - Select either **Platform Server** or **Custom Server**.

       Platform Server: Use the Platform Server option if this will be a complete server that will install all server features.

       Custom Install: Use the **Custom Install** option if this server will only host certain server features. If you choose the Custom Install option, you must select the individual features that you want installed on this server.
     - Select the appropriate database option for your installation.
   - If you selected **Client System**, configure the following options:
     - Select either **Typical System** which includes the standard features of the system, or a **Custom System** where you can specify server locations and choose the features to install.
     - Select the appropriate database option for your installation.
   - If you selected **Monitoring Client**, configure the database type information options.
   - If you selected **Badging and Credential Client**, configure the database type information options.
9. Click [Next].
10. The System Location Information window is shown.
    - Either accept the default installation directory or click [Change] and specify a different destination folder.
    - Accept the default location of the License Server or click [Browse] and specify a different location.
    - In the **Port** field, enter the number of the port to be used for access control system communication. It is recommended that you accept the default value of 8189.
    - In the **Provide the database login user** field, enter the name of the name of the database login user.

    Notes: If you want to use a different port than the default port 8189, use the Configuration Editor to make this change. For more information, refer to Appendix A: Configuration Editor on page 91.

    By default, the login name for the OnGuard database is “Lenel.” This can now be customized as needed. If this name is changed, make sure to update or set up a corresponding user account in your database.

    - In the **Provide the location of your database** field, accept the default location or click [Browse] and specify a different location.
    - Click [Next].
11. If you selected **Custom Install** in step 7, the Custom Setup window is shown. Select the access control system features you wish to have installed.

    Notes: Click the name of a feature on the left to display its description on the right.

    Below the Feature Description, the disk space requirements of the selected feature are displayed.

    a. Click the icon to the left of a feature to display a popup menu of installation choices for that feature.

b. Click [Next].

12. Click [Install] to begin the installation.
13. After Windows configures OnGuard, the status and progress bar are updated.
14. Once the installation is complete, click [Finish].
15. Depending on the components that you chose to install, you might need to reboot the computer. If you are prompted to do so, reboot the computer.
16. Setup Assistant launches automatically.

Setup Assistant

To simplify OnGuard installations and upgrades, Setup Assistant helps users with the configuration steps required before successfully logging into the OnGuard software. Setup Assistant launches automatically after the OnGuard installer finishes the installation or upgrade process.

Notes: After the OnGuard installation or upgrade is complete, launch Setup Assistant.

Users must be logged into the workstation with Administrator rights to run Setup Assistant. Users not logged in with Administrator rights are shown a dialog asking them to enter an Administrator password.

The Setup Assistant dialog consists of three primary sections:

- The status pane on the left side of the window lists the tasks performed by the Setup Assistant.
  - A green check indicates that the task was performed successfully.
  - A yellow check indicates that the user either chose to skip the task, or there was a warning that prevented the task from completing. Some Setup Assistant tasks can be skipped by the user, and then run manually at a later time.
  - A red “X” indicates that the task failed, and that errors must be corrected before using the system.
  - A blue arrow indicates that the task is running.
  - No icon indicates that the task has not run yet.
- The main pane provides additional data, status, fields, buttons, and so on related to the active task.
- The description pane provides a brief description of each task’s purpose.

Security Utility

Security Utility functionality is now embedded into Setup Assistant. You should run Security Utility again whenever a Windows Update or Service Pack is installed on the workstation. For more information, refer to Manually Running Security Utility on page 50.

IMPORTANT: OnGuard 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.

Configuration Editor

Configuration Editor functionality is now embedded into Setup Assistant. The Configuration Editor screen shows the current configuration of the:

- Database
- License Server

If there is a configuration issue with any of these items, the Configuration Editor highlights the issue, making it easy to correct the issue. There are three situations in which the Configuration Editor will identify an issue that must be resolved:

- The database and license configuration is not consistent between the **application.config** and **ACS.INI** files
- Setup Assistant cannot locate the database
- Setup Assistant cannot locate the License Server

If you want to store an encrypted database password in the **application.config** file during the OnGuard installation, you can make that configuration during this Setup Assistant step. For more information, refer to refer to Appendix A: Configuration Editor on page 91.

Client Support in Configuration Editor (using Client Connect)

Another function of Configuration Editor in Setup Assistant on a client workstation is to configure the workstation with all information required for connecting to the LS Login Driver through the LS Message Broker service. During the Configuration Editor step in Setup Assistant, you are given two options to configure the client:

- Provide the database configuration details, which allows Setup Assistant to fetch the required information directly
- Provide a Client Connect file, which securely stores the required information.

Client Connect

Use the Client Connect file to distribute LS Login Driver connectivity details to client workstations, eliminating the need for installation personnel to have direct database access during the Setup Assistant process. The system administrator can prepare the encrypted file in advance, and then distribute it with the OnGuard installation ISO file to provide an alternative method of configuring the client workstations.

There are multiple ways to create a Client Connect file:

- Using the Client Connect form located on the **System Administration > System Options** form. For more details, refer to “Client Connect Form” in the *System Administration User Guide*.
- Using the Client Connect Tool. For more information, refer to “Using Client Connect Tool to Create Configuration File” in the *Advanced Installation Topics Guide*.

There are multiple ways to provide the Client Connect file to Setup Assistant:

- Manually in the Configuration Editor step of Setup Assistant. Select the “Client Connect configuration file” as the preferred configuration option for your client and point to the file path.
- Automatically, by placing the file in the default path **C:\ProgramData\Lnl\clientConnect.ogcc**. Setup Assistant will automatically fetch the file and then continue to the next Setup Assistant step.
- During unattended installations. Use the **ClientConnectFilePath** parameter to specify a location for the file.

Note: You can also deploy the Client Connect configuration file to the workstation without using Setup Assistant, by using the Client Connect Tool import option. For more information, refer to “Using Client Connect Tool to Create Configuration File” in the *Advanced Installation Topics Guide*.

System License

System License (License Administration) is used to install a valid license, or to verify that a valid license is already installed. This functionality is now embedded into Setup Assistant.

Note: You must have a valid license before Setup Assistant will continue with the OnGuard configuration process. If License Administration finds a valid license, Setup Assistant passes the System License step automatically. If License Administration does not find a valid license, it prompts you to locate a valid license file.

Run License Administration manually whenever you purchase additional licensable OnGuard features and receive a new license from the factory.

- For information on how to run License Administration manually, refer to Log into License Administration on page 51.
- For information on how to install a new license, refer to Install a New License on page 52.

Service Log On

Enter the Windows user name and password of the account that will run the OnGuard software. This Windows user must have database access, and also have read/write access to the OnGuard directory for writing to the log files.

Database Installation

For new OnGuard server installations using SQL Express, Setup Assistant provides an easy method for installing a new ACCESSCONTROL database for the OnGuard software.

1. If you do not want to use the default source database (.MDF) file, click the first [Browse] button and navigate to the alternate source file.
2. If you do not want the database stored at the default path, click the second [Browse] button and navigate to the alternate database location.
3. Click [Install database].

Database Installation (Archival)

If the system is configured to archive to a SQL or SQL Express database, then Setup Assistant gives you the option of backing up the new ACCESSCONTROL database in addition to the Live database. For more information on the fields and buttons shown on this Setup Assistant form, refer to Database Backup on page 47.

Database Backup

If updating an existing OnGuard installation, Setup Assistant provides an easy method for backing up a SQL Server or SQL Server Express database before it is upgraded during Database Setup. It is *strongly* recommended that you make a database backup, although you can skip this step if desired.

IMPORTANT: It is possible that encrypting or re-encrypting your database will corrupt the database. Having a current database backup is the only way of recovering your data.

To create a database backup

1. Either use the default **Backup set name**, **Backup set description**, and **Server backup file path**, or modify those defaults.
2. Select the check box to confirm that you have read the warning at the top of the dialog.

3. Click [Backup].
4. If the backup fails for any reason, Setup Assistant shows a backup error. If possible, correct the error and then click [Backup] again.

Notes:

The backup set path is the path on the database server workstation. If running Setup Assistant on a workstation other than the database server and the default **Server backup file path** is **C:\Program Files\Microsoft SQL Server\...**, this refers to the database server's **C:** drive, not the workstation's **C:** drive.

The backup path cannot be a network drive. It must be a local drive.

The **Browse** button is available only if Setup Assistant is running on the database server. Click [Browse] to locate a backup path other than the default path.

If Setup Assistant is running on a workstation other than the database server, the **Browse** button is replaced with the **Reset Path** button. If your manually modified backup path does not function correctly, click [Reset Path] to return to the default backup path.

If the system is configured to archive to a SQL or SQL Express database, then Setup Assistant gives you the option of backing up the Archival database in addition to the Live database.

This database backup function only allows you to create the database backup. It does not allow you to restore from the backup. Use the standard SQL tools if you need to restore the database. For more information, refer to Restoring Databases on page 20.

Database Backup (Archival)

If the system is configured to archive to a SQL or SQL Express database, then Setup Assistant gives you the option of backing up the Archival database in addition to the Live database. For more information on the fields and buttons shown on this Setup Assistant form, refer to Database Backup on page 47.

Database Setup and Encryption

For server installations, Setup Assistant runs Database Setup automatically. The Database Setup program sets up the database as needed by the current OnGuard version, installs reports as needed, sets encryption key management and recovery options, updates database field encryption as needed, and runs Forms Translator.

For more information, refer to Run Database Setup on page 56.

Database Setup (Archival)

For server installations that are also configured to archive into an Archival database, Setup Assistant runs Database Setup on the Archival database in addition to the Live database. For more information about Database Setup, refer to Run Database Setup on page 56.

LS Message Broker Service

Setup Assistant helps resolve issues with the LS Message Broker service configuration. If there is a configuration error, Setup Assistant suggests what to change for a successful configuration.

OnGuard Reports & Dashboards Database

Setup Assistant creates and populates the reports and dashboards database on the OnGuard database server (specified in the **application.config** file). If an alternate host was provided, then this step is not shown. For more information on using an alternate host, refer to Running OnGuard Reporting and Dashboards from an Alternate Server on page 115.

IMPORTANT: If the Reporting and Dashboards feature is installed on the server, the Configuration Editor uses the information contained in the **ACS.INI** and **application.config** files to configure the contents of the **C:\Program Files\JReport\Server\bin\dbconfig.xml** file. Editing the **ACS.INI** or **application.config** files manually is not advised. If you manually edit these files instead of using the Configuration Editor, the **dbconfig.xml** file might not be configured correctly, resulting in unexpected system behavior.

OnGuard Reports & Dashboards

Setup Assistant first sets the **AccessControl_ReportsConfig** database users and tables. Setup Assistant then populates the required data into those tables, if necessary. If an alternate host was provided, then this step is not shown.

Note: The naming convention for the ReportsConfig database is ***<Live OnGuard database name>*_ReportsConfig**. Since the default name of the Live OnGuard database is *AccessControl*, the default name of the ReportsConfig database is **AccessControl_ReportsConfig**. But if you manually changed the name of your Live OnGuard database to *AccCtrl*, for example, then your ReportsConfig database would be named **AccCtrl_ReportsConfig**.

Service Startup

Setup Assistant then starts all product services configured to start automatically. Setup Assistant lists all services that will be started, each service's status, and provides a progress bar.

Login Driver Verification

Setup Assistant then tests that all encryption-related settings are configured correctly. If the test doesn't pass, Setup Assistant provides a description of the failure.

Finished

Setup Assistant notifies users when it is finished. When appropriate, the Finished page lists:

- Tasks that were skipped.
- Warnings encountered during a task.
- Errors that were found.

If no tasks were skipped, warning were encountered, or errors were found, then the Finished page shows only that Setup Assistant is complete, and the software is ready for normal operations.

Setup Assistant notifies users upgrading a server with versions of OnGuard earlier than 6.3 that they should run the Universal Time Conversion Utility. To run the utility, click [Launch Universal Time Conversion Utility].

This utility converts local times stored in the database to Coordinated Universal Time for multi-time zone compatibility, and ensures accurate historical data reporting. The utility does not interfere with normal system operation, although the conversion can take a significant amount of time for large databases.

For more information, refer to the Universal Time Conversion Utility appendix in the Upgrade Guide or the Enterprise Setup & Configuration User Guide.

Manually Running Security Utility

You should run Security Utility again whenever a Windows Update or Service Pack is installed on the workstation.

To run the Security Utility manually:

1. Launch the OnGuard Security Utility.
2. Click [More Info] to review the Security Utility release notes.
3. Click [Agree] if you agree with the disclaimer notice.
4. Follow the on-screen instructions and click [Apply] when ready.

Install Your OnGuard License

You must have a license to run the OnGuard software. The license comes to you from the factory, and has the extension *.xml, *.lic, or *.lic.xml. Licenses only need to be installed one per system and are usually installed on the server. To use License Administration, you may need to update your Internet browser security settings to allow pop-ups and add the License Server to the list of trusted sites.

Information regarding your dongle or software license ID, referred to as your System ID, can be found in the ***Help > About*** section of the OnGuard applications.

Below are listed several license elements that should be noted.

Software Licenses: OnGuard now utilizes a software license, which works without the need for a hardware dongle. When using a software license you are able to use License Administration to activate, return, or repair your license.

IMPORTANT: Software licenses can only be used on a physical computer or in a VMware ESX virtual environment. In a VMware ESX virtual environment, only the License Server is supported. The License Server must be used with a software-based license and not with a dongle-based license. For more information, refer to the OnGuard compatibility charts, located on the LenelS2 Connect™ portal at: https://connect.lenels2.com/s/downloads. Once there, select **Compatibility Charts** from the **Choose type of download** menu.

Note: When accessing the **Downloads** section on the LenelS2 Connect™ portal at https://connect.lenels2.com/s/downloads., make sure to select the version of OnGuard that is currently installed.

It is important that access to https://activate.lenels2.com:443 is allowed through your proxy if you wish to activate and deactivate licenses. If it is not, you must activate by phone.

IMPORTANT: TCP port 443 is required for online activation and deactivation. While it does not need to be added as a firewall exception, it should not be restricted or filtered.

Licenses for Hardware: Hardware licenses are based on the number of controllers for a given panel class. For example, instead of having different licenses for different types of panels in the same class (such as fire) a single license covers all the different panels that are in the same class.

Note: If you are installing non-LenelS2 HID access panels you must purchase a separate license. LenelS2-branded HID access panels, however, come with a built-in license. You can add any combination of HID access panels and other types of access panels up to the maximum capacity of your OnGuard system.

Expired Licenses: An alarm is generated when the system license is set to expire. This alarm is dependent on Linkage Server being configured and running on a host workstation. Although not required, it is advised that this alarm be configured to be emailed to the system administrator to ensure proper notification. For more information, see the Acknowledge Alarms chapter in the Alarm Monitoring User Guide.

IMPORTANT: In order for the alarm to be reported to monitoring stations there must be at least one panel configured and marked online. The panel does not need to exist or actually be online in Alarm Monitoring, it simply needs to exist in the System Status view.

Log into License Administration

1. Make sure that the License Server is running. The License Server must run on the server specified in the Configuration Editor.
2. Launch License Administration. If your browser has JavaScript support enabled, a new window will open with the License Administration application in it. Otherwise, follow the directions in the browser's window and click the hyperlink to continue. The License Administration application will then open in the same browser window. You must have cookie support enabled for this to work.

Notes: The URL for License Administration is: https://*LICENSESERVERHOST*:9999/. Replace *LICENSESERVERHOST* with the name of the machine the License Server is running on. For example, if the machine running the License Server is named alpha, the License Administration URL will be: https://alpha:9999/.

The License Server host name should match the Fully Qualified Domain Name (FQDN) of the machine. The certificates used by the License Server are the same as the certificates used by other OnGuard services (for example, the OpenAccess service). If the License Server host name and the certificate common name do not match, then License Administration and Setup Assistant might not function correctly.

If the License Server does not start, OnGuard may have been installed directly on a non-default drive (X). If this is the case, the following setting needs to be added to the **ACS.ini** file so the License Server can locate the JRE:

```
[LicenseServer]
JAVA_HOME=<X>:\OnGuard\JRE
```

For example, if installing on E drive:

```
[LicenseServer]
JAVA_HOME=E:\OnGuard\JRE
```

3. In the **Username** field, type a valid username. Usernames must contain at least eight characters.

Note: License Administration requires creation of an Administrator account to operate. Before creating an Administrator account (with associated username and password), License Administration will be in Maintenance Mode. While in Maintenance Mode, users can only access License Administration from the Local Machine, and all license requests are ignored. Once the Administrator account is created (typically during Setup Assistant), License Administration will operate as expected.

4. In the **Password** field, type a valid password that corresponds to the username entered. Passwords:
   - Are at least eight characters long
   - Are case sensitive
   - Contain at least two of the following three attributes: upper-case characters, lower-case characters, special characters
   - Do not expire
5. Click [Save]. The License Administration options will be displayed.

Changing Administrator Properties for License Administration

To change the user name and password, do the following:

1. Log into License Administration.
2. Click [Administrator Properties]. The administrator properties are shown in the right half of the window.
3. You can change the user name, password, or both.
4. To change the user name, enter a new value in the **Username** field.
5. To change the password, enter a new value in the **Password** field.
6. If you are changing the password, you must reenter the password in the **Confirm Password** field.
7. Click [Update]. A message will be displayed that indicates whether the administrator properties were successfully updated.

Install a New License

Note: All customers upgrading to OnGuard 7.5 and later from earlier versions must return their Software License. A license check dialog is shown during the upgrade process from OnGuard 7.4 and earlier to OnGuard 7.5 and later. This dialog is not shown if upgrading from OnGuard 7.5 and later to a newer version. The OnGuard subscription software license does not require activation, but is associated to the OnGuard license activation through the System ID.

1. Obtain a new license file from the factory. Be sure that you know where the license file is saved, as you will need to know the location to successfully install the license.
2. Make sure that the License Server is running.
3. Log into License Administration.
4. Click [Install New License].
5. Under **Main License File** and/or **Subscription License File**, click [Choose File] to locate the license file, and then double-click to select the file.
6. Click [Next].
7. View the license to verify that the software license is active, and confirm that it is the correct license.

8. Scroll down to the bottom of the window and click [Next], or if it is incorrect, click [Back] and select another license file.
9. Read the terms of the license agreement and select the **Yes** radio button if you agree with the terms of the license. If you disagree, then you will not be able to install the license.
10. If the license file is already activated, click [Finish].

    If the license file is not active yet, you must activate it. For more information, refer to Activate a Software License on page 53.

The license installs and an entry is displayed in the **Installed Licenses** drop-down list box indicating the name of the product that the license controls.

Activate a Software License

You must activate the software license to have a functioning system.

Note: All customers upgrading to OnGuard 7.5 and later from earlier versions must return their Software License. A license check dialog is shown during the upgrade process from OnGuard 7.4 and earlier to OnGuard 7.5 and later. This dialog is not shown if upgrading from OnGuard 7.5 and later to a newer version. The OnGuard subscription software license does not require activation, but is associated to the OnGuard license activation through the System ID.

There are three ways to activate a license:

- Online (which requires an Internet connection)
- Text message (SMS)
- Phone

To activate, you will need the **System ID** and the **Activation Code**. The System ID is the 5- or 6-digit ID associated to the license being activated, and the Activation Code is a 24-digit alphanumeric code.

Online Activation

Your Internet browser must allow the URL https://activate.lenels2.com:443 to activate and return licenses. In addition, port 443 is required for online activation and revocation.

1. In License Administration, view the license you have installed.
2. Click **Activate**.
3. Choose the **Online** activation.
4. Click [Activate].
5. Click [Close] once the license has activated.

Text Message (SMS) Activation

1. In License Administration, view the license you have installed.
2. Click **Activate**.
3. Choose **Phone** activation.
4. Click [Activate].
5. Send a text message to 585-673-7750. EMEA customers should text +44 7937 947945. Use the following format in your text message: [System ID][required space][Activation Code].

Note: Activation Codes are case-sensitive. For additional assistance, text the word **HOWTO**.

6. You will receive a confirmation code in seconds. Enter the confirmation code in License Administration. The license will activate.
7. Click [Close] once the license has activated.

Phone Activation

1. In License Administration, view the license you have installed.
2. Click **Activate**.
3. Choose **Phone** activation.
4. Before calling, have your **System ID** and **Activation Code** ready.
5. Call 1-866-788-5095 option (5), or email sig@carrier.com with the System ID and Activation Code. EMEA customers should call +48 5832 62240, or email sig.emea@carrier.com.
6. Click [Close] once the license has activated.

Returning an OnGuard Software License

There are three ways to return an activated license before moving it to another server:

- Online (which requires an Internet connection)
- Text message (SMS)
- Phone

To return, you will need the **System ID** and the **Return Code**. The System ID is the 5- or 6-digit ID associated to the license being returned, and the Return Code is a 24-digit alphanumeric code.

Online Returning

Your Internet browser must allow the URL https://activate.lenels2.com:443 to activate and return licenses. In addition, port 443 is required for online activation and revocation.

1. In License Administration, view the license you have installed.
2. Click **Return**.
3. Choose the **Online** revocation.
4. Click [Return].
5. Click [Close] once the license is returned.

Text Message (SMS) Returning

1. In License Administration, view the license you have installed.
2. Click **Return**.
3. Choose the **Phone** method.
4. Click [Return].
5. Send a text message to 585-673-7750. EMEA customers should text +44 7937 947945. Use the following format in your text message: [System ID][required space][Return Code].

Note: Return Codes are case-sensitive. For additional assistance, text the word **HOWTO**.

6. You will receive a confirmation code in seconds. Enter the confirmation code in License Administration.
7. Click [Close] once the license is returned.

Phone Returning

1. In License Administration, view the license you have installed.
2. Click **Return**.
3. Choose the **Phone** method.
4. Before calling, have your **System ID** and **Return Code** ready.
5. Call 1-866-788-5095 option (5), or email sig@carrier.com with the System ID and Return Code. EMEA customers should call +48 5832 62240, or email sig.emea@carrier.com.
6. Click [Close] once the license is returned.

License Troubleshooting

In the event of a software license failure, a message is displayed with the date and time the OnGuard application will close if the license is not repaired.

License Administration provides two additional options: **Repair** and **Update**. These options are not used during normal license operation and are there to help you more easily correct specific issues with your software license. If you need to use them, they operate similar to the Activate and Return options, so please follow the prompts in the interface.

- **Repair** is used to repair/restore the license activation on the current server in the event of a failure of the software license.

  The Repair option IS NOT visible unless the license server detects your software license is broken (signature or trust failure).
- **Update** is used to cause the license server to refresh the Support Subscription (SUSP) information for your OnGuard Server (after the renewal/update of a SUSP contract).

  You may need to wait 24 to 48 hours after updating your SUSP contract for the information to propagate to our licensing server.

Symptom: Activation Code is blank.

Resolution:

1) Stop LS License Server and FLEXnet Licensing Service.
2) Browse to the following location: **C:\ProgramData\FLEXnet**.
3) Delete all of the existing files in that location.
4) Start the FLEXnet Licensing Service and LS License Service. You should now see an Activation Code.

If the above process does not work, do the following:

1) Open the command prompt on the License Server workstation.
2) Change directories until you are at the root of the OnGuard directory (typically **C:\Program Files\OnGuard** for 32-bit systems and **C:\Program Files(x86)\OnGuard** for 64-bit systems).
3) Type the following and then press [Enter]:
   appactutil.exe -shortcode OnGuard.asr -return SCASR_FID_1_OnGuard
4) A code is provided. Give that code to Tech Support or SIG. Tech Support or SIG will then provide you with a Return Code that will allow your software license to be returned.
5) Once the license is returned, you can activate it on a new machine online or over the phone.

For other OnGuard license installation issues, please consult the LenelS2 Knowledgebase online (https://kb.lenels2.com).

Run Database Setup

The Database Setup program sets up the database and installs the reports needed. This only needs to be run on a server. This is also part of the Setup Assistant. For more information, refer to Setup Assistant on page 45.

When using Crystal Reports, the database name can begin only with a letter. The rest of the name can contain only numbers, letters, and underscores.

IMPORTANT: The installation and upgrade process assumes your OnGuard database is called "AccessControl." If this is not the case, use the Configuration Editor to modify the **application.config** file to correct this. For more information, refer to Database section on page 92.

1. Launch Database Setup.
2. If upgrading the database, the Choose Task window opens. Select the action you would like to perform. Click [Continue]. The choices include:
   - **Live** or **Archival** - If upgrading a database, these allow you to choose if you want to upgrade the Live database or the Archival database (if database archiving is enabled; for more information, refer to the Archives Folder chapter in the System Administration User Guide).

Note: The ACS.INI and application.config files must always point to the Live database, not the Archival database.

   - **Add/remove missing system data for current build** - If you feel that you are missing system data, selecting this will add information back into the build.
   - **Compare database schema [no data]** - Checks to see if the schema has changed. This does not compare data. This would be useful to run before upgrading to see if any schema changes have occurred, though it is not necessary.
   - **Upgrade database** - Select to upgrade your database.
   - **Re-encrypt database with a new key** - Select to re-encrypt a database that was already encrypted with a new encryption key. For more information, refer to Encrypting and Re-encrypting Databases on page 57.
3. For new installations, the Database Setup Progress window opens telling you that you are about to create a new database. Click [Execute].

   If upgrading a database, a warning message appears reminding you to back up your database. For more information, refer to Chapter 3: Database Backup and Restoration on page 17. If your database is backed up, click [Yes].
4. The database installs. If upgrading the database, the system will be checked for anomalies. Anomalies are database features that are unknown to OnGuard and can include custom tables, triggers, stored procedures, and so on. Not all users will encounter anomalies. When prompted to take action on anomalies, the items listed should be familiar to the person performing the upgrade. Select all items that you know should exist and click [Continue]. Failure to select known anomalies may result in the failure of custom functionality.

Note: Form Translator runs automatically, allowing you to use the OnGuard Web Applications, if desired. This occurs only after Database Setup runs on the Live database. Form Translator does not run on the Archival database.

5. The database is encrypted using the encryption key stored in the Login Driver.

Note: It is important that you do not interrupt the database encryption process before it completes. If this occurs, unexpected system behavior will result. For information on troubleshooting database encryption errors, refer to Database Encryption Errors on page 88.

Encrypting and Re-encrypting Databases

When running Database Setup for the first time after a fresh installation of OnGuard, or when upgrading from OnGuard 8.0 or earlier, or when upgrading an existing database that was already encrypted and selecting the **Re-encrypt database with a new key** option in the **Choose Task** window, the **Encryption key entry** dialog opens. Perform the following procedure:

Note: Since encrypting or re-encrypting the database involves generating the encryption key, you must perform this procedure on the workstation with the LS Login Driver installed. After running Setup Assistant, the LS Login Driver service on this workstation will be active, and will respond to clients and other services.

1. Choose whether you want Database Setup to either:
   - **Generate a key from a passphrase** - You provide a passphrase that is used to generate the encryption key, or
   - **Generate a random key** - Database Setup will generate a random encryption key automatically.
   - **Import a key from a file** - You import a ***.og** key file that was exported during an earlier OnGuard installation.
2. If you selected **Generate a key from a passphrase**, type your passphrase into the fields. The length of your passphrase must be from 10 to 36 characters. If you want to see the passphrase you typed, select **Show passphrase**.
3. LenelS2 *recommends* that you export your encryption key to a file to support restoration of the key, if necessary. Select **Export key to a file**, and then click [Browse] to identify the directory into which the file will be written. You *must* export your encryption key to a file if you selected **Generate a random key** above.

   IMPORTANT: The exported key file is required to allow access to encrypted data if the system must be reinstalled due to disaster recovery or other loss. Consider this file a tightly-controlled cryptographic resource that you would provide to the end-user for secure storage and key management.
4. Click [OK].

Blocking All Connections to the Database

With OnGuard 8.1 and above, re-encryption of the database is performed automatically when performing a new installation of OnGuard, or when upgrading to these OnGuard versions for the first time. Once the customer specifies a system-specific encryption key, the re-encryption process does not need to be done again, unless the encryption key used has been lost or compromised.

IMPORTANT: It is very important to block other connections to the OnGuard database before re-encrypting the database.

When using the Microsoft SQL database engine, OnGuard blocks all connections automatically. This does not happen automatically if using an Oracle database. Because the Oracle database engine does not have a “Single user mode” administrative mode, you must block other database connections manually:

1. Disconnect the Oracle database server from the local network, or

   Limit access to the Oracle database server to only allow client applications from the Oracle server workstation:

   1) Edit the **SQLNET.ORA** file. This file can be found in the **$ORACLE_HOME/network/admin** directory. Add this line to the file:

      ```
      tcp.validnode_checking = yes
      ```

   2) Supply a list of nodes to allow, including **localhost**:

      ```
      tcp.invited_nodes = (localhost,<yourOracleServerHostName>)
      ```

      For example:

      ```
      tcp.invited_nodes = (localhost, OracleHost)
      ```

   3) Restart the Oracle server workstation to close existing database connections from other client workstations.
2. Stop every OnGuard service or application except LS License Server, LS Message Broker, and LS Login Driver.
3. Start the re-encryption procedure either with Setup Assistant while upgrading to OnGuard 8.1 or later, or with Database Setup when re-enrolling the database encryption key.
4. When the re-encryption procedure finishes, re-enable the connections to the Oracle OnGuard database. Depending on the method used to block the database connections, either:
   - Re-connect the Oracle server to the local network, or
   - Edit the **sqlnet.ora** file and remove the lines added above. Then restart the Oracle server to apply this change.

For more information about Oracle databases, refer to the *Advanced Installation Guide*.

Encryption Key Troubleshooting

The encryption key was not generated using Setup Assistant because the OnGuard installer was first run on a workstation that didn't have the Login Driver installed, or this was not the Message Broker host. Setup Assistant never forced the user to configure the encryption options.

Perform the following procedure to correct this issue:

1) Confirm this situation applies to your system by viewing the **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Lenel\OnGuard\LD** registry entry on the workstation running the Login Driver, and that is also the Message Broker host.
2) If that registry entry is empty, run Database Setup on that same workstation.
3) When prompted, provide the encryption key configuration details in the **Encryption key entry** dialog.

When starting any OnGuard thick-client application, the following error is shown:

Login Driver is not connected to the message broker. Confirm that the Login Driver service is started and available for DSN <workstation name>.

This error message can be caused for several reasons. Perform the following procedure to troubleshoot this error message:

1) If the Login Driver service is running, stop it and then run the Login Driver as an application. You might have to wait until the process stops running, or close it manually using Task Manager.
2) Check to see if the Login Driver application shows any errors.

   Refer to Encryption key set up for this Login Driver does not match the database in use on page 59 if you see that Login Driver error message.

   Refer to Encryption key loading failed...The data is invalid on page 59 if you see that Login Driver error message.

   Refer to Encryption key loading failed...Login failed for user on page 59 if you see that Login Driver error message.

   Refer to Login Driver is not connected to the Message Broker because you must set the RabbitMQ LD credentials on page 60 if you see that Login Driver error message.

Encryption key set up for this Login Driver does not match the database in use

When running the Login Driver as an application, the following error is shown:

Encryption key set up for this Login Driver is not in match with the database in use. Login Driver will not function properly until proper encryption key is provided.

Perform the following procedure to troubleshoot this error message:

1) If you see this error, open the Login Driver using the encryption key that corresponds with your database. To do so, open the Login Driver as an application, then select ***Edit > Set Encryption Key***. An ODBC dialog might open. If it does, enter the database credentials to establish the database connection. Then enter the encryption key passphrase, or set the encryption key using a ***.og** file.
2) If the encryption key provided is correct, the system will show a success message.

Encryption key loading failed...The data is invalid

When running the Login Driver as an application, the following error is shown:

Encryption key loading failed. Login driver will not function properly. Error: The data is invalid.

Perform the following procedure to troubleshoot this error message:

1) Configure the Login Driver with the same encryption key used with your database. Open the Login Driver as an application, then select ***Edit > Set Encryption Key***.
2) An ODBC dialog might open. If it does, enter the database credentials to establish the database connection.
3) Enter the encryption key passphrase, or set the encryption key using a ***.og** file.
4) If the encryption key provided is correct, the system will show success message.

Encryption key loading failed...Login failed for user

When running the Login Driver as an application, the following error is shown:

Encryption key loading failed. Login driver will not function properly. Error: Login failed for user '<user name>'

Perform the following procedure to troubleshoot this error message:

1) Select ***Edit > Change Database Password*** and update the password to match your LENEL password.
2) The Login Driver dialog opens, indicating that the database and Login Driver passwords are not synchronized. Click [Yes] to open the Change Password dialog.
3) Provide the correct database password in the dialog, then click [OK].

Login Driver is not connected to the Message Broker because you must set the RabbitMQ LD credentials

When running the Login Driver as an application, the following error is shown:

Login Driver is not connected to the message broker. Confirm that the Login Driver service is started and available for DSN <workstation name>.

Perform the following procedure to troubleshoot this error message:

1) Since there is no connection to the Message Broker, the Login Driver cannot confirm that the encryption key is correct. To fix this issue, you must provide the encryption key and connect to the database using the ODBC dialog.
2) When this is done, the Login Driver automatically tries to connect to the Message Broker, and will force you to provide the correct username and password in the **Set RabbitMQ LD credentials** dialog.

Configure the OnGuard Logs Folder

Some OnGuard applications use the files located in the logs folder and if a user does not have the appropriate Windows permissions to access these files they may encounter errors.

1. Navigate to the OnGuard logs folder. Its default location is **C:\ProgramData\Lnl\logs**.
2. Right-click the folder and select **Properties**.
3. Select the Security tab.
4. In the Groups or user names listing window, select the group or user name that will be using the OnGuard software.
5. Select the **Allow** check boxes for the permissions: Read, Write, and List Folder Contents.
6. Click [OK].

Remotely Hosted Databases

If you are using Windows Authentication in your application.config file and your Live database is hosted remotely from your server, the LS Site Publication Server (if Enterprise or Distributed ID) might need to be configured to log on as a specific user with NT authentication access to the database. You will know that this configuration is required if this service refuses to start, and the error log shows *unable to connect to database* errors.

To configure a service to log on as a specific user:

1. Click [Start], and then select **Control Panel > Administrative Tools**.
2. Double-click on **Services**.
3. Double-click on the service you wish to configure.
4. Select the **Log On** tab, and then select **This account**.
5. Enter the username and password. The best method for this is to click [Browse], type the username and then confirm it by clicking [Check Names]. Then enter the user's password.
6. Click [OK] to close the Select User dialog.
7. Click [OK] to close the service's Properties dialog.
8. Restart the service.
9. Close the Services window.

This will start the service so that it is logged on as the user you specified. The service will then have the same network permissions as that user.

CHAPTER 7

Installing OnGuard on a Client Machine

Installing OnGuard on a client machine has only two general steps: installing the software and verifying the system's license has been installed.

The installation is the same as on the server except you do not need to install a database, run Database Setup, install a license, or install a hardware key (dongle).

There are two ways to install OnGuard on client machines:

- Manually install OnGuard on each client workstation using either the **OG.iso** or the **OGCLIENT.iso** file. For more information, refer to Chapter 6: Installing OnGuard 8.3 on page 41.
- Install OnGuard silently using a PowerShell wrapper script and either the **OGCLIENT.iso** or the **OG.iso** file. For more information, refer to "Unattended Installation of OnGuard" in the *Advanced Installation Topics* guide.

The **OGCLIENT.iso** file has a smaller file size than the **OG.iso** file because it only includes the OnGuard features required for a client workstation, and does not include the following third-party support items:

  - Crystal Reports
  - RabbitMQ
  - Erlang
  - OnGuard Modules

CHAPTER 8

Database Authentication for Web Applications

The following situations require the configuration of a method of authentication:

- Systems with Oracle databases. For Oracle installation instructions, refer to the Advanced Installation Topics guide.
- Systems using browser-based OnGuard applications.

There are two methods of authentication available:

1. Windows authentication within the database server.
   - Refer to Configure Windows Authentication with SQL Server on page 65, or
   - Windows Authentication with Oracle on page 66.
2. Provide Credentials in the Protected File on page 68.

Note: When used in this chapter, *Windows authentication* refers to the use of a single log on to gain access to both Windows and the database.

Windows Authentication with SQL Server

SQL requires authentication configuration for browser-based applications to run successfully.

Configure Windows Authentication with SQL Server

The following process will take you through the process of configuring Windows authentication.

Add the Windows user to SQL Server

1. Launch the SQL Server Management Studio.
2. In the Object Explorer pane of the SQL Server Management Studio, expand the Security folder.
3. Right-click the Logins folder and select **New Login**.
4. In the General page of the Login window:
   a. In the **Login name** field, type <*server-name*>\<*username*>, where <*server-name*> is the name of the server and <*username*> is the name of the Windows user.

b. Select the **Windows authentication** radio button.

5. Click [Search] to launch the Select User or Group dialog. This dialog is used to verify that the Login name is correct.
   a. In the **Enter the object name to select** text box, enter the user name.
   b. Click [Check Names]. If the user is found it will appear underlined.
   c. Click [OK].
6. Select **User Mapping** from the **Select a page** pane.
   a. Select (check) the `<Server Name>lenel` database from the Users mapped to this login list.
   b. In the Database role membership for `<Server Name>lenel`, the recommended settings are (check):
      - db_owner
      - public

      For advanced users who do not want the **db_owner** role assigned to the user, the minimum required settings are:
      - public
      - db_datareader
      - db_datawriter
      - db_ddladmin
      - db_executor

Note: If the db_executor role does not already exist, refer to step 7a through step 7e in the procedure, Create a Login on page 33.

   c. Click [OK].

The new login will appear in the Logins folder.

Verify the Integrated Security Setting

Use the Configuration Editor to verify that the **application.config** file is configured for Windows authentication. For more information, refer to Advanced Database section on page 93.

Windows Authentication with Oracle

Oracle requires authentication configuration for Database Setup and the browser-based applications to run successfully.

Add the Windows user to Oracle

To configure Windows authentication with Oracle, a new Oracle user must be created with Windows authentication credentials.

1. Launch SQLPlus.
2. Log in using the **system** account. Enter SYSTEM@<SID> for the username and password.

IMPORTANT: You must be logged in as SYSTEM to run the script.

3. Verify Oracle connects properly. You should see "Connected to" in the console.

   IMPORTANT: We do not recommend granting the DBA role to a Windows Authenticated user. To restrict the users' roles and system privileges, refer to step 4. If restricting the Windows Authenticated user, then the user provides OnGuard functionality only. Any database level administration, such as backups ad restores, must be performed by a different user with higher database roles and system privileges.

4. To create the Windows Authenticated user with the desired level of roles and system privileges, at the SQL prompt, run the following command(s):

   IMPORTANT: If you are not using the LENEL_DATA and LENEL_TEMP data spaces, you must change the LENEL_DATA and LENEL_TEMP references in the CREATE USER line to the desired table spaces you want to use. Contact your database adminstrator for details. Update both references to OPS$DOMAIN\DOMAINUSER with the actual domain and user name of the Windows User you are creating.

   a. **@@<Path to OnGuard Installation Directory>\program files\OnGuard\DBSetup\New\WindowsUser_Authentication.ora** or

   b. If the LENEL_RESTRICTEDUSER_ROLE has not been created, then enter commands described in "Create a Restricted User Role" in the Advanced Installation Topics guide. Then run the following commands, replacing both occurrences of "*<OPS$DOMAIN>**<DOMAINUSER>*" with the actual domain name and user.

   ```
   CREATE USER "<OPS$DOMAIN>\<DOMAINUSER>" PROFILE "DEFAULT"
   IDENTIFIED EXTERNALLY DEFAULT TABLESPACE "LENEL_DATA"
   TEMPORARY TABLESPACE "LENEL_TEMP" ACCOUNT UNLOCK;
   GRANT CONNECT, RESOURCE, LENEL_RESTRICTEDUSER_ROLE TO
   "OPS$DOMAIN\DOMAINUSER";
   COMMIT;
   ```

5. Verify there were no errors. You should see output similar to:

   "User created."

   "Grant succeeded."

   "Commit complete."

6. Exit SQL Plus.

7. Navigate to the **sqlnet.ora** file located at **$ORACLE_HOME\Network\Admin** and edit it to verify authentication is set to "NTS" on the following line:

   ```
   SQLNET.AUTHENTICATION_SERVICES=(NTS)
   ```

Verify the Integrated Security Setting

Use the Configuration Editor to verify that the **application.config** file is configured for Windows authentication. For more information, refer to Advanced Database section on page 93.

Provide Credentials in the Protected File

Windows authentication is the recommended method of configuration. You can also store the authentication information in the **application.config** file. When this method is used, it is highly recommended that you secure the file with Access Control Lists (ACL). When ACL is used, the information within the file is very secure.

This authentication method requires advanced knowledge of Windows security and is not recommended.

IMPORTANT: When providing credentials in a protected file, the ODBC authentication method must not be set to Windows authentication.

Securing Files with the Access Control List

The Access Control List (ACL) is a highly secure method of protecting information stored within a file. OnGuard can be configured to store user credentials within a file which must be secured to protect the information. This configuration can be performed on the Security tab of the file properties dialog. Right-click on the file and select **Properties**.

The account that administers the system should have read and write access any file containing user credentials so that they can maintain the file information. In addition, certain other accounts must have access to the files.

- The **application.config** file is used by the services and applications to determine where the database is and how to authenticate (by indicating integrated authentication or providing credentials):
  - LS Site Publication Server
  - Database Setup
  - Form Translator
  - Setup Assistant
  - Universal Time Conversion Utility
  - Configuration Editor
  - and more

Application.config

The **application.config** file can be used to store the **lenel** user account credentials for access to the database when Windows authentication is not used. This is not the recommended configuration, however, with ACL the login credentials can be secured.

Store the lenel User Account Credentials

You can use the Configuration Editor to store the **lenel** user account credentials in the **application.config** file for authentication with the database server account. For more information, refer to Advanced Database section on page 93.

Oracle Users

Oracle users must also edit the **sqlnet.ora** file to specify the authentication method.

1. Navigate to **\oracle\product\10.1.0\Db_1\NETWORK\ADMIN** and edit the **sqlnet.ora** file.
2. Verify that authentication is set to “None” in the following line:

```
SQLNET.AUTHENTICATION_SERVICES=(None)
```

CHAPTER 9

Logging Into the OnGuard System

The following chapter deals with everything you need to know about logging into the OnGuard system.

Windows User Permissions

The Windows user logged in to the OnGuard applications must have read/write access to the OnGuard directory. This permission is required so that users can write to the log files.

Error Messages

Read weak password messages/warnings carefully to avoid confusion about whether your user password or database password is weak.

If you have a weak database password you will receive a warning every time you log into any application, until you change your database password. Although it is not recommended, you can acknowledge the warning and continue working in the application. This table describes the password-related error messages that may be generated and which password you need to correct.

- To correct the database password, refer to the Accounts and Passwords chapter in the Installation Guide.
- To correct the user password, select a password that meets the standards specified in Password Standards on page 79.

Warning message	Password to correct
Database password violations: Your password is a keyword that is not allowed. It is highly recommended that you change your password to meet our minimum password standards.	Database
Your password cannot be blank. Please enter a password.	User
User password violations: Passwords cannot be the same as the user name.	User

Warning message	Password to correct
Your password is a keyword that is not allowed.	User

Accounts

Anyone who wishes to use OnGuard applications must enter a user name and password in order to access the software. The System Administrator should create a unique account for each user of the applications. The System Administrator can also, for each user, create a list of permissions, which specifies precisely which screens, fields, and buttons the user can access.

During initial installation of the application, default accounts are created. These include:

User name	Password	Type
SA	SA	system account
admin		sample
user		sample
badge		sample

These are provided as samples. You may change the passwords and use the accounts, or remove them. The exception to this is the system account, SA. By definition this account has permission to do anything in the system. A user with system access has unlimited access to the application. You cannot delete or change the system account except to modify the password.

The first time you log into OnGuard to configure the application, use **SA** as the user name and the password. Change the password according to the policies and standards described in Passwords on page 78.

Log In

This procedure describes how to log in without using single sign-on. For a description of single sign-on, refer to Single Sign-On on page 73. To log in using single sign-on, refer to Configure Single Sign-On on page 74.

1. In Windows, start the desired application.

   For more information, refer to “Using OnGuard on Supported Operating Systems” in the Installation Guide.

2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to the next step. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. The Log On window displays.
   a. In the **User name** field, type the user name assigned to you. When logging in for the first time, your user name is **SA**.
   b. In the **Password** field, type the password assigned to you. When logging in for the first time, your password is **SA**. Note that the characters you type do not appear in the field. Instead, for

each character you type, an "*" displays. This is intended to protect against unauthorized access in the event that someone else can see the screen while you type.

IMPORTANT: After logging in for the first time, you are strongly encouraged to modify the password for the system account as soon as possible to discourage unauthorized use.

c. In the **Directory** field, select the directory that you wish to log into. For user accounts not using single sign-on, the default is "<Internal>."

d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.

e. Click [OK].

4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning click [Yes].

Single Sign-On

Single sign-on simply means logging into OnGuard with the same user name and password that you use to log into Windows or logging into OnGuard using an LDAP user name and password for authentication. *LDAP* (Lightweight Directory Access Protocol) is a software protocol that enables you to locate businesses, people, files, and devices without knowing the domain name (network address).

Notes: Windows Authentication should be used when single sign-on is desired. In other scenarios, use Anonymous Authentication. For more information, refer to:

http://support.microsoft.com/kb/258063

and

http://msdn.microsoft.com/en-us/library/aa292114%28VS.71%29.aspx.

Note: The use of the explicit username and password for directory authentication to Windows is strongly discouraged. It is recommended that you do not store Windows passwords in the OnGuard system, since OnGuard uses reversible encryption and Windows does not. If explicit authentication is required, you should use an account that has view only permission to the directory in question.

It is possible to assign both an internal account and one or more directory accounts to a single user. Assigning both types of accounts increases the flexibility of the system during the authentication process. If the directory service is down or cannot be found from the workstation where the user is logging on, that user can instead use the internal account. Using both types of accounts means that you need to manage the internal account user names and passwords in addition to managing the directory accounts.

IMPORTANT: Allowing a user to log on in multiple ways increases the probability that the user's access to the system could be compromised. It is recommended that you standardize on either internal or directory accounts, but not both.

There are cases where assigning both an internal account and a directory account to a user may make sense. In a system where directory accounts are predominantly used, you may also assign an internal account to a user who needs to access the system from locations where the directory service is

unavailable. If internal accounts are predominantly used, you may want to assign a directory account to a user so that the user does not need to enter in a password to log on.

Directory Accounts

To log into OnGuard using single sign-on, a user name, password, and directory are required. A *directory* is a database of network resources, such as printers, software applications, databases, and users. The following directories are supported by OnGuard: Microsoft Active Directory, Microsoft Windows NT 4 Domain, Microsoft Windows Local Accounts, and LDAP.

Automatic and Manual Single Sign-On

When a user account is configured for single sign-on, the user can log into OnGuard automatically or manually.

For example, with automatic single sign-on, users simply start OnGuard and they are automatically logged in under their Windows account and directory.

With manual single sign-on, users must manually enter their Windows or LDAP account information (user name and password). Users also have the option of selecting a different configured directory.

If single sign-on is not used, users manually enter a user name and a password that is different from their Windows or LDAP password. The directory is hard-coded to refer to the internal OnGuard user directory.

Notes: Manual single sign-on can be used with the following directories: Microsoft Active Directory, Microsoft Windows NT 4 Domain, and LDAP.

Automatic single sign-on can be used with every directory supported by OnGuard except LDAP because it doesn't provide all the account information required.

Configure Single Sign-On

By default, user accounts do not use sign-on. To configure single sign-on the System Administrator must add a directory and link a user account to the directory.

Log In Using Automatic Single Sign-On

Automatic single sign-on is supported with Windows domain accounts.

1. In Windows, start the desired application.
   For more information, refer to "Using OnGuard on Supported Operating Systems" in the Installation Guide.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. If your Windows account is linked to a user, a message will be displayed that says, "Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT." To automatically be logged in, do nothing.
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].

Log In Using Manual Single Sign-On

Both users who want to log into OnGuard using an LDAP user name and password for authentication and users who want to log in using a Windows domain account can do so using manual single sign-on.

1. In Windows, start the desired application.
   For more information, refer to "Using OnGuard on Supported Operating Systems" in the Installation Guide.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. If your Windows account is linked to a user, a message will be displayed that says, "Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT."

   To manually login or to login using a different user name and password, hold down the <Shift> key. The Log On window opens.

   a. In the **Directory** field, select the directory that you wish to log into. The default is "<Internal>."
   b. In the **User name** field, type the Windows user name assigned to you. Do not enter the domain\user name just enter your user name.
   c. In the **Password** field, type the Windows password assigned to you.
   d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.
   e. Click [OK].
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].

Troubleshoot Logging In

If you attempted to log in and were unable to do so, make sure that the following conditions have been met:

- You entered the correct user name and password for the selected directory of a user with permission to use the application.
- If your system is configured to display an authorization warning, you accepted the terms.
- A valid license is installed:
  - Verify your License Server settings (refer to the *Configuration Editor* appendix in the *Installation Guide*). The LS License Server service must be started on the specified Host.
  - Log into the License Administration application to verify a valid license is installed.
  - Software-based licenses must be activated.
  - USB licenses must have License Key Drivers installed.
- If using single sign-on, ensure the PC user you are logged in as is linked to an internal OnGuard user through an operational directory.

- Verify that the LS OpenAccess service is running (contact your OnGuard system administrator if necessary).

Assigning Directory and Internal Accounts to the User

It is possible to assign both an internal account and one or more directory accounts to a single user. Assigning both types of accounts increases the flexibility of the system during the authentication process. Meaning, if the directory service is down or cannot be found from the workstation where the user is logging on, then the user can use the internal account instead.

However, using both types of accounts means that you need to manage the internal account user names and passwords in addition to managing the directory accounts. Allowing a user to log on in multiple ways increases the probability that the user's access could be compromised. For that reason, it is recommended that you standardize on either internal or directory accounts, but not both.

There are cases where assigning both an internal account and a directory account to a user may make sense. In a system where directory accounts are predominantly used, you may also assign an internal account to a user who needs to access the system from locations where the directory service is unavailable. If internal accounts are predominantly used, you may want to assign a directory account to a user for that user's convenience, so that the user does not need to enter in a password to log on.

LenelS2 Console

LenelS2 Console is a web-based application designed to launch OnGuard web and desktop applications as well as third-party applications and websites.

To access LenelS2 Console, type `https://<hostname>:8080` into the address bar of a supported browser ("hostname" = the address of the OnGuard OpenAccess Server), and enter your OnGuard username and password.

LenelS2 Console consists of cards representing licensed and installed desktop and web-based applications with icons to identify desktop applications from web-based applications. To open an application, click the card.

Note: In order for LenelS2 Console to open a desktop application, the desktop application must be installed on the local workstation from which LenelS2 Console is opened.

Depending on permissions, an OnGuard users can re-arrange, re-color, and create custom cards for themselves only in LenelS2 Console, or they can create, modify, and delete templates.

For more information, refer to the online help available in LenelS2 Console.

CHAPTER 10

Accounts and Passwords

Accounts

The System Administrator should create a unique account for each user of the applications. The System Administrator can also, for each user, create a list of *permissions*, which specifies precisely what the user can access.

An SA Delegate user account can be created by the default system account (SA) user and assigned all permissions. Then the SA Delegate user can disable the default system account (SA) to increase the security of the system by having no default user accounts.

During initial installation of the application, default accounts are created. These include:

User name	Password	Type
SA	SA	system account
admin		sample
user		sample
badge		sample

These are provided as samples. You may change the passwords and use the accounts, or remove them. The exception to this is the system account, SA. By definition this account has permission to do anything in the system. A user with system access has unlimited access to the application.

The first time you log into OnGuard to configure the application, use **SA** as the user name and the password. Change the password according to the policies and standards described in Passwords on page 78.

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

The following table summarizes the OnGuard default accounts and passwords:

OnGuard Default Accounts and Passwords

Description	User name	Password	How to change the password
Default system administrator account. This is the account that is used initially to log into the main OnGuard applications, such as System Administration. **Note:** Upon initial login, OnGuard requires that the default password be changed. **Security recommendation**: After logging into OnGuard, create an SA Delegate user with all permissions and as the SA Delegate user, disable the default system account user.	SA	SA	For more information, refer to Change the System Administrator Password for the Database on page 81.
OnGuard database. This is the actual OnGuard SQL Server Desktop Engine, SQL Server, or Oracle database. By default, the login name for the OnGuard database is “Lenel.” This can now be customized as needed. If the name is changed, make sure to update or create a corresponding user account in your database.	LENEL	Secur1ty#	For more information, refer to Change the Database Password on page 80.
License Administration account. This is the account that is used initially to log into the License Administration application.	No default user name	No default password	For more information, refer to Install Your OnGuard License on page 50.

Passwords

OnGuard checks the user’s password against password standards. This functionality is designed to enhance password security if single sign-on is not used. If single sign-on is used (automatic or manual), OnGuard does not enforce password standards. For more information on single sign-on, refer to Single Sign-On on page 73.

Password Policies

OnGuard supports the configuration of password policies:

- A minimum password length
- Complex passwords (for example, a mix of uppercase alphabetic, lowercase alphabetic, numeric, and non-alphanumeric characters)

- Case-sensitivity of passwords
- Password expiration
  - Expiration after specified number of days
  - Warning to the user to change the password after a specified number of days
  - Force a change of password on next login
- Rejection of passwords that match entries on the list of prohibited keywords
- Rejection of re-using prior passwords based on a specified number of prior passwords
- Inactivity timeout after a specified amount of elapsed idle time
- Invalid login lockout after a specified number of failed attempts

Notes: When an OnGuard system is upgraded, current user passwords are supported until the configurations listed above require the passwords to be changed.

OnGuard also checks the OnGuard database user's password to ensure that it is not blank, it is not the same as the username, and it is not the same as an entry on the list of prohibited keywords. Database passwords conform to the rules of the specific database being used. For example, passwords in SQL Server are case-sensitive. For Oracle, passwords are case-sensitive by default, but there is an option to make them case-insensitive (not recommended for security purposes). Database user passwords apply to SQL Server Desktop Engine, SQL Server, and Oracle. For information on changing your database password refer to Change the Database Password on page 80.

Password Standards

When creating a strong password keep the following guidelines in mind:

- Passwords cannot be blank
- Passwords cannot be the same as the user name (for example, SA, SA)
- Passwords cannot be on the list of prohibited keywords.
- Depending on the configured password policies, it may be required that your password contain numbers, letters, and symbols. Spaces are also acceptable. (for example, August 18, 1967)
- OnGuard user passwords are case-sensitive.
- The maximum value for a strong password is 127 characters. The minimum value is 1. The default is 8.

Notes: Password policies can be configured to accept passwords that have a minimum value of 1 character and a maximum value of 127 characters. By default, the password length is set to 8 characters. To change system-wide password requirements, use the OnGuard Users browser-based client application. For more information, refer to the Administration Guide for OnGuard Browser-based Client Applications (DOC-6015-EN-US).

Database passwords conform to the rules of the specific database being used; passwords in SQL Server and Oracle 12 c are case-sensitive.

For Oracle databases the following account username and passwords are not allowed to be used together:

System and Manager

Internal and Oracle

Sys and Change_On_Install

Change the Database Password

In addition to user accounts and passwords, your OnGuard system has a database password. During installation, this password is typically set to `Secur1ty#`. If the database credentials were changed, they must also get updated in the Login Driver. When you log on, the application contacts the Login Driver for the username and password, allowing you to access the database.

It is highly recommended that you change the default database password. Although all the machines in an Enterprise or Distributed ID system start by using the same database password (`Secur1ty#`), the database password does not need to be the same on all machines. The procedure for changing the database password varies depending on whether the Login Driver is running on the same computer that has the database, and which options you choose to use. The SQL Server, Oracle, or SQL Server Desktop Engine password and the password in the Login Driver must be the same or you will not be able to log into any OnGuard applications.

- If the Login Driver and the database are on different computers, you have two options:
  - Change the database password, and change the password in the Login Driver manually later
  - Change both the database password and the Login Driver password at once. If you choose this option, the password will be sent over the network as plain text.

Change the Lenel Account Password

1. To change the Lenel account password using the Login Driver:
   a. Stop the LS Login Driver service, and then run it as an application.
   b. The  icon appears in the system tray. Right-click the icon, then select **Open**.
   c. The Login Driver window opens. From the ***Edit*** menu, select ***Change Password***.
2. If the password is considered weak, the database server Account Passwords window is displayed. Refer to Password Standards on page 79 to determine a secure password.
3. Click [Continue]. If you wish to change the password for a database server account now, that is, “LENEL”, select the account from the list, then click [Change Password].
   a. The Change Password window is displayed. In the **Old password** field, type your current password. For security reasons, your password is not displayed as you type it.
   b. In the **New password** field, type the new password.
   c. In the **Confirm password** field, type the new password again. Because the password can’t be seen while you type, this gives you an extra assurance that you typed it correctly.
   d. When the password is changed, it must be changed in the Login Driver and on the database server. If the Login Driver and the database server are running on the same machine, proceed to step e.

      If the Login Driver and the database server are not running on the same machine, the **When I change this password on the Login Driver, do not change the password on the database server. I will change the password manually on the database server.** check box appears in the Change Password window. (If they are on the same machine, this check box does not appear.)

      - If the check box is not selected (default), the password will be changed in both places. However, the password is sent as plain text over the network. This is the only case where the password is passed across the network in plain text when changing the password.

Note: A connection to the Login Driver is required to connect successfully to the database. The Login Driver can be run on either the database server or the license server.

- If the check box is selected, the password in the Login Driver will be changed, but you will need to change the password manually on the database server. For more information, refer to Change the Lenel Account Password on page 80.

e. Click [OK] to save the new password.

4. Exit the LS Login Driver application and restart the service.

Change the System Administrator Password for the Database

It is very important that you have a secure password for your database administrator account. For SQL Server Desktop Engine and SQL Server databases, this account is "SA." Oracle has several default administrator accounts, including INTERNAL, SYS, and SYSTEM. These passwords must be changed to a secure password if strong password enforcement is enabled. Two steps are required to change the system administration password:

Change the SYSTEM Account Password Using Database Setup

To change the SYSTEM account password using Login Driver, follow the same instructions listed in Change the Lenel Account Password on page 80, with the following exception: in step 3 of Change the Lenel Account Password on page 80, select the system account from the list ("SA" by default), then click [Change Password].

Key Points for System Account Password Change

- The system account (SA) and password should be carefully safeguarded and stored in a secure location.
- In the event that further assistance is needed, contact LenelS2 OnGuard Technical Support.
- It 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 user accounts assigned to specific users is recommended after commissioning.

Managing the Login Driver Encryption Key

The Login Driver holds the encryption key for the entire OnGuard system. This key is then used to encrypt the OnGuard database, and is distributed to all OnGuard clients in the system. A client cannot function if it does not have the encryption key that matches the key on the OnGuard server.

Note: In a clustered environment with the Login Driver residing on a clustered server, you must also update the encryption key (using the same passphrase, or import the same **.og** file) on the other node.

1. To set the OnGuard system encryption key using the Login Driver:
   a. Stop the LS Login Driver service, and then run it as an application.
   b. The  icon appears in the system tray. Right-click the icon, then select **Open**.
   c. The Login Driver window opens. From the ***Edit*** menu, select ***Manage Encryption Key***. The **Manage encryption key** dialog opens.
   d. In the Key entry options drop-down, you can select either:

- **Set with the passphrase** - Type the passphrase in the field. If you want to see the passphrase, select **Show Passphrase**.
- **Set with the file** - Click [Browse] to navigate to the file containing the encryption key.

e. Click [Apply].

2. To change your encryption key recovery preferences:
   a. From the Login Driver window, select ***Edit*** > ***Manage Encryption Key***. The **Manage encryption key** dialog opens.
   b. Select the **Emergency Key Recovery** option so that the OnGuard System software provider can help you recover the encryption key if there is a system failure. This process will create and securely store a Key Recovery String for the system that can be provided to support the recovery process. The Key Recovery String will be updated each time the Encryption Key is changed for the system.
   c. Click [Apply].

Setting Login Driver RabbitMQ Credentials

The Login Driver holds the RabbitMQ credentials.

Note: Before changing the RabbitMQ credentials for the Login Driver, you must also update the password using the RabbitMQ console tool as described in Restore Microsoft SQL Server Database Onto a Different Server on page 21.

1. To configure the RabbitMQ credentials using the Login Driver:
   a. Stop the LS Login Driver service, and then run it as an application.
   b. The  icon appears in the system tray. Right-click the icon, then select **Open**.
   c. The Login Driver window opens. From the ***Edit*** menu, select ***Set RabbitMQ LD credentials***. The **Set RabbitMQ LD credentials** dialog opens.
2. Type the RabbitMQ **Username** and **Password** into the text fields. If you want to see the password, select **Show Password**.
3. To test the workstation's connection to the RabbitMQ server, click [Test Connection].
4. Select **Allow users to re-establish connection for offline clients** if you want users to reconnect to the RabbitMQ server on their own.
5. If you only want workstations to re-connect to the RabbitMQ server without user interaction for a limited time, select **Prevent silent client reconnection after**, and then fill in the date and time you want that permission to expire.
6. Click [Apply].

Note: In a clustered environment with the Login Driver residing on a clustered server, you must also update the RabbitMQ credentials for the Login Driver on the other node.

CHAPTER 11

Maintaining the OnGuard Installation

This chapter will show you how to perform some simple maintenance to your installation.

Modify OnGuard

OnGuard can be modified by following these steps:

1. Insert the OnGuard installation media into the workstation.
2. The installation application should launch automatically. If it doesn't, browse the contents of the installation media and double-click **setup.exe**.
3. The Welcome dialog opens. Click [Next].
4. Select Modify, and then click [Next].

   The installation application lists all features available for the OnGuard software. Select the feature(s) you want to modify, and then choose either:

   - This feature will be installed on local hard drive
   - This feature, and all subfeatures, will be installed on local hard drive
   - This feature will not be available.
5. After making your choices, click [Next] and then click [Install].

Repair OnGuard

OnGuard can be repaired by following these steps:

1. Insert the OnGuard installation media into the workstation.
2. The installation wizard should launch automatically. If it doesn't, browse the contents of the installation media and double-click **setup.exe**.
3. The Welcome dialog opens. Click [Next].
4. Select Repair, and then click [Next].

5. The installation wizard provides a workstation-specific list of files you should back up before continuing the repair. Back up these files.
6. Click [OK].
7. Click [Install].
8. When the installation wizard completes, click [Finish].
9. Restore the backed-up files from step 5.

Remove OnGuard

OnGuard can be removed by following these steps:

1. In Windows:
   a. Open the ***Programs and Features*** application.
   b. In the Currently installed programs list, select **OnGuard 8.3**.
   c. Click [Remove].
2. You are asked if you are sure you want to remove the OnGuard software. If you are, click [Yes].

OnGuard Fixes and Maintenance

OnGuard Software Update

An OnGuard Software Update is a cumulative package with guided installation that resolves customer issues.

IMPORTANT: Apply a software update to all servers and workstations running the OnGuard software. If the software update is not applied to all OnGuard computers, you cannot log into the OnGuard system until the software update is applied to all computers in the OnGuard system.

To obtain a software update, go to the LenelS2 Connect™ portal at: https://connect.lenels2.com/s/downloads.

IMPORTANT: OnGuard software updates cannot be uninstalled. Before installing a software update, back up your system. For more information, refer to Chapter 3: Database Backup and Restoration on page 17.

Third-Party Service Packs and Updates

Third-party service packs and updates should only be installed after they have been fully tested with the OnGuard system. Approved updates can be found on the Supplemental Materials media. See the release notes or www.lenels2.com to see what latest updates have been approved.

Note: The Security Utility also needs to be run whenever any update to the operating system takes place.

Language Packs

Language packs are automatically installed when OnGuard is installed. Run the Database Translator utility to configure the OnGuard system to use a language pack. For more information, refer to the Language Pack User Guide (DOC-930).

Log Files

OnGuard log files are created and stored in the OnGuard folder. The default path is **C:\ProgramData\Lnl\logs**.

Note: The License Server does not create and store log files in the default OnGuard log files path. Instead, the License Server creates and stores the log file **log.xml** in **C:\Program Files (x86)\OnGuard\LicenseServerConfig**.

When you upgrade OnGuard, your current log folder is renamed to “logs.old”. Only one “logs.old” folder will ever exist. It is overwritten at every upgrade.

Log files are not truncated and regular maintenance is suggested, as files may grow rather large.

The most frequently used log files are:

- LenelError.log
- DataExchange.log
- Replicator.Log
- LnlLogError.log

Server Maintenance

Daily

- Perform routine backups of databases.
- Monitor disk and database utilization.
- Monitor CPU and bandwidth utilization.
- Repair and maintain all failed transactions in a timely manner.

Monthly

- Perform routine event archive and backup of events.
- Perform routine database maintenance (that is, SQL Server Database Maintenance Plan).
- Check all text file log sizes under the installation directory logs folder and purge as necessary.

CHAPTER 12

Troubleshooting

This chapter provides information for troubleshooting an OnGuard installation.

.DLL Errors

If you get .dll errors, the cause is usually that Microsoft .NET Framework or Microsoft Visual C++ 20## Redistributable did not install.

To fix this issue, download these installers from Microsoft, and then run the installers as an administrator.

Cannot Create File In Windows Directory Errors

If you get an error similar to:

```
Cannot create file "C:\Windows\Fonts\[font name]". Access is denied.
```

...the cause is that you do not have sufficient read and write permissions to the Windows directory. Get full read/write permissions to the Windows directory, and then repeat the OnGuard installation.

1152 Error

If you get the error:

```
1152: Error Extracting Microsoft Visual C++ 20## Redistributable
Package (x86).prq to the temporary location.
```

...the cause is that the Temp directory (commonly **%USERPROFILE%\AppData\Local\Temp**) was deleted from the workstation. All Microsoft prerequisites, including Microsoft Visual C++ 20##, use this directory to extract their installation files. Re-create this directory, and then repeat the OnGuard installation.

Database Encryption Errors

OnGuard Database is in Single User Mode

If the database encryption process is interrupted while running Database Setup, the OnGuard SQL database might remain in Single User mode. You can confirm that the database is in Single User mode by looking at the database list in SQL Management Studio. If "(Single User)" is shown after the database name, then the database is in Single User mode.

To correct this problem:

1. Open SQL Server Management and log into the SQL database server. If the database encryption process is not running, you can edit the database properties.
2. Select the database, then open the **Options** page.
3. In the **State** options, change the **Restrict Access** option from **SINGLE_USER** to **MULTI_USER**.

If the database encryption process is still running, the only way to change the Restrict Access option is by running the following SQL script on the database server while connected to any database other than AccessControl (this example assumes the OnGuard database name is **AccessControl**):

```
alter database AccessControl set multi_user
```

Note: The operation will fail if you run this script while connected to the AccessControl database.

Appendices

APPENDIX A

Configuration Editor

OnGuard database connection and License Server configuration information is stored in two files:

- **ACS.INI**
- **application.config**

The Configuration Editor provides a user interface that makes configuration and maintenance of these files fast and easy.

IMPORTANT: If the Reporting and Dashboards feature is installed on the server, the Configuration Editor uses the information contained in the **ACS.INI** and **application.config** files to configure the contents of the **C:\Program Files\JReport\Server\bin\dbconfig.xml** file. Editing the **ACS.INI** or **application.config** files manually is not advised. If you manually edit these files instead of using the Configuration Editor, the **dbconfig.xml** file might not be configured correctly, resulting in unexpected system behavior.

The stand-alone Configuration Editor application also provides advanced functions, such as Windows authentication, verbose logging, and browser-based client reporting configuration.

The Setup Assistant contains a Configuration Editor module that provides database and License Server connection information, but does not allow the advanced configuration options found in the stand-alone application.

When Configuration Editor Identifies an Issue

There are three situations in which the Configuration Editor will identify an issue that must be resolved:

- The database and license configuration is not consistent between the **application.config** and **ACS.INI** files (stand-alone version of Configuration Editor and Setup Assistant module)
- Setup Assistant cannot locate the database (Setup Assistant module only)
- Setup Assistant cannot locate the License Server (Setup Assistant module only)

The **ACS.INI** and **application.config** files must always point to the Live database, not the Archival database. For more information, refer to the *Archives Folder* chapter in the *System Administration User Guide*.

Launching the Configuration Editor Stand-alone Application

Launch the OnGuard Configuration Editor.

Notes: To use the Configuration Editor, you must have write access to the registry, **ACS.INI** file, **application.config** file.

The **ACS.INI** file is located in the **C:\Windows** directory.

The **application.config** file is located in the **C:\Users\<user name>OnGuard\CommonAppData\Lnl** directory.

For Windows 11 and later, the a**pplication.config** file is located in the **C:\Program Data\Lnl** directory. By default, the **Program Data** directory is hidden in Windows.

The Configuration Editor application opens, and then checks the configuration of the **ACS.INI** and **application.config** files. If there is a configuration issue, the Configuration Editor highlights the discrepancy.

Standard Fields and Buttons

The following sections describe the standard Configuration Editor fields and buttons.

Save Changes

Click [Save Changes] to save and synchronize your changes across the affected OnGuard configuration files.

Note: [Save Changes] only becomes active after the user completes all of the Database and License information, and provides a valid DSN name.

Revert

Click [Revert] to return your changes to their previous values.

Show advanced settings

Select **Show advanced settings** to show the advanced sections of the Configuration Editor user interface. For more information, refer to Advanced Settings Fields and Buttons on page 93.

Database section

Database type

Identifies if the database type is **SQL Server** or **Oracle**. This information is view only.

DSN name

The Lenel Data Source Name, as defined in the ODBC configuration.

Server name
The name of the server hosting the database.

Database name
The name of the database (default for a SQL Server database is **AccessControl**).

License Server section

Server name
The name of the server hosting the License Server.

Server port
The port the server is using to host the License Server.

Advanced Settings Fields and Buttons

The following sections describe the advanced Configuration Editor fields and buttons.

Advanced Database section

Windows authentication
When selected, the **application.config** uses the user's Windows user name and password when connecting to the database. This check box is selected by default.

When deselected, the Configuration Editor provides the **User name** and **Password** fields into which you can enter the credential information required when connecting to the database. Select **Show password** if you want the password to be readable within the Configuration Editor user interface.

Notes: When the **Windows authentication** check box is deselected, the credential information is saved as plain text in the application.config file. Make sure the **application.config** file is secured. For more information, refer to Provide Credentials in the Protected File on page 68.

The **ACS.INI** file requires the LS Login Driver, and requires this credential information.

Store Password Encrypted
Select this checkbox if you want to encrypt the database password in the **application.config** file, then provide a password that meets the password requirements. When you click [Save changes], a new **EncryptedDBPassword** key is added to **application.config**.

Note: If your OnGuard installation has a Custom Solution that relies on the database password being in plain text, you must update that Custom Solution with a different method for retrieving the database password.

Advanced Verbose Logging section

Use the following check boxes to enable enhanced logging when troubleshooting OnGuard issues.

Setup Assistant

Enables verbose logging for Setup Assistant. Selecting this check box automatically selects the **Form Translator** and **Database Setup** check boxes because they are also Setup Assistant modules.

Form Translator

Enables verbose logging for Form Translator.

Database Setup

Enables verbose logging for Database Setup. This check box is only available if Database Setup is installed.

LS DataConduIT Service

Enables verbose logging for DataConduIT. You must restart the LS DataConduIT service after selecting this check box. This check box is only available if DataConduIt is installed.

LS Site Publication Server

Enables verbose logging for the Site Publication Server. You must restart the LS Site Publication Server service after selecting this check box. This check box is only available if the Site Publication Server is installed.

LS OpenAccess

Enables verbose logging for OpenAccess.

Alternative SQL Authentication Methods

This section describes methods of performing database authentication other than the default SQL password and username.

Azure Service Principal

Perform the following procedure to implement the Azure Service Principal method of database authentication:

1. Create a new valid ODBC connection, or update current one.
2. Run Configuration Editor to update the **application.config** file by providing the following information in the **Database** section of Configuration Editor.

   #### Principal ID

   The Azure Service Principal **Client ID**.

   #### Authentication method

   To implement Azure Service Principal, select **Active Directory Service Principal**.

   #### Secret

   The Azure Service Principal **Secret**.
3. Run Login Driver run as an application, and replace the database user name with the Principal ID, and replace the password with the Secret.

Note: Ensure you have your Azure Service Principal configured as the user in the AccessControl, AccessControl_ReportsConfig, and Archival databases.

Fixing Synchronization Issues

If the Configuration Editor detects a synchronization issue between the **application.config** and **ACS.INI** files, it highlights the issue.

1. Use the **Correct file** drop-down menu to select which file is correct.
2. If necessary, click [Select] to select the correct DSN name.
3. Click [Save Changes] to synchronize the application.config and **ACS.INI** files.

APPENDIX B

Custom Installation of OnGuard

Performing a custom installation allows you to install as few or as many OnGuard features and applications as you wish.

Performing a Custom Installation

First Time and Existing OnGuard Installation

1. Begin installing the OnGuard software. For more information, refer to Chapter 6: Installing OnGuard 8.3 on page 41.
2. During the installation you are prompted to choose the system type. Select **Custom Install**.
3. You will be prompted with the custom setup screen. Choose which features to install.
4. Continue with the installation by following the installation steps.

Device Discovery Console

This feature enables the discovery and maintenance of devices on a network or system.

APPENDIX C

Using OnGuard on Supported Operating Systems

This appendix contains procedures, paths to applications and services, and other items pertaining to OnGuard and its supported operating systems.

Using OnGuard on Windows 11

This section contains procedures, paths to applications and services, and other items pertaining to OnGuard and Windows.

Locating OnGuard Applications and Services

Refer to the following table to locate the desired OnGuard application or service in Windows 11.

Note: In the following table, "Start" refers to the ***Start*** screen in Windows 11. Some scrolling may be required to find the application icons on the Start screen.

Application/Service	Path
Communication Server	***Start > Communication Server***
Configuration Editor	***Start > Configuration Editor***
Database Setup	***Start > Database Setup***
Database Translation Utility	***Start > Database Translation Utility***
FormsDesigner	***Start > FormsDesigner***
Global Output Server	***Start > Global Output Server***
Import Utility	***Start > Import***
License Administration	***Start > License Administration***
License Server	***Start > License Server***

Application/Service	Path
Linkage Server	***Start > Linkage Server***
Login Driver	***Start > Login Driver***
MapDesigner	***Start > MapDesigner***
Replicator	***Start > Replicator***
Security Utility	***Start > Security Utility***
Setup Assistant	***Start > Setup Assistant***
Site Publication Server (Enterprise only)	***Start > Site Publication Server***
System Management Console	***Start > System Management Console***
Universal Time Conversion Utility	***Start > Universal Time Conversion Utility***
Video Archive Server	***Start > Video Archive Server***

Locating Operating System Applications

Refer to the following table to locate the desired operating system application in Windows 11.

Notes: In the following table, "Start" refers to the ***Start*** screen in Windows 11.

For faster results, use the ***Search*** field to find the location of any operating system application.

Application	Path
Administrative Tools	***Control Panel > Administrative Tools***
Citrix Studio	***Start > All apps > Citrix > Citrix Studio***
Command Prompt	***Start > All apps > Windows System > Command Prompt***
Component Services	***Start > All apps > Control Panel > Administrative Tools > Component Services***
Control Panel	***Windows Key + [X] Quick Link Menu > Control Panel***
Devices and Printers	***Start > All apps > Control Panel > Devices and Printers***
Failover Cluster Manager	***Start > All apps > Administrative Tools > Failover Cluster Manager***
File History	***Start > All apps > Control Panel > System and Security > File History***
License Manager	***Start > All apps >NEC ExpressCluster Server > License Manager***
NEC ExpressCluster Server	***Start > All apps > NEC ExpressCluster Server***
Network and Sharing Center	***Start > All apps > Control Panel > Network and Sharing Center***

Application	Path
Phone and Modem	***Start > All apps > Control Panel > Phone and Modem***
Programs and Features	***Start > All apps > Control Panel > Programs > Programs and Features***
Region and Language	***Start > All apps > Control Panel > Region and Language***
Run	***Start > All apps > Run***
Server Manager	***Start > All apps > Administrative Tools > Server Manager***
SQL Server Management Studio	***Start > All apps > SQL Server Management Studio***
Task Scheduler	***Start > Settings > Task Scheduler***
Touch-It Virtual Keyboard	***Start > Touch-It Virtual Keyboard***

Using OnGuard with Windows Server

This section contains procedures, paths to applications and services, and other items pertaining to OnGuard and Windows Server.

Note: Instructions may differ depending on the currently supported version of the Windows Server system.

Locating OnGuard Applications and Services in Windows Server

Refer to the following table to locate the desired OnGuard application or service in Windows Server.

Note: In the following table, "Start" refers to the ***Start*** screen in Windows Server.

Application/Service	Path
Communication Server	***Start > Service and Support > Communication Server***
Configuration Editor	***Start > Service and Support > Configuration Editor***
Database Setup	***Start > Service and Support > Database Setup***
Database Translation Utility	***Start > Database Translation Utility > Database Translation Utility***
FormsDesigner	***Start > System Tools > FormsDesigner***
Global Output Server	***Start > Global Output Server***
Import Utility	***Start > Service and Support > Import***
License Administration	***Start > License Administration***
License Server	***Start > Service and Support > License Server***
Linkage Server	***Start > Linkage Server***

Application/Service	Path
Login Driver	***Start > Service and Support > Login Driver***
MapDesigner	***Start > System Tools > MapDesigner***
Replicator	***Start > System Tools > Replicator***
Security Utility	***Start > System Tools > Security Utility***
Setup Assistant	***Start > Service and Support > Setup Assistant***
Site Publication Server (Enterprise only)	Start > Site Publication Server
System Management Console	***Start > System Management Console***
Universal Time Conversion Utility	***Start > Service and Support > Universal Time Conversion Utility***
Video Archive Server	***Start > Service and Support > Video Archive Server***

Locating Operating System Applications in Windows Server

Refer to the following table to locate the desired operating system application in Windows Server.

Notes: To launch the ***Start*** screen in Windows Server, press ***Ctrl+Esc***.

For faster results, use the ***Search*** field to find the location of any operating system application.

Application	Path
Administrative Tools	***Start > Apps > Administrative Tools > Services***
Citrix Director	***Start > Apps > Citrix > Citrix Director***
Citrix License Administration Console	***Start > Apps > Citrix > Citrix License Administration Console***
Citrix Scout	***Start > Apps > Citrix > Citrix Scout***
Citrix Simple License Service	***Start > Apps > Citrix > Citrix Simple License Service***
Citrix StoreFront	***Start > Apps > Citrix > Citrix StoreFront***
Citrix Studio	***Start > Apps > Citrix > Citrix Studio***
Command Prompt	***Start > Apps > Command Prompt***
Component Services	***Start > Control Panel > Administrative Tools > Component Services***
Control Panel	***Start > Control Panel***
Devices and Printers	***Start > Control Panel > Devices and Printers***
Failover Cluster Manager	***Start > Control Panel > Administrative Tools > Failover Cluster Manager***

Application	Path
License Manager	***Start > Apps >NEC ExpressCluster Server > License Manager***
NEC ExpressCluster Server	***Start > Control Panel > NEC ExpressCluster Server***
Network and Sharing Center	***Start > Control Panel > Network and Sharing Center***
Phone and Modem	***Start > Control Panel > Phone and Modem***
Programs and Features	***Start > Control Panel > Programs > Programs and Features***
Region and Language	***Start > Control Panel > Region and Language***
Run	***Start > Apps > Run***
Server Manager	***Start > Apps > Administrative Tools > Server Manager***
SQL Server Management Studio	***Start > Apps > SQL Server Management Studio***
Task Scheduler	***Start > Control Panel > System and Maintenance > Administrative Tools > Task Scheduler***
Touch-It Virtual Keyboard	***Start > Touch-It Virtual Keyboard***
Windows Server Backup	***Start > Control Panel > Admin Tools > Windows Server Backup***

APPENDIX D

OnGuard and the Use of Certificates

This appendix describes configuration and use information for setting up certificates with OnGuard, which is also useful when troubleshooting certificate issues.

General Description

Transport Layer Security (TLS) certificates, also known as Secure Socket Layer (SSL) certificates, are installed on web servers (either automatically when OnGuard is installed, or manually) and clients to create a secure encrypted connection between the server and the client. The private certificate is installed on the server, and the public certificate is sent to the client when the secure connection is initiated. The client uses the public certificate to verify the server's identity.

Any client or service that communicates with the LS Message Broker service is secured by TLS, such as: LS Site Publication Server service used in an OnGuard Enterprise installation, LS OpenAccess, and more. TLS is also used by clients of NGINX, such as OnGuard Monitor, OnGuard Credentials, LenelS2 Console, and more.

Where to Get Certificates

You have two options for getting certificates:

- From a trusted Certificate Authority. You can use whichever Certificate Authority you prefer. Certificates typically expire in 1 to 3 years.
- Use a self-signed certificate. When OnGuard is installed or upgraded, a self-signed certificate is installed by default. Certificate will expire in 3 years.

Note: Certificates have expiration dates. You must renew your certificates before they expire to maintain secure connectivity. If you allow your certificates to expire, data exchanged between your server and your clients will not be secure, and in some cases will fail. Web application users might lose access to the application or receive warnings. Starting with OnGuard 8.1, LenelS2 self-signed certificates have a 3-year expiration to align with security expectations in the industry (in prior versions, 10+ year certificates were used).

OnGuard uses self-signed certificates by default to facilitate installation and setup. This usage is designed primarily for support of evaluation and demonstration environments, as well as stand-alone systems not expected to have public access. Self-signed SSL certificates are used to encrypt communication, but when used in a browser-based environment, they cause the display of a security alert in the address bar of the browser. This is because the certificate could not be verified by a trusted Certificate Authority. Browsers also generally provide for an “acceptance” on the part of the user to indicate understanding that this trust does not exist.

Some organizations consider self-signed certificates acceptable for internal sites and would advise their users to ignore the browser warnings, but this can encourage bad browsing habits in their users that could create consequences on an internal site. A public certificate establishes trust and provides a path for revocations should the trusted certificate be compromised.

The other value of using a Certificate Authority-assigned certificate is that an organization can revoke the certificate after discovering it has been compromised. An organization cannot revoke a self-signed certificate. Instead the organization must replace or rotate that certificate. This inability to rapidly revoke a compromised private key associated with a self-signed certificate can allow malicious attacks.

Certificate Management

If the following OnGuard components are all installed on the same server, they will utilize the same certificate. If they are installed on different servers, then each server will require its own unique certificate.

- LS Web Server (NGINX)
- LS Message Broker Service (RabbitMQ)

Viewing the Existing Certificate

To configure where certificates are installed, refer to Configure the Name and Location of the Certificate on page 107. To install a custom certificate, refer to *For OnGuard 7.6:* on page 107.

Installing a Certificate Manually

Notes: If you are re-issuing a certificate, you should delete all existing certificates.

To ensure live events work on mobile devices, you must install a trusted certificate on the OnGuard server (the machine where the OpenAccess service is running).

After making any certificate change, restart the LS Web Service and the LS Message Broker service.

Installing a self-signed certificate. OnGuard installs a self-signed certificate by default. In some cases the default certificate might not match the server name, such as in a virtual or cluster environment, or when the server is in a workgroup or not connected to any domain.

Run the following command manually to reissue the certificate with the correct server name, placing the certificate in the **nginx\conf** directory for the web server. The server name is “server” in the following sample code:

For OnGuard 8.0 and later:

```
<OnGuard installation directory>\Certificates\
lnl_app_server_certificate_installer.exe -
key=C:\ProgramData\Lnl\nginx\conf\ls_server_cert_key.pem -
cert=C:\ProgramData\Lnl\nginx\conf\ls_server_cert.pem -
keystore="C:\Program Files (x86)\OnGuard\LicenseServerConfig" -
cn=<virtual computer name>
```

For OnGuard 7.6:

```
<OnGuard installation directory>\Certificates\
lnl_app_server_certificate_installer.exe -
key=C:\ProgramData\Lnl\nginx\conf\ls_server_cert_key.pem -
cert=C:\ProgramData\Lnl\nginx\conf\ls_server_cert.pem -
cn=<virtualcomputer name>
```

Import a custom certificate. Follow the instructions provided by the trusted Certificate Authority to first generate a Certificate Signing Request (CSR). Once the certificate is issued by the Certificate Authority, install the certificate and key onto the NGINX/LS Web Server by following the instructions provided by the Certificate Authority for the NGINX Web Server. If your private key is encrypted, you must either configure NGINX and RabbitMQ with the appropriate passphrase, or alternatively decrypt your private key and then configure NGINX and RabbitMQ to not require a passphrase.

Decrypt a private key file. An encrypted key file will have a header containing the text "BEGIN ENCRYPTED PRIVATE KEY" and "END ENCRYPTED PRIVATE KEY." To decrypt an encrypted private key file named **key.pem** and store the decrypted key in a file named **server.key**, run the **openssl** command as follows:

```
openssl rsa -in key.pem -out server.key
```

LS Web Server (NGINX)

Configure the Name and Location of the Certificate

Note: The default location of the certificate for NGINX is **C:\ProgramData\Lnl\nginx\conf**.

Locate the following lines in the **C:\ProgramData\Lnl\nginx\conf\nginx.conf** file:

```
ssl_certificate      ls_server_cert.pem;
ssl_certificate_key  ls_server_cert_key.pem;
```

These lines identify where NGINX expects to find the certificate files. The **ls_server_cert.pem** file is the public key, and the **ls_server_cert_key.pem** file is the private key. If your certificate authority requires the use of an intermediate certificate, you must concatenate the server certificate and the intermediate certificate together to create the **ls_server_cert_key.pem** file. The server certificate must be first and the intermediate certificate must follow it.

Optional: If the private key is encrypted, add the following line to the **C:\ProgramData\Lnl\nginx\conf\nginx.config** file after the `ssl_certificate_key` line above:

```
ssl_password_file      ls_server_cert_key.pass;
```

This line identifies where NGINX expects to find the passphrase for the encrypted private key file that was specified earlier using the **ssl_certificate_key** parameter. For example, the passphrase for

the key file should be added as a line of plain text in the file **ls_server_cert_key.pass** to configure NGINX to be able to decrypt the encrypted private key file.

IMPORTANT: This process must be repeated if the OnGuard installation is reinstalled or upgraded.

IMPORTANT: Never share the key file. Doing so can compromise your TLS security.

LS Message Broker Service (RabbitMQ)

Note: When editing a **.config** file or **.ini** file using the examples provided, remove characters such as quotation marks (“”) or carrots (< >) to ensure the action executes as expected. Quotation marks are required if they surround a file path that has spaces in it.

By default, the LS Message Broker Service uses the same certificate as the LS Web Service (NGINX).

If required, you can change the location of where the LS Message Broker Service (RabbitMQ) will find its certificate:

1. Open the **C:\Users\<username>\AppData\Roaming\RabbitMQ\advanced.config** file in a text editor.
2. Locate and update the following section, while also following the existing formatting:

```
{ssl_options, [{cacertfile,"C:\\Program Files
(x86)\\OnGuard\\Certificates\\ca.cer"},
{certfile,"C:\\ProgramData\\Lnl\\nginx\\conf\\ls_server_cert.pem"},
{keyfile,"C:\\ProgramData\\Lnl\\nginx\\conf\\ls_server_cert_key.pem"},
{verify,verify_peer},
{fail_if_no_peer_cert,false}]
}
```

Optional: If the private key is encrypted, add the following line to the **C:\Users\<username>\AppData\Roaming\RabbitMQ\advanced.config** file after the `keyfile` line above:

```
{password, "passphrase"},
```

Performing Peer Verification on Clients Connecting to LS Message Broker Server

Note: When editing a **.config** file or **.ini** file using the examples provided, remove characters such as quotation marks (“”) or carrots (< >) to ensure the action executes as expected. Quotation marks are required if they surround a file path that has spaces in it.

You can configure the LS Message Broker server to perform peer verification, rejecting clients that do not provide a valid certificate. To configure peer verification:

1. Open the **C:\Users\<username>\AppData\Roaming\RabbitMQ\advanced.config** file in a text editor.
2. Add or modify the file to include these two lines:

```
{verify, verify_peer},
{fail_if_no_peer_cert, true}
```

3. Add to the **acs.ini** file:

```
[LSMessageBrokerClientSecurity]
CertificatePath=<"path to client-side certificate">
```

4. On every OnGuard client and server machine in your system (or within a Region, if it's an Enterprise system), add to the **acs.ini** file:

```
[LSMessageBrokerClientSecurity]
CertificatePath=<"path to client-side certificate">
```

5. Modify configuration files for all applications using TLS to add the following XML section. This must be performed on every client machine.

• *WARNING!* • Modifying these files incorrectly might cause OnGuard to malfunction.

   a. Open the file in a text editor.

   b. Navigate to the appSettings element:

```
<?xml version="1.0"?>
<configuration>
   <appSettings>
```

   c. Add the following line:

```
<add key="X509CertPath" value="path/to/client/cert/cert.p12"/
>
```

   The resulting XML should look similar to this:

```
<?xml version="1.0"?>
<configuration>
   <appSettings>
   ... some existing data ...
   <add key="X509CertPath" value="path/to/client/cert/
   cert.p12"/>
   ... some existing data ...
   </appSettings>
</configuration>
```

   The files affected by this change are:

   - Lnl.OG.EventContextProviderService.exe.config
   - Lnl.OG.Replicator.Service.exe.config
   - Lnl.OG.WebEventBridgeService.exe.config

Notes: Client-side certificates must be in .p12 file format. The OnGuard server does not accept other formats.

Additionally, client-side certificates must be decrypted. There is no place to store an encrypted certificate's passphrase.

To learn more about configuring peer verification and other advanced details, go to https://www.rabbitmq.com/ssl.html#peer-verification.

Apple Wallet Certificates

Visitors who receive a visit notification email on an Apple (iOS) device that supports the Apple Wallet app can add this pass to the Apple Wallet on that device by clicking the attachment in the email and selecting the [Add] button when the pass is displayed. After adding the pass to the Apple Wallet, a card is shown in Apple Wallet containing information about the visit, including a barcode that can be scanned when the visitor arrives for the visit.

To take advantage of this functionality, some certificate management is required on the part of the OnGuard administrator:

1. To generate Apple Wallet passes, obtain certificates from the Apple Developer portal located at:
   http://developer.apple.com/account

Note: You must create an Apple Developer account before obtaining these certificates.

2. Download the Apple Wallet Intermediate CA certificate **AppleWWDRCA.cer**.
3. Generate a pass signing certificate for your organization (**<*YourCertificateName*>.*p12***). This certificate will contain a specific:
   - Team identifier
   - Pass type identifier

   This pass should be named in the format **pass.com.<*your organization domain*>.OnGuard-Visitor**.
4. Install the new certificates into your certificate store:
   a. Install **AppleWWDRCA.cer** into the Local Machine certificate store, in the Intermediate Certificate Authorities store.
   b. Right-click on the Apple certificate, select Open and then select the **Details** tab.
   c. Select the **Thumbprint** for the Apple certificate and then copy the thumbprint's value. You will paste this thumbprint value later in the **ACS.ini** file.
   d. Install the organization-specific certificate you generated earlier (**<*YourCertificateName*>.*p12***) into the local machine's Personal Certificates store.

Note: When importing the certificate, enable the *Mark this key as exportable* option.

   e. Right-click on the Apple Pass certificate, select Open and then select the **Details** tab.
   f. Select the **Thumbprint** for the Apple certificate and then copy the thumbprint's value. You will paste this thumbprint value later in the **ACS.ini** file.

To configure visit notification emails with Apple Wallet support, refer to "Configure Apple Wallet Support in Visit Notification Emails" in the *Visitor Management User Guide*.

HTTPS Support for the License Server

This section provides instructions to do the following:

- Disable HTTPS for License Administration if needed (enabled by default)
- Generate self-signed CA certificates as needed

The **ACS.ini** file has new parameters for the `[LicenseServer]` block:

- **SSLEnabled:** By default, this parameter is set to **TRUE** (server runs HTTPS). To run the server on HTTP, set this parameter to **FALSE**.
- **ssl_certificate:** This parameter specifies the file path where the SSL certificate .pem file is stored. The default path is ***C:\ProgramData\Lnl\nginx\conf\ls_server_cert.pem***.
- **ssl_certificate_key:** This parameter specifies the file path where the key to the SSL certificate .pem file is stored. The default path is ***C:\ProgramData\Lnl\nginx\conf\ls_server_cert_key.pem***.
- **SSLProtocol:** This parameter accepts the following values: **TLSv1.2** or **TLSv1.3**. The default value is **TLSv1.2**.

Note: The `[LicenseServer]` block parameters are not required to use the default self-signed certificates that come with the OnGuard software. These parameters are required to use CA-signed certificates.

APPENDIX E

OnGuard Reporting and Dashboards

This appendix describes any necessary installation and configuration of the server for OnGuard Reporting and Dashboards beyond the installation of the OnGuard software.

General Description

OnGuard Reporting and Dashboards is a reporting engine that enables browser-based report execution and scheduling on a variety of platforms, including desktop and mobile (included in OnGuard 8.0 and higher). An optional "OnGuard Advanced Reporting" license allows customization of reports and dashboards. OnGuard Reporting and Dashboards provides a new set of reports that complement and extend the reports already provided in OnGuard, and allows graphical dashboards to be embedded in LenelS2 Console.

Required Configurations for OnGuard Reporting and Dashboards

Use of SQL Server with OnGuard Reporting and Dashboards (8.0 and forward), requires SQL Server Configuration to have TCP/IP network protocol as ENABLED prior to installation of the OnGuard software.

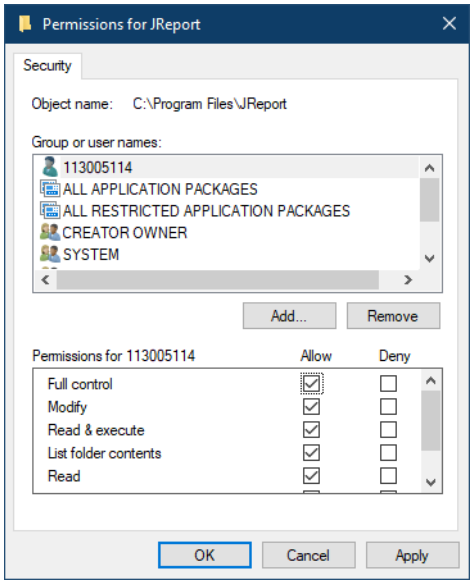
For more information, refer to Required Installations and Configurations on page 13.

Backing up OnGuard Reporting and Dashboards

For more information on backing up and restoring the OnGuard database and the database, report history and custom reports for OnGuard Reporting and Dashboards, refer to Database Backup and Restoration on page 17.

Permissions for Log On As Windows User Account

OnGuard Reporting and Dashboards requires that the Windows Log On As user account has full access to ***C:\Program Files\JReport***.



If this user account has read-only access, then the LS Reporting service will not work as expected and errors will occur.

Modifying Web Reports and Dashboards

In order to modify a web report or a dashboard, the **OnGuard Advanced Reporting (SWG-OAR-xxx)** license bit must be enabled (set to **true**) in ***License Administration > General***. When this bit is enabled, the **Modify** option in ***System Administration > Administration > Users > Report Permission Groups > OnGuard Reporting & Dashboards*** is also enabled. Users will have full access to modify web reports and dashboards as needed.

If the **Reporting and Dashboards** license bit is enabled and the **OnGuard Advanced Reporting (SWG-OAR-xxx)** license bit is disabled (set to **false**), then the user can only access and view web reports and dashboards, but cannot modify them.

Running OnGuard Reporting and Dashboards from an Alternate Server

By default, OnGuard Reporting and Dashboards is installed on the same machine that OnGuard and OpenAccess are installed on. Perform the following steps if you want to run OnGuard Reporting and Dashboards from a server (referred to as “Server 2” in the following steps) other than the server already running OnGuard and OpenAccess (referred to as “Server 1” in the following steps):

1. On Server 1, stop the LS Reporting service.

Perform the following steps if you want to run OnGuard Reporting and Dashboards on an alternate server.

1. On Server 1:
   a. In System Administration, go to ***Administration > System Options > General System Options***. In the **Reports and Dashboards Server Host** field, browse to the location of the new server host, or enter its fully qualified domain name (FQDN).
   b. Run Setup Assistant. Confirm that the LS Reporting service is stopped and set to manual.
2. On Server 2:
   a. Run Setup Assistant.
   b. Confirm that the LS Reporting service starts as expected. If it does not start, restart Server 2, wait approximately five (5) minutes after the restart, and check the status of the LS Reporting service again.
3. On Server 1, go to ***C:\ProgramData\Lnl\nginx\conf\modules\reports.conf*** and confirm that the file points to Server 2 (<NEW_REPORTS_SERVER>):

```
location /reports {
    if ( $request_uri = "/reports/jinfonet/welcome.jsp" ) {
        return 301 /;
    }

    proxy_pass http://<NEW_REPORTS_SERVER>:8888;
}
location /vt/ {
    proxy_pass http://<NEW_REPORTS_SERVER>:8888;
    add_header Cache-Control private;
}
```

   If Server 2 is not referenced as shown above, edit the **reports.conf** file accordingly.
4. To continue using any custom reports that existed on Server 1, copy the ***C:\Program Files\JReport\Server\history*** and ***C:\Program Files\JReport\Server\realm\defaultRealm*** directories and its contents from Server 1 to the same location on Server 2.

Running OnGuard Reporting and Dashboards on a System with LS OpenAccess and LS Web Service on Different Servers

In a typical installation, the LS Web Service runs on the same server that runs the LS OpenAccess service. Perform the following steps if you want to run OnGuard Reporting and Dashboards on a system with the LS Web Service running on a different server than the LS OpenAccess service. For the following steps, Server 1 is running the LS OpenAccess service, and Server 2 is running the LS Web Service:

1. On Server 1, modify the **application.config** file with the following line:

   ```
   <add key="WebService" value="hostname.domain.com:8080" />
   ```

2. On Server 1, modify the **appSetting** section of the **application.config** file similarly to the following:

   ```
   <appSettings>
      <add key="ApplicationServerUri" value="http://localhost:9111/
      Lnl/ApplicationServer.rem"></add>
      <add key="SkipSchemaGeneration" value="True"></add>
      <add key="ReportTemporaryFilePath"
      value="C:\Temp\LnlWebServiceReports\"></add>
      <!-- Path where the temporary Crystal Report files will be
      generated when running a report. The user that the Web Service
      is running under will need ability to create and delete files
      in this directory. -->
      <add key="ConnectionString" value="Data
      Source=computer_name;Initial Catalog=AccessControl;Integrated
      Security=True"></add>
      <add value="" key="CustomDatabaseType"></add>
      <add key="DatabaseType" value="SqlServer"></add>
      <add value="computer_name"
      key="Lnl.LicenseSystem.Client.Host"></add>
      <add value="8189" key="Lnl.LicenseSystem.Client.Port"></add>
      <add key="SRConnectionString" value="Data Source=C:\Program
      Files (x86)\OnGuard\DBSetup\SR.db"></add>
      <add key="SchemaOwner" value="dbo"></add>
      <add key="DebugFormXml" value="false" />
      <add key="WebService" value="computer_name:8080" />
   </appSettings>
   ```

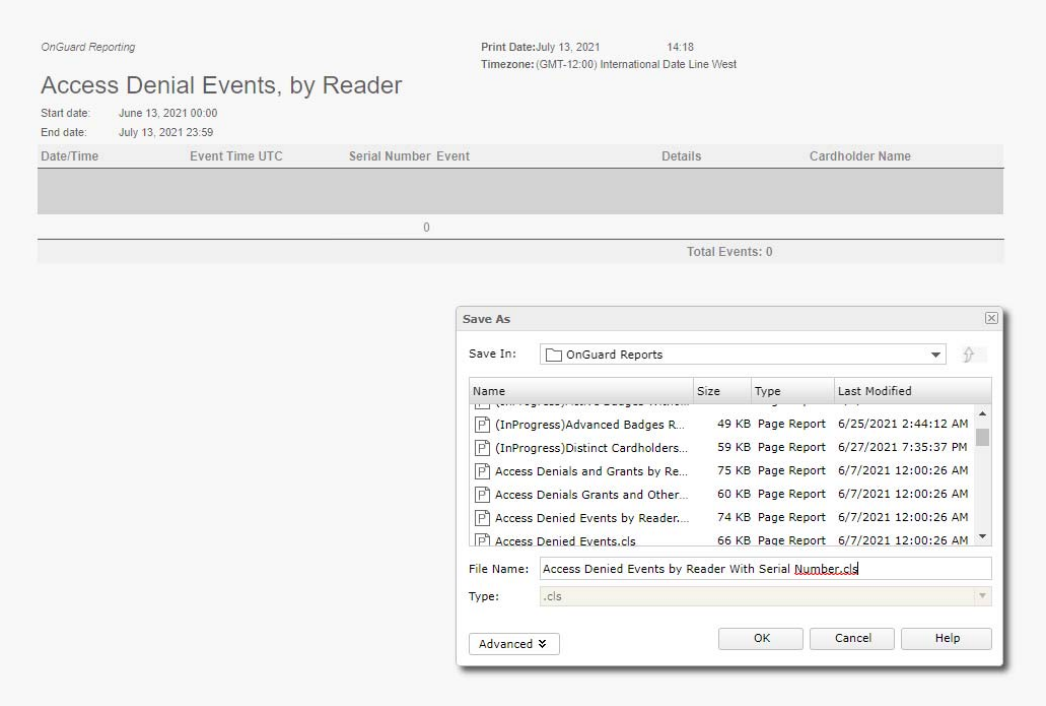
Note: You can change the LS Web Service's port number from 8080 to another port number, if necessary.

Copying Custom Reports between Enterprise Regions

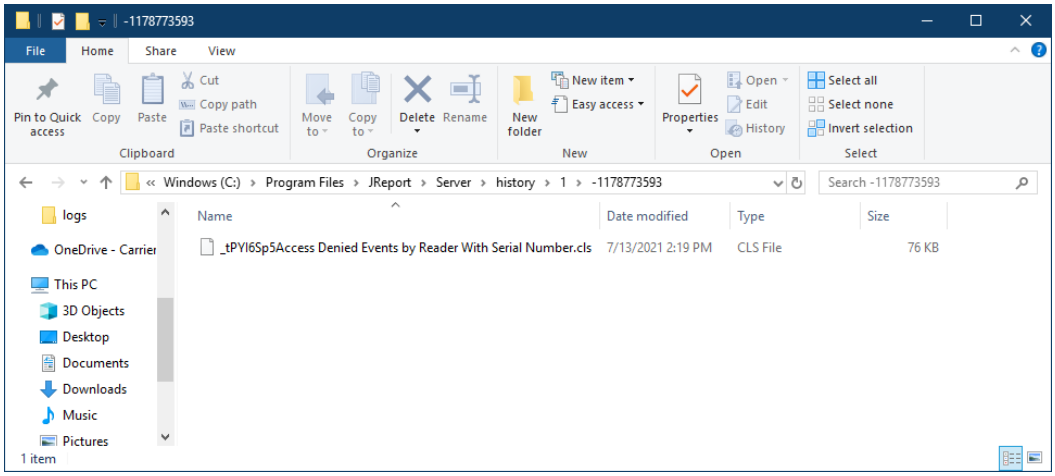
Note: Copying custom reports is only supported on an OnGuard Enterprise system. Custom reports cannot be copied from one non-Enterprise system to another.

To copy custom reports from one Enterprise region to another (for example, Region A and Region B):

1. From OnGuard Reporting and Dashboards on Region A, create a custom report by saving a copy (**Save As**) of an existing report.



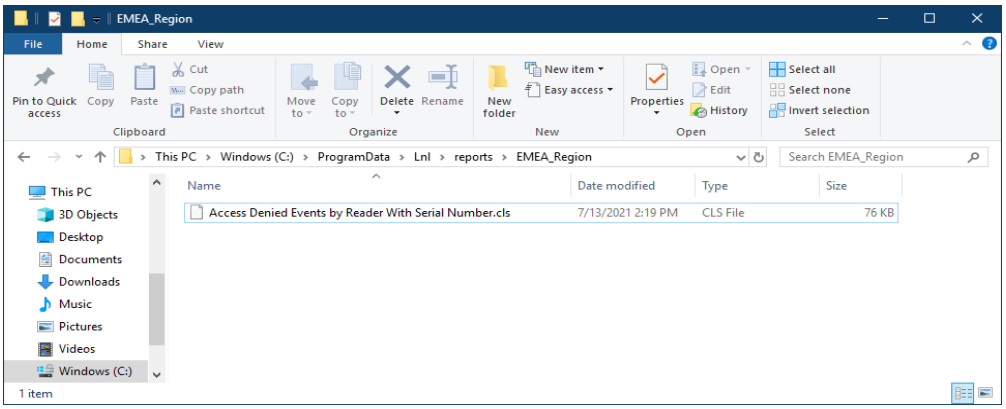
2. Locate the new report in ***C:\Program Files\JReport\Server\history\1***. It will look similar to the following:



3. Upload the new report to a dedicated folder on Region B such as ***C:\ProgramData\Lnl\reports\<regional folder>***.

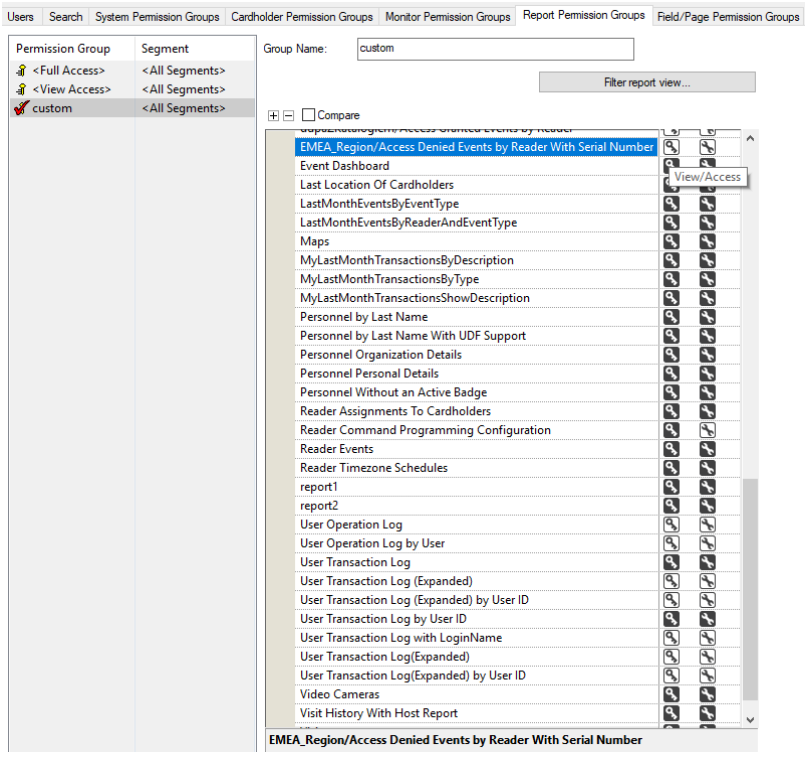
Note: Make sure that there are no catalog files (***.cat** or ***.cat.xml**) in the dedicated folder before running Setup Assistant.

4. Rename the report file by removing the prefix.



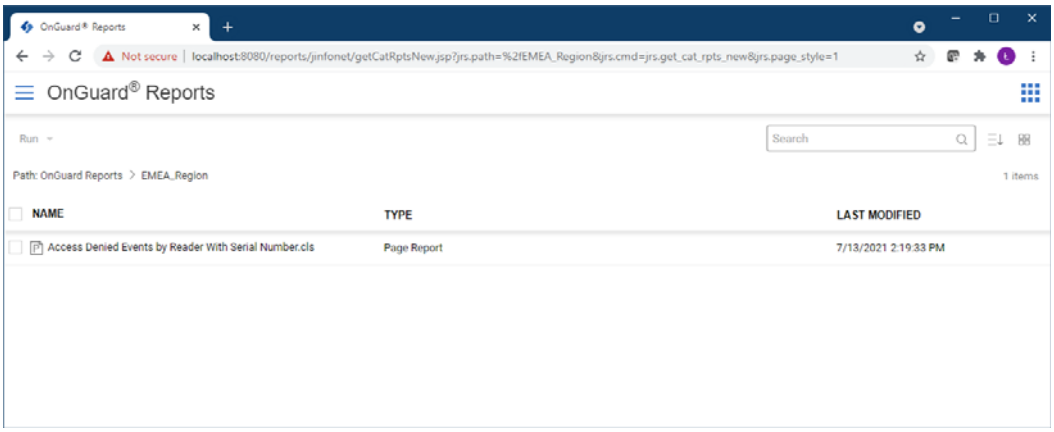
5. Run Setup Assistant.
6. Log out of LenelS2 Console and the log back in.
7. To create permissions for the new report, log out of OnGuard Reporting and Dashboards, wait some time, log back in and then try to run the report.

   The new report is not yet replicated across the Enterprise system.
8. To allow access to the report, go into System Administration and assign permissions as needed.



9. Open OnGuard Reporting and Dashboards.

   The new report should be ready to use a few minutes after logging in once any UDFs have been regenerated.



Changing the Session Timeout in LenelS2 Console

If the session timeout is changed in LenelS2 Console, the LS Reporting service must be restarted in order for the change to take effect in OnGuard Reporting and Dashboards.

Changing the Inactivity Timeout Session to Generate Reports

Generating long or complex reports in OnGuard Reporting and Dashboards could take several hours to complete. As a result, the inactivity timeout timer in OnGuard may expire, thus logging the user out of OnGuard and OnGuard Reporting and Dashboards, and an error message will appear in OnGuard Reporting and Dashboards. To prevent this from occurring, set the **Inactivity timeout** setting in OnGuard Users to a value long enough to accommodate the amount of time needed to generate long and complex reports.

Changing the OpenAccess Port Number

To change the public IP port on which the OpenAccess API server responds to HTTPS requests (for example, such as those made by OnGuard browser-based client applications like OnGuard Reporting and Dashboards or partner integrations), you must manually configure the new port number in System Administration and the **nginx.conf** file. For more information, refer to “Change the OpenAccess Port Number” in the OnGuard System Administration User Guide (DOC-200).

Notes: If the port number is changed for OpenAccess, you must also update the LS Web Event Bridge service configuration to reflect this change. Event subscriptions will not function if you don’t make this configuration change. To do this, edit the file

Lnl.OG.WebEventBridgeService.exe.config, located in the OnGuard installation directory. Update the line:

```
<add key="OpenAccessProxyUri" value="https://
localhost:8080/api/access/onguard/openaccess/" />
```

to change the default port number (8080) to the new port number.

APPENDIX F

Uninstalling an OnGuard Installation

This appendix provides useful information for uninstalling an OnGuard installation.

Files Removed During OnGuard Uninstallation

An OnGuard uninstallation removes all application code and components installed with the original OnGuard installation.

Files Not Removed During OnGuard Uninstallation

The following items are not uninstalled during an OnGuard uninstallation:

- Installation packages not installed with OnGuard
- Common system components that might be shared by other applications, and have their own installation processes (prerequisites)
- OnGuard localizations containing customer data or customizations
- Configuration files that have been customized (.ini, .config, and so on)
- Files that are created during the use of the applications (reports, logs, and so on)
- Registry options and settings that would support re-installation

Index

1212 Pittsford-Victor Road
Pittsford, New York 14534 USA
Tel +1.866.788.5095
www.LenelS2.com