



# OnGuard<sup>®</sup>

## Installation Guide

PERPETUAL INNOVATION



A UTC Fire & Security Company

Lenel OnGuard® 2009 Installation Guide, product version 6.3. This guide is item number DOC-110, revision 1.038, May 2009

Copyright © 1992-2009 Lenel Systems International, Inc. 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 express written permission of Lenel Systems International, Inc.

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

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that agreement. Lenel and OnGuard are registered trademarks of Lenel Systems International, Inc.

Microsoft, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Integral and FlashPoint are trademarks of Integral Technologies, Inc. Crystal Reports for Windows is a trademark of Crystal Computer Services, Inc. Oracle is a registered trademark of Oracle Corporation. Other product names mentioned in this User Guide may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Portions of this product were created using LEADTOOLS © 1991-2009 LEAD Technologies, Inc. ALL RIGHTS RESERVED.

OnGuard includes ImageStream® Graphic Filters. Copyright © 1991-2009 Inso Corporation. All rights reserved. ImageStream Graphic Filters and ImageStream are registered trademarks of Inso Corporation.

---

# Table of Contents

---

<b>CHAPTER 1</b>	<b><i>About This Guide</i></b> . . . . .	<b>9</b>
	The Installation Guides . . . . .	10
<b>CHAPTER 2</b>	<b><i>Introduction</i></b> . . . . .	<b>11</b>
	Required Installations . . . . .	12
	Steps for Installing OnGuard . . . . .	12
	<i>Installing OnGuard with SQL Server</i> . . . . .	13
<b>CHAPTER 3</b>	<b><i>Database Backup and Restoration</i></b> . . . . .	<b>15</b>
	Backing Up Your Database to File . . . . .	15
	<i>Back Up to a File on SQL Server 2008 Database</i> . . . . .	16
	<i>Back Up to a File on SQL Server Express Edition</i> . . . . .	17
	Backing Up to CD/DVD . . . . .	18
	Backing Up to Tape . . . . .	19
	<i>Back Up to Tape on SQL Server Database</i> . . . . .	19
	<i>Back Up to Tape on SQL Server 2008 Express Edition</i> . . . . .	21
	Restoring Databases . . . . .	22
	<i>Restore the Database on SQL Server 2008</i> . . . . .	22
	<i>Restore the Database on SQL Server Express</i> . . . . .	24
<b>CHAPTER 4</b>	<b><i>Transferring a SQL Server Express Database</i></b> . . . . .	<b>25</b>
	Steps to Transfer a SQL Server Express Database . . . . .	25
	<i>Ensure Minimum Server Requirements are Met</i> . . . . .	26

	<i>Stop the SQL Server Service</i> . . . . .	26
	<i>Copy Files from the Old Server to the New Server</i> . . . . .	26
	<i>Restart the SQL Server Service</i> . . . . .	26
	<i>Change the Database Owner</i> . . . . .	27
	<i>Verify the Database Transfer was Successful</i> . . . . .	28
<b>CHAPTER 5</b>	<b><i>Microsoft SQL Server 2008</i></b> . . . . .	<b>29</b>
	Prerequisites . . . . .	30
	SQL Server 2008 Express Edition . . . . .	30
	<i>Upgrading to SQL Server 2008 Express Edition</i> . . . . .	31
	<i>Installing SQL Server Management Tools</i> . . . . .	32
	SQL Server 2008 Standard Edition . . . . .	33
	<i>Installation Steps</i> . . . . .	33
	<i>Upgrade Steps</i> . . . . .	34
	<i>Installing SQL Server 2008</i> . . . . .	34
	<i>Configuring SQL Server 2008</i> . . . . .	36
<b>CHAPTER 6</b>	<b><i>Installing OnGuard on a Server</i></b> . . . . .	<b>41</b>
	Install Prerequisites from the Supplemental Materials Disc . . . . .	41
	Configuring the Hardware Key . . . . .	42
	<i>Configure a Parallel Port Hardware Key</i> . . . . .	43
	<i>Configure a USB Hardware Key</i> . . . . .	43
	Install the OnGuard Software . . . . .	44
	Running the Security Utility . . . . .	47
	Install Your OnGuard License . . . . .	48
	<i>Log into License Administration</i> . . . . .	49
	<i>Changing Administrator Properties for License Administration</i> . . . . .	50
	<i>Install a New License</i> . . . . .	51
	<i>Activate a Software License</i> . . . . .	52
	<i>Return a Software License</i> . . . . .	52
	<i>Repair a Software License</i> . . . . .	53
	Run Database Setup . . . . .	53
	Configure the OnGuard Logs Folder . . . . .	55
<b>CHAPTER 7</b>	<b><i>Installing OnGuard on a Client Machine</i></b> . . . . .	<b>57</b>
<b>CHAPTER 8</b>	<b><i>Database Authentication for Web Applications</i></b> . . . . .	<b>59</b>
	Windows Authentication with SQL Server . . . . .	59
	<i>Configure Windows Authentication with SQL Server</i> . . . . .	60

---

<i>Configure Authentication for Reports in Area Access Manager</i> . . .	61
Windows Authentication with Oracle . . . . .	63
<i>Create a new Windows user</i> . . . . .	63
<i>Add the Windows user to Oracle</i> . . . . .	63
<i>Verify the Integrated Security Setting</i> . . . . .	65
Provide Credentials in the Protected File . . . . .	65
<i>Securing Files with the Access Control List</i> . . . . .	65
<i>Store the Lenel User Credentials</i> . . . . .	66
<b>CHAPTER 9</b> <i>Configuring the Web Application Server</i> . . . . .	69
Custom Install the Web Application Server . . . . .	70
Running Form Translator . . . . .	70
Internet Information Services (IIS) . . . . .	71
<i>.Net Configuration with SQL Server</i> . . . . .	71
<i>Serving Dynamic Content with Windows Server 2003</i> . . . . .	72
<i>Creating Virtual Directories</i> . . . . .	72
<i>Configure SSL</i> . . . . .	73
Authentication . . . . .	73
<i>Configure the LS Application Server Service Log On Account</i> . . . .	73
Area Access Manager and VideoViewer Browser-based Clients . . . . .	74
<i>Browser-based Reports</i> . . . . .	74
<i>Configuration Download Service</i> . . . . .	76
<i>OnGuard User Permissions</i> . . . . .	76
Client Configuration . . . . .	77
<i>Internet Browser Security Level</i> . . . . .	77
<i>Configure Single Sign-on for Browser-based clients</i> . . . . .	78
<i>Accessing the Browser-based Applications</i> . . . . .	79
<i>Create Bookmarks</i> . . . . .	80
<b>CHAPTER 10</b> <i>Visitor Management Installation</i> . . . . .	81
Using SSL . . . . .	81
<i>Security and Authentication</i> . . . . .	81
ClickOnce for Front Desk and Kiosk . . . . .	83
<i>Prerequisites</i> . . . . .	83
ClickOnce Setup . . . . .	83
<i>Methods of Deployment</i> . . . . .	84
<i>Installation</i> . . . . .	85
Workaround for Security Policies . . . . .	86
<i>Support Two Security Policies</i> . . . . .	86

<b>CHAPTER 11</b>	<b><i>Logging Into the OnGuard System</i></b>	<b>89</b>
Windows User Permissions		89
Passwords		89
<i>Password Standards</i>		90
<i>Enable/Disable Strong Password Enforcement</i>		90
<i>Error Messages</i>		91
<i>Accounts</i>		91
<i>Log In</i>		92
Single Sign-On		93
<i>Directory Accounts</i>		94
<i>Automatic and Manual Single Sign-On</i>		94
<i>Configure Single Sign-On</i>		94
<i>Log In Using Automatic Single Sign-On</i>		95
<i>Log In Using Manual Single Sign-On</i>		95
Single Sign-On for Browser-based Clients		96
<i>Configure the Web Server</i>		96
<i>Configure the Clients</i>		97
Troubleshoot Logging In		97
<b>CHAPTER 12</b>	<b><i>Accounts and Passwords</i></b>	<b>99</b>
Password Standards		100
<i>Enable/Disable Strong Password Enforcement</i>		101
Change the Database Password		102
<i>Change the Lenel Account Password</i>		102
About Accounts		104
Change the System Administrator Password for the Database		104
<i>Change the SYSTEM Account Password Using Database Setup</i>		105
<i>Write Down and Inform Administrators of the Password Change</i>		105
<b>CHAPTER 13</b>	<b><i>Maintaining the OnGuard Installation</i></b>	<b>107</b>
Remove OnGuard 2009		107
OnGuard Fixes and Maintenance		108
<i>Hot Fixes</i>		108
<i>Third-Party Service Packs and Updates</i>		108
<i>Language Packs</i>		109
<i>Log Files</i>		109
<i>Server Maintenance</i>		110
<b>Appendices</b>		<b>111</b>

---

---

<b>APPENDIX A</b>	<b><i>The Application.config File</i></b>	<b>113</b>
	Modifying the Application.config File	113
	Application.config File Settings	116
	<i>ConnectionString</i>	116
	<i>DatabaseType</i>	117
	<i>Lnl.LicenseSystem.Client.Host</i>	117
	<i>Lnl.LicenseSystem.Client.Port</i>	117
	<i>SRConnectionString</i>	118
	<i>SchemaOwner</i>	118
	<i>Error Log</i>	118
<b>APPENDIX B</b>	<b><i>Custom Installation of OnGuard</i></b>	<b>119</b>
	Performing a Custom Installation	119
	<i>First Time and Existing OnGuard Installation</i>	119
	Custom Features	120
	<i>Application Server</i>	120
	<i>Device Discovery Console</i>	120
<b>APPENDIX C</b>	<b><i>Network Video over HTTP via Proxy</i></b>	<b>121</b>
	VideoViewer (Browser-based Client)	121
	Network Requirements	121
	<i>Index</i>	123





---

This is the Installation Guide. This guide will walk you through the installation of the OnGuard software with a SQL Server or SQL Server Express database. It also includes steps to install the browser-based applications. The 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, see 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.

---

## *The Installation Guides*

The following table describes the different installation guides available.

Document Name	Item Number	Document Description
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 an OnGuard system that utilizes SQL Server or SQL Server Express.

---

Installing OnGuard<sup>®</sup> requires you to do 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 on the root of the OnGuard 2009 disc.

**Important:** Lenel 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***

The following must be installed before installing OnGuard:

- If using Windows Vista or Windows Server 2008, the OnGuard setup requires that you have administrative privileges.
- All prerequisite software, on the Supplemental Materials disc, must be installed.
- Each OnGuard computer must be configured for the TCP/IP network protocol prior to installation of the OnGuard software.
- Windows Service Packs are also required but are not provided on the Supplemental Materials disc. See the OnGuard release notes on the Installation disc to see which service packs are required for your operating system. Adobe Reader is not required but highly recommended as you need it to read the OnGuard documentation.
- All database systems must be upgraded to a supported version with the latest approved service pack and updates. Refer to the release notes for specific information.
- The latest approved drivers are required for any video capture devices and printers you have installed on workstations.
- If there is new firmware for the Lenel Digital Video recorders you should upgrade this firmware before upgrading the software. If there is an upgrade it can be found on the Supplemental Materials disc.
- Any third-party applications you are using, such as Crystal Reports, must be purchased and upgraded separately. Verify the most current version that is supported in OnGuard 2009 by referring to the release notes.
- OnGuard servers hosting Web applications must be running Windows XP or Windows Server 2003.
- All servers hosting Web applications must have Internet Information Services (IIS) installed.

---

## ***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.

## Installing OnGuard with SQL Server

1. Make sure you have the proper hardware requirements.
2. Install IIS (only if using the OnGuard browser-based applications). For more information, refer to [Internet Information Services \(IIS\)](#) on page 71.
3. Install and configure SQL Server or SQL Server Express. For more information, refer to [Chapter 5: Microsoft SQL Server 2008](#) on page 29.
4. Install prerequisites from the Supplemental Materials disc. For more information, refer to [Install Prerequisites from the Supplemental Materials Disc](#) on page 41.
5. Configure the hardware key. For more information, refer to [Configuring the Hardware Key](#) on page 42.
6. Install the OnGuard software. For more information, refer to [Install the OnGuard Software](#) on page 44.
7. Run the Security Utility. For more information, refer to [Running the Security Utility](#) on page 47.
8. Install the OnGuard license. For more information, refer to [Install Your OnGuard License](#) on page 48.
9. Configure authentication with the database (only if using the OnGuard browser-based applications). For more information, refer to [Chapter 8: Database Authentication for Web Applications](#) on page 59.
10. Run Database Setup. For more information, refer to [Run Database Setup](#) on page 53.
11. Configure the Web Application Server (only if using the OnGuard browser-based applications). For more information, refer to [Configuring the Web Application Server](#) on page 69.
12. Configure the client (only if using the OnGuard browser-based applications). For more information, refer to [Client Configuration](#) on page 77.

To access the browser-based Area Access Manager, VideoViewer, or Visitor Management Host or Administration pages, the link syntax is as follows (where *<machinename>* is the location of the Web Application Server):

- [http://<machinename>/lnl.og.web/lnl\\_og\\_aam.aspx](http://<machinename>/lnl.og.web/lnl_og_aam.aspx)
- [http://<machinename>/lnl.og.web/lnl\\_og\\_videoviewer.aspx](http://<machinename>/lnl.og.web/lnl_og_videoviewer.aspx)

- <http://<machinename>/IdvmHost>

Or, if you are using manual sign-on for the Visitor Management Host:

<http://<machinename>/idvmhost/?useAutomaticSSO=false>

- <http://<machinename>/AdminApp>

To access the Visitor Management Front Desk or Kiosk ClickOnce pages, use the following URLs:

- <http://<machinename>/FrontDeskClickOnce>
- <http://<machinename>/KioskClickOnce>

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 tape drive.
- 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.

**Note:** Some of the procedures in this chapter require the use of SQL Server Management Studio. If have SQL Server 2008 Express Edition and you do not have the SQL Server Management Studio Express application, you can download the software from Microsoft's Web site: <http://www.microsoft.com/downloads/details.aspx?FamilyID=08e52ac2-1d62-45f6-9a4a-4b76a8564a2b&displaylang=en>.

---

## ***Backing Up Your Database to File***

This section includes information on how to:

- [Back Up to a File on SQL Server 2008 Database](#) on page 16

- [Back Up to a File on SQL Server Express Edition](#) on page 17

## Back Up to a File on SQL Server 2008 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. Click the Windows Start button, then select **All Programs > Microsoft SQL Server 2008 > 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 displayed.
  - 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].
5. Expand the Management folder in the Object Explorer.
6. Right-click on the Maintenance Plans folder and select **Maintenance Plan Wizard**.
7. The SQL Server Maintenance Plan Wizard is displayed. Click [Next].
8. On the Select Plan Properties window:
  - a. In the **Name** field, enter a name for the maintenance plan.
  - b. Click [Change].
9. The Job Schedule Properties window is displayed.
  - 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.



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

## **Back Up to a File on SQL Server Express Edition**

1. Click Start, then select **All Programs > OnGuard 2009 > Database Backup**.

2. The Database Backup window displays. Click [Connect] and connect to the AccessControl database.
3. Verify the **Backup** radio button is selected in the Database operation section.
4. Select the **File** radio button in the To/From section and click [Browse] and navigate to the directory or network connection you would like to save the backup file to.
5. Enter a name for the file and click [Save].
6. Verify the **Overwrite backup set** radio button is selected and click [Run].
7. Click [OK] after the database is successfully backed up.
8. Exit the Database Backup application.

---

## ***Backing Up to CD/DVD***

The process of backing up to CD/DVD is the same for SQL Server Standard and Express Editions. You can use other CD/DVD burning programs but you must consult their specific documentation on how to do so.

To back up your database to CD or DVD using Windows, follow these steps:

1. Back up your database to a file. For more information, refer to [Backing Up Your Database to File](#) on page 15.
2. Right-click on the file(s) to be backed up and click [Send to]. Choose the CD or DVD writable drive on your computer.
3. You receive a message that files are waiting to be backed up.
4. Click on the My Computer icon on your desktop and double-click the CD or DVD drive that you saved the files to. You should see the files you want to burn.
5. Make sure the proper media is in the drive and click **File** in the menu bar and select **Write these files to CD/DVD**.
6. The CD/DVD writing wizard opens. Follow the on screen instructions to burn your files to CD/DVD.

When the CD or DVD is written, store it in a safe location. You will need the files saved on the disc to restore the database if something ever happens to it. You should back up your database as often as you can.

---

## ***Backing Up to Tape***

This section includes:

- [Back Up to Tape on SQL Server Database](#) on page 19
- [Back Up to Tape on SQL Server 2008 Express Edition](#) on page 21
- [Verify that the Backup \(to Tape\) is Set Up Correctly](#) on page 20

### **Back Up to Tape on SQL Server Database**

Before conducting the backup, make sure that there is a tape in the drive that is labeled and is of a supported media format for the drive that you are using.

1. Start the Windows Backup software. To do this:
  - In Windows XP and Windows Server 2003, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**.
  - In Windows Vista, open Control Panel and open the Backup and Restore Center.
  - In Windows Server 2008, open Control Panel and navigate to **Admin Tools > Windows Server Backup**.
2. If the Wizard starts, click the Advanced Mode link.
3. Click the Backup tab.
4. Navigate to the file that you want to back up.
5. In the **Backup media or file name** drop-down, select “Accesscontrol Backup”.
6. Select “Travan” in the **Backup destination** drop-down.
  - a. Click [Start Backup].
  - b. The Backup Job Information window opens.

- c. In the **Backup description** field, type `Accesscontrol Backup`.
  - d. In the **If the media is overwritten, use the label to identify the media** field, type `Accesscontrol Backup`.
  - e. Click [Schedule].
7. A message is displayed. Click [Yes] to save the backup selections now.
8. The Save Selections window opens.
  - a. Specify a name and location for the backup. The recommended filename is “AccessControl.bks”, and that file can be saved in the **C:\** root directory.
  - b. Click [Save].
9. The Set Account Information window opens.
  - a. In the **Password** field, type `admin`.
  - b. In the **Confirm password** field, retype the password.
  - c. Click [OK].
10. The Scheduled Job Options window opens.
  - a. In the **Job name** field, type a descriptive name for the job.
  - b. Click [Properties].
11. The Properties are displayed in the Schedule Job window.
  - a. In the **Schedule task** drop-down, select “Daily”.
  - b. In the **Start time** field, select a time that is 30 minutes later than the time that the SQL backup job is set to start. For example, if the SQL backup job is set to start at 1:00 am, then the start time should be 1:30 am.
  - c. Verify that “1” is selected in the Schedule Task Daily section.
  - d. Click [OK].
12. In the Schedule Job window, click [OK].
13. Click the Schedule Jobs tab and verify that the calendar is full of scheduled jobs.

### Verify that the Backup (to Tape) is Set Up Correctly

After the backup schedule has been set up, you can run your backup immediately. You should do this rather than waiting until the first scheduled backup to occur.

1. Open Control Panel, and then double-click “Scheduled Tasks”.
2. Right-click on the task, and then select **Run**.
3. After a short delay, the backup runs.

### Verify that the Backup Ran

1. Start the Windows Backup software. To do this:
  - a. In Windows XP and Windows Server 2003, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**. In Windows Vista, open Control Panel and open the Backup and Restore Center. In Windows Server 2008, open Control Panel and navigate to **Admin Tools > Windows Server Backup**.
  - b. Click the Restore and Manage Media tab.
  - c. The backup is listed.

### Back Up to Tape on SQL Server 2008 Express Edition

If you are using SQL Server 2008 Express Edition then you cannot have your database backed up automatically. Instead, follow this procedure to back up the database manually.

**Note:** This procedure can also be used to manually back up SQL Server 2008 databases.

Before conducting the backup, make sure that there is a tape in the drive that is labeled and is of a supported media format for the drive that you are using.

1. Start the Windows Backup software. To do this:
  - In Windows XP and Windows Server 2003, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**.
  - In Windows Vista, open Control Panel and open the Backup and Restore Center.
  - In Windows Server 2008, open Control Panel and navigate to **Admin Tools > Windows Server Backup**.
2. If the wizard starts, click the Advanced Mode link.
3. Click the Backup tab.

4. Navigate to the file that you want to back up. In most cases, this will be the **accesscontrol\_backup** file that is in the **C:\Program Files\OnGuard\database\_backup** directory.
5. Select “Accesscontrol Backup” in the **Backup media or file name** drop-down list.
6. Select “Travan” in the **Backup destination** drop-down.
7. Click [Start Backup].
8. The Backup Job Information window opens.
  - a. In the **Backup description** field, type `Accesscontrol Backup`.
  - b. In the **If the media is overwritten, use the label to identify the media** field, type `Accesscontrol Backup`.
9. Click [Start Backup].
10. The backup will run. The Backup Progress window displays, and the backup is complete.

---

## ***Restoring Databases***

This section includes:

- [Restore the Database on SQL Server 2008](#) on page 22
- [Restore the Database on SQL Server Express](#) on page 24

### **Restore the Database on SQL Server 2008**

To restore a SQL Server 2008 database from a tape drive complete the following steps. If you are restoring from a file on either a network connection, CD, or DVD then skip to step 2.

1. Restore the database in the tape drive to a file by running the Windows Backup software. For more information, refer to [Restore the Database from a Tape Drive](#) on page 23. If you backed up to a CD or DVD then you can skip this step and go on to the next step.
2. Restore the file to the database via the SQL Server Management Studio. For more information, refer to [Restore Microsoft SQL Server 2008 Database from a File](#) on page 23.

## Restore the Database from a Tape Drive

1. Insert the tape that contains the database that you wish to restore into the proper drive.
2. Start the Windows Backup software. To do this:
  - In Windows XP and Windows Server 2003, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**.
  - In Windows Vista, open Control Panel and open the Backup and Restore Center.
  - In Windows Server 2008, open Control Panel and navigate to **Admin Tools > Windows Server Backup**.
3. If the wizard starts, click the Advanced Mode link.
4. Click the Restore and Manage Media tab.
5. Select “Travan”, and then navigate to the database that you wish to restore.
6. Click [Start Restore].

## Restore Microsoft SQL Server 2008 Database from a File

1. Click the Windows Start button, then select **All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio**.
2. The SQL Server Management Studio window displays.
  - a. Navigate to OnGuard database.
  - b. Right-click on the OnGuard database and select **Tasks > Restore > Database**.
3. The Restore database window displays.
  - a. For the **To database** and **From database** drop-downs, select the OnGuard database.
  - b. Click the Options page from the Select a page list view.
4. The Options page is displayed.
  - a. Select the **Overwrite the existing database** check box.
  - b. Click [OK].
5. A success message is displayed. Click [OK].

## Restore the Database on SQL Server Express

To restore a SQL Server 2008 Express Edition database from a tape drive do the following two steps. If you are restoring from a file on either a network connection, CD, or DVD then skip to step 2.

1. Restore the database in the tape drive to a file by running the Windows Backup software. For more information, refer to [Restore the Database from a Tape Drive](#) on page 23. If you backed up to a CD or DVD then you can skip this step and go on to the next step.
2. Restore the file to the database via the OnGuard Database Backup utility. For more information, refer to [Restore the File to the Database](#) on page 24.

## Restore the File to the Database

1. Click the Windows Start button, then select **All Programs > OnGuard > Database Backup**.
2. Login as the SA account; the password can be blank. The Database Backup window displays.
3. Before continuing, stop all LS and LPS services through the Administrative Tools section of Windows Control Panel. Click [Connect] and connect to the AccessControl database.
4. Select the **Restore** radio button in the Database operation section.
5. Select the **File** radio button in the To/From section and then browse for the file to restore.
6. Click [Run].
7. Click [OK] when the restoration is complete.
8. Exit the Database Backup application.



# *Transferring a SQL Server Express Database*

---

You may wish to transfer a SQL Server Express 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 Express database to a new server, complete the following procedures in the order listed:

- [Back up the SQL Server Express database. Refer to \*Back Up to a File on SQL Server Express Edition\* on page 17 or \*Back Up to Tape on SQL Server 2008 Express Edition\* on page 21.](#)
- [Ensure Minimum Server Requirements are Met](#) on page 26.
- [Stop the SQL Server Service](#) on page 26.
- [Copy Files from the Old Server to the New Server](#) on page 26.
- [Restart the SQL Server Service](#) on page 26.
- [Change the Database Owner](#) on page 27.
- [Verify the Database Transfer was Successful](#) on page 28.

## 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 XP 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\_data.mdf** and **AccessControl\_log.ldf** files on the old server to the new server, making sure to replace the files that 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 XP 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**.

## Change the Database Owner

SQL Server Express provides a user interface for accessing the database engine via the SQL Express Management Studio application. To install the SQL Express Management Studio application, download the software from Microsoft's Web site: <http://www.microsoft.com/downloads/details.aspx?FamilyID=08e52ac2-1d62-45f6-9a4a-4b76a8564a2b&displaylang=en>.

### 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 OnGuard 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.

### Change the Database Owner Manually

The following steps are for the manual process of changing the database owner. Follow this procedure to log into the database directly using the ODBC connection created for OnGuard. Once you've done that you can execute the "sp\_changedbowner" command.

1. On the taskbar, click the Start button, and then click **Run**.
2. Click [Browse], navigate to the OnGuard installation directory, and then click on the **ACCESSDB.exe** application. The path to the application will then be listed in the **Open** field. Click [OK].
3. The AccessDB application opens. From the **Management** menu, select **Data Source > Connect**.
4. Click the Machine Data Source tab, select the "Lenel" Data Source Name, and then click [OK].
5. The SQL Server Login window opens.

- a. In the **Login ID** field, type SA.
  - b. Leave the **Password** field blank and click [OK]. The SQL Server Login window will close, leaving just the main window open.
6. Execute the “sp\_changedbowner” commands using the following method:
  - a. From the **SQL** menu, select **Statement**. The Enter SQL Statement window opens.
    - 1) Type the following: `sp_changedbowner sa`
    - 2) Click [OK]. If the command gets highlighted in blue, then it completed without error, and you are ready to enter the next command.
    - 3) Type the following: `sp_changedbowner lenel`
    - 4) Click [OK]. As long as the command gets highlighted blue, the database owner has been successfully changed.

### **Verify the Database Transfer was Successful**

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

---

OnGuard 2009 supports Microsoft SQL Server 2008. There are several editions of SQL Server 2008; refer to the release notes for specific support information.

SQL Server 2008 Express Edition can be installed automatically during the OnGuard installation or upgrade process. During the OnGuard installation or upgrade process an option is presented asking if you would like to install SQL Server 2008 Express Edition.

**Important:** If you have SQL Server 2005 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 from SQL Server 2005 Express to SQL Server 2008 Express are provided in this chapter.

**Note:** When installing SQL Server 2008 on a computer running Windows Vista you may receive warning messages if specific IIS components are disabled which many of them are by default. For information on how to enable these components refer to <http://support.microsoft.com/kb/920201>.

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

- [SQL Server 2008 Express Edition](#) on page 30.
  - [Installing SQL Server Management Tools](#) on page 32
- [SQL Server 2008 Standard Edition](#) on page 33.

---

## ***Prerequisites***

The following prerequisites are required prior to installing SQL Server 2008. If SQL Server 2008 Express is installed by the OnGuard installation, .NET Framework and Windows Installer will be installed automatically.

- Microsoft .NET Framework 3.5 SP1
- Microsoft Windows Installer 4.5 or later
- Microsoft Windows PowerShell 1.0

**Note:** Windows PowerShell can be downloaded from the Microsoft Web site: <http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.msp>.

---

## ***SQL Server 2008 Express Edition***

**Important:** SQL Server 2008 Express Edition can be installed or upgraded from MSDE automatically during the OnGuard installation process. Manual instructions are provided for upgrading from SQL Server 2005 Express in the following section.

**Important:** When installing on Windows Vista, you may be presented with a user account control dialog box asking you to click continue to proceed with the installation. You must click continue to proceed with the installation.

## Upgrading to SQL Server 2008 Express Edition

This section describes the upgrade of SQL Server 2005 Express to SQL Server 2008 Express Edition. Other versions may have different steps.

**Important:** Before upgrading SQL Server, be sure to back up your database!

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. To perform the upgrade you must have the latest service pack approved for use with OnGuard applied.

1. On the Supplemental Materials disc, navigate to the **Prerequisite Software > Microsoft SQL Server 2008 Express** directory and run the **SQLEXPRT\_x86.exe** file.
2. The SQL Server Installation Center is displayed. Click **Installation** from the left pane, then click **Upgrade from SQL Server 2000 or SQL Server 2005**.
3. The Setup Support Rules window will identify potential problems that might occur during installation. You must correct any failures before setup can continue. If no problems are identified, click [OK].
4. In the Product Key window, click [Next].
5. In the License Terms window:
  - a. If you agree with the license terms, select **I accept the license terms**.
  - b. Click [Next].
6. In the Setup Support Files window, click [Install].
7. After the setup files have been installed, the Setup Support Rules will run again to identify potential issues. You must resolve any failures before setup can continue. Once the check has completed successfully, click [Next].
8. In the Select Instance window, select the existing SQL Server installation from the drop-down and click [Next].
9. In the Select Features window, click [Next].
10. In the Instance Configuration window, click [Next].

11. Review the Disk Space Requirements information and click [Next] if you have sufficient space.
12. In the Error and Usage Report Settings window, deselect both options. Click [Next].
13. The Upgrade Rules window will determine if there are any barriers to the installation process. If there are no failures, click [Next].
14. In the Ready to Upgrade window, click [Upgrade] to begin the installation.
15. Once the setup process is complete, you will be notified that you need to restart your computer to complete the process. Click [OK] to close the message, then click [Next].
16. In the Complete window, click [Close] to exit.
17. You will receive another message to remind you to restart your computer. Your computer will not automatically be restarted; you must manually restart your computer to complete the upgrade process.

## Installing SQL Server Management Tools

SQL Server Management Studio is required if the server intends to use Database Authentication or Windows single sign-on.

1. On the Supplemental Materials disc, navigate to the **Prerequisite Software > Microsoft SQL Server 2008 Express** directory and run the **SQLEXPRT\_x86.exe** file.
2. Click **Installation**, then click **New SQL Server stand-alone installation or add features to an existing installation**.
3. The Setup Support Rules window will identify potential problems that might occur during installation. You must correct any failures before setup can continue. If no problems are identified, click [OK].
4. In the Setup Support Files window, click [Install].
5. After the setup files have been installed, the Setup Support Rules will run again to identify potential issues. You must resolve any failures before setup can continue. Once the check has completed successfully, click [Next].
6. In the Installation Type window, select **Perform a new installation of SQL Server 2008** and click [Next].



7. In the Product Key window, click [Next].
8. In the License Terms window:
  - a. If you agree with the license terms, select **I accept the license terms**.
  - b. Click [Next].
9. In the Feature Selection window, select **Management Tools - Basic** and click [Next].
10. Review the Disk Space Requirements information and click [Next] if you have sufficient space.
11. In the Error and Usage Report Settings window, deselect both options. Click [Next].
12. The Installation Rules window will determine if there are any barriers to the installation process. If there are no failures, click [Next].
13. In the Ready to Install window, click [Install] to begin the installation.
14. After all installation progress has completed, click [Next].
15. In the Complete window, click [Close].

---

## ***SQL Server 2008 Standard Edition***

The instructions that follow are for the Standard edition. The installation and upgrade steps for SQL Server 2008 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.

Before upgrading SQL Server, be sure to back up your database!

### **Installation Steps**

To perform the installation, complete the following steps:

1. [Installing SQL Server 2008](#) on page 34.
2. [Configuring SQL Server 2008](#) on page 36.
  - a. [Create the Database](#) on page 36.

- b. [Create a Login](#) on page 37.
- c. [Run New Query](#) on page 38.
- d. [Set Memory Usage](#) on page 38

## Upgrade Steps

- [Installing SQL Server 2008](#) on page 34.
- [Set Memory Usage](#) on page 38.

## Installing SQL Server 2008

**Note:** SQL Server 2008 setup requires Microsoft .NET Framework 3.5 SP1 and Windows Installer 4.5. If you do not have these prerequisites prior to installing SQL Server 2008, the setup will prompt you before installing them.

1. Insert the SQL Server 2008 disc.
  - If autorun is enabled, the SQL Server Installation Center is automatically opened.
  - If the SQL Server Installation Center does not automatically appear, click the Windows Start button, then select **Run**. In the Run window, browse for **setup.exe** on the disc drive. Alternatively, you can run **setup.exe** from Windows Explorer.
2. The SQL Server Installation Center is displayed. 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 2000 or SQL Server 2005**.
3. The Setup Support Rules window is displayed. You must correct any failures before setup can continue. If no problems are identified, click [OK].
4. The Product Key window is displayed. Enter your product key and click [Next].
5. In the License Terms window:
  - a. If you agree with the license terms, select **I accept the license terms**.

- b. Click [Next].
6. The Setup Support Files step will install any of the listed components that are missing from your system.
  - a. Click [Install].
  - b. Once the prerequisite installation is complete, click [Next].
7. Upgrade only: In the Select Instance window, select the **Instance to upgrade** from the drop-down and click [Next].
8. In the Feature Selection window:
  - a. Under Instance Features, select **Database Engine Services, SQL Server Replication, and Full-Text Search**.
  - b. Under Shared Features, select **Management Tools - Basic** and **Management Tools - Complete**.

**Note:** For upgrades these features may already be selected and it may not be possible to change the selections.

- c. Click [Next].
9. In the Instance Configuration window:
  - For new installations, select **Default instance** and click [Next].
  - For upgrades, the **Named instance** should already be selected. Click [Next].
10. Review the Disk Space Requirements information and click [Next] if you have sufficient space.
11. The Server Configuration window is displayed.
  - For new installations, select “NT AUTHORITY\SYSTEM” from the **Account Name** column drop-down for SQL Server Agent and SQL Server Database Engine. Click [Next].
  - For upgrades, click [Next].
12. Upgrade only: In the Full-text Upgrade window, click [Next].
13. 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].
14. In the Error and Usage Report Settings window, deselect both options. Click [Next].
15. The Installation Rules or Upgrade Rules window will determine if there are any barriers to the installation process. If there are no failures, click [Next].
16. In the Ready to Install or Ready to Upgrade window, click [Install] or [Upgrade] to begin the installation.
17. After all installation progress has completed, click [Next].
18. In the Complete window, click [Close].
19. Reboot the computer, even if you are not prompted to do so. This completes the installation of SQL Server 2008. You can now go on to configure SQL Server 2008.

## Configuring SQL Server 2008

### Create the Database

- 1. Click the Windows Start button, then select **All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio** to start the SQL Server Management Studio.
- 2. Select your method of authentication, provide credentials if required, and click [Connect].
- 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 column of the log file row.
  - e. Select the **Restricted File Growth (MB)** radio button and set a maximum log file size. The recommended maximum log file size is 2048.
  - f. Click [OK].
5. Select the Options page from the Select a page pane.
- a. Change the **Recovery model** drop-down to “Simple”.
  - b. Change the **Compatibility level** drop-down to “SQL Server 2005 (90)”.
  - c. In the Other options list view, set the **Auto Shrink, Auto Update Statistics, Auto Create Statistics, and Recursive Triggers Enabled** drop-downs to “True”.
  - 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.
  - b. Select the **SQL Server authentication** radio button.
    - For **Password**, type MULTIMEDIA.
    - For **Confirm password**, type MULTIMEDIA.

**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 Lenel Login Driver. Failure to update the Login driver will cause OnGuard not to function properly.

4. Select Server Roles from the Select a page pane.
  - a. We recommend that you select (check):
    - dbcreator
    - serveradmin
5. Select User Mapping from the Select a page pane.
  - a. Select the following databases from the Users mapped to this login list:
    - master
    - tempdb
  - b. Click [OK].
6. The new login will appear in the Logins folder.

## Run New Query

1. In the Object Explorer pane of the SQL Server Management Studio, right-click on the OnGuard database and select **New Query**.
2. A query tab is displayed.
  - a. In the text window, type `sp_changedbowner lenel`
  - b. Press <F5> to execute the command.
  - c. The message “Command(s) completed successfully” is displayed in the Messages tab.
3. Click the close (“X”) button to close the query tab, then click [No] when prompted if you want to save the changes.

## 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

**Note:** This procedure requires that the **Recovery Model** is set to "Simple" in the Database Properties > Options page.

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].





---

The following chapter takes you through the installation process for the OnGuard software. Read all the instructions carefully and proceed in the order presented.

---

### ***Install Prerequisites from the Supplemental Materials Disc***

Before you install OnGuard you must first install the third-party requirements from the Supplemental Materials disc. Windows Service Packs are also required but are not provided on the Supplemental Materials disc. See the OnGuard release notes on the Installation disc to see which service packs are required for your operating system. Adobe Reader is not required but highly recommended as you need it to read the OnGuard documentation.

1. Insert the Supplemental Materials disc into a disc drive on a computer running the Windows operating system.
2. Install the components that are needed from the prerequisites section:
  - Adobe Reader - required to read the OnGuard help documentation

- Microsoft .NET Framework 3.5 - Required for some applications to work correctly. While installed automatically during the OnGuard installation some systems have shown that installing it beforehand increases the speed of the OnGuard installation significantly.
- Crystal .NET Components - Required if installing the browser-based applications. This is not necessary for Windows Vista installations.
- Microsoft DirectX - Required on all machines running OnGuard except if using Windows Vista.

3. Install your database system.

**Note:** If you do not install a database system, SQL Server 2008 Express edition can be installed during the OnGuard installation.

4. Restart your computer.

**Note:** Internet Information Services (IIS) is required for use of the Web applications, but is not included on the Supplemental Materials disc. IIS can be installed from **Control Panel > Add or Remove Programs > Add/Remove Windows Components**. The Windows installation disc may be required.

---

## *Configuring the Hardware Key*

**Important:** If you are using a software license you do not need to use a hardware key or install the Sentinel drivers. For information on activating a software license, refer to [Install Your OnGuard License](#) on page 48.

OnGuard software is most commonly protected by a hardware key that connects to the server.

There are two types of hardware keys available for use with OnGuard: parallel port and USB. Please remember to physically attach the hardware key (“dongle” adapter) directly to the respective 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.

## Configure a Parallel Port Hardware Key

If you are using a hardware key that attaches to the parallel port you must also install the Sentinel parallel key driver found on the Supplemental Materials disc.

## 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 disc and then double-click the .exe file. This can be found by navigating through the following folders on the Supplemental Materials disc: **/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. Click on both the Sentinel Protection Server and Sentinel Keys Server and select, "This feature will not be available." [Click Next].
  - f. Click [Install].
  - g. When 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.

---

## *Install the OnGuard Software*

1. Insert the OnGuard Installation disc into a disc drive on a computer running the Windows operating system.
2. If auto-run is enabled, simply click the [Install Now] button. If not, click the Windows Start button, then click **Run**. In the Run window, browse to the disc and select **setup.exe** from the disc drive. Alternatively, you can navigate to the disc manually and run **setup.exe**.
3. You may receive a message recommending that you upgrade your database. Please follow the on-screen directions carefully. Contact your OnGuard representative if you have any questions. Having an improper database will cause your system to be unstable.
4. The Microsoft .NET Framework 3.5 SP1 installation wizard begins. Click [Install] to begin installation. Microsoft .NET Framework 3.5 SP1 must be installed for some OnGuard features to work correctly.
5. When prompted, read the Software License Agreement. If you agree to its terms:
  - a. Select the **I accept the terms in the license agreement** radio button.
  - b. Click [Server] or [Client], depending on the computer on which you are installing.

6. Next, you will be prompted to enter the system type information.

If you would like to install all the features, select the **Typical System** radio button.

If you would like to include or exclude certain features, select the **Custom System** radio button. If you select this option a window will appear allowing you to select your features. You must do a custom install to use the browser-based clients. Before installing browser-based applications your system must have IIS installed and meet other requirements. Installing the browser-based applications without meeting the proper requirements could result in major system problems. For more information, refer to [Chapter 9: Configuring the Web Application Server](#) on page 69.

7. Choose your database.

**Note:** SQL Server 2008 Express Edition can be installed automatically during the OnGuard installation process. During the OnGuard installation process an option is presented asking if you would like to install SQL Server 2008 Express Edition. It is highly recommended that you install SQL Server 2008 Express Edition automatically.

8. Click [Next].
9. In the System Location Information window:
  - a. Either accept the default installation directory or click [Browse] and specify a different destination folder.
  - b. Accept the default location of the License Server or click [Browse] and specify a different location. If a mistake occurs and you accept a different location for your License Server than you meant to then you must adjust this in the **ACS.INI** file and **Application.config** file.
  - c. 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.

**Note:** If you accept the default port setting of 8189, it is written into the **ACS.INI** file. If you want to enter a port setting other than 8189, it is written into both the **ACS.INI** file AND the

...**OnGuard\LicenseServerConfig\Server.Properties** file.

This file will only be created during the install *if* the port setting is changed. If you want to change the port setting in the **ACS.INI** file *after* the installation (either to a new setting or back to 8189), then you must also change it in the **Server.Properties** file.

- d. In the **Choose the location of your [SQL/Oracle/SQL Express] Database** section, accept the default location or click [Browse...] and specify a different location.

**Note:** When installing with an Oracle database the [Browse...] button is grayed out.

- e. If you selected the **Typical System** radio button in the previous window, click [Install], and the OnGuard installation will begin. Proceed to step 14. If you selected the **Custom System** radio button, the [Install] button is replaced by a [Next] button. Click [Next].

10. The Custom Setup window will be displayed and you must 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.

11. Click the icon to the left of a feature to display a popup menu of installation choices for that feature. Once completed click [Next].
12. Click [Install] to begin the installation.

**Note:** If you chose to custom install the Web Application Server, additional prompts will be displayed. Follow the on-screen instructions and provide the Web address of the computer, username, and password.

13. A check is performed “behind the scenes” to determine if a language pack is installed. If an old language pack is installed, you receive a warning message. Do one of the following:

- If you wish to cancel the installation and remove the language pack by yourself, click [Cancel].

- If you wish to remove the language pack and continue the installation, click [Remove & Continue].
14. The installation may take several minutes as indicated by the progress bar.

**Important:** Lenel 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.

15. Once the installation is complete, the database installation utility and Security Utility run. Follow the on-screen instructions to finish the installation.

**Important:** The database installation utility will prompt you for the SQL Server “sa” password. If you installed SQL Server Express as part of the OnGuard installation, the password is “Expres\$”. If you installed SQL Server Express prior to the OnGuard installation, the “sa” password is the one you set during the manual SQL Server Express installation.

16. Depending on the components that you chose to install, you may need to reboot the computer. If you are prompted to do so, reboot the computer.

---

## ***Running the Security Utility***

Lenel 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.

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

To run the Security Utility manually:

1. Click **Start > All Programs > OnGuard 2009 > 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 Lenel 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 VMware Products Compatibility Guide, located at <https://customer.lenel.com/?q=filemanager/active&#38;fid=2087>. (You will need a Lenel login to gain access to this site.)



It is important that access to licensing.lenel.com is allowed through your proxy if you wish to be able to activate and deactivate licenses. If it is not you will have to use activate by phone.

**Important:** TCP Port 8888 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-Lenel HID access panels you must purchase a separate license. Lenel 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 e-mailed 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 be run wherever you wish to use License Administration.
2. Click the Windows Start button, then select **All Programs > OnGuard 2009 > 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.

**Note:** The URL for License Administration is: **http://  
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: **http://alpha:9999/**

3. In the **Username** field, type a valid username. When logging in for the first time, the **Username** is **admin**.
4. In the **Password** field, type a valid password that corresponds to the username entered. When logging in for the first time, the password is **admin**.
5. Click [Log In]. The License Administration options will be displayed.
6. The first time you log in you are strongly encouraged to change the password. To do this, click the “Change Your Password” hyperlink.
7. The Administrator Properties page is displayed. You can change the user name, password, or both. This user name and password is only used for the License Administration application.
  - a. To change the user name, enter a new value in the **Username** field.
  - b. To change the password, enter a new value in the **Password** field.
  - c. If you are changing the password, you must reenter the password in the **Confirm Password** field.
  - d. Click [Update]. A message will be displayed that indicates whether the administrator properties were successfully updated.

## Changing Administrator Properties for License Administration

After logging in for the first time, you are strongly encouraged to modify the default user name and password as soon as possible to discourage unauthorized use. To change the user name and password, do the following:

1. Log into License Administration.
2. Click the Administrator Properties... hyperlink. The administrator properties will be displayed in the right half of the window.
3. You can change the user name, password, or both.

- a. To change the user name, enter a new value in the **Username** field.
  - b. To change the password, enter a new value in the **Password** field.
  - c. If you are changing the password, you must reenter the password in the **Confirm Password** field.
4. Click [Update]. A message will be displayed that indicates whether the administrator properties were successfully updated.

### **Install a New License**

1. Obtain a new license file from Lenel. 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. Start License Administration.
4. Log into License Administration.
5. Click the **Install New License...** hyperlink.
6. In the **License file** field, enter the name and location of the file containing the license that you want to install. You can use [Browse] to locate the file.
7. Click [Next].
8. View the license and make sure that it is the correct license.
9. Scroll down to the bottom of the window and click [Next].  
If the license is not the correct license, click [Back] to go back and choose another license file.
10. Read the terms of the license agreement and select the **Yes** radio button if you agree with the terms of the license.
11. Click [Finish]. The license will be installed. The entry that is displayed in the **Installed Licenses** drop-down listbox indicates the name of the product that the license controls, and will be updated to include the new license.
12. If you are installing a software license you must now activate it. For more information, refer to [Activate a Software License](#) on page 52.

## Activate a Software License

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

1. View the license that you have installed.
2. Click the **Activate** hyperlink.
3. Choose an activation method:
  - **Online** - select this option to activate the license over the Internet. You may be prompted to provide proxy information to connect to the activation server.
  - **Phone** - select this option if you do not have an Internet connection. You are given a phone number to call for activation. If you activate by phone you will be unable to return or repair the license online and must do so over the phone.
4. Click [Activate]. If you are activating by phone follow the on-screen instructions.
5. Click [Close] once the license has activated.

## Return a Software License

You may find it necessary to return a software license if, for example, you are moving an OnGuard installation from one computer to another. To do so:

1. View the license that you have installed.
2. Click the **Return** hyperlink.
3. Choose a return method:
  - **Online** - select this option to return the license over the internet. You may be prompted to provide proxy information to connect to the activation server.
  - **Phone** - select this option if you do not have an internet connection. You are given a phone number to call to return the license.
4. Click [Return]. If you are returning by phone follow the on-screen instructions.
5. Click [Close] once the license has been returned.

## Repair a Software License

If your software license has become corrupt or if you have made certain computer hardware changes you may have to repair the license. To do so:

1. View the license that you have installed.
2. Click the **Repair** hyperlink.
3. Choose a repair method:
  - **Online** - select this option to repair the license over the Internet. You may be prompted to provide proxy information to connect to the activation server.
  - **Phone** - select this option if you do not have an Internet connection. You are given a phone number to call to repair the license.
4. Click [Repair]. If you are repairing by phone follow the on-screen instructions.
5. Click [Close] once the license has been repaired.

---

## *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.

**Important:** 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 you need to modify the **application.config** file to correct this. For more information, refer to [The Application.config File](#) on page 113.

1. Click the Windows Start button, then select **All Programs > OnGuard 2009 > 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:

- **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.
3. A warning message appears and reminds you to back up your database. For more information, refer to [Chapter 3: Database Backup and Restoration](#) on page 15. If your database is backed up, click [Yes].
  4. The database server account passwords window opens. If your passwords are considered weak then you must exit the application, change the passwords, and run Database Setup again. Continuing with weak passwords will cause the OnGuard Web-based applications to not function properly. If your passwords are strong, click [OK].
  5. The database will install. 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, etc. 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.
  6. When the database setup has been completed successfully you will receive a message telling you that to use the OnGuard Web applications you will need to run the Form Translator Utility. If you plan on running the browser-based applications click [Yes]. Otherwise, click [No].
  7. Log into Form Translator. Enter in the OnGuard “sa” login information for the fields, which include User Name, Password, and Directory. Click [OK].

**Note:** If Form Translator happens to fail, try running it again. For more information, refer to [Running Form Translator](#) on page 70.

## *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:\Program Files\OnGuard\Logs folder**.
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 OnGuard.
5. Select the **Allow** check boxes for the permissions: Read, Write, and List Folder Contents.
6. Click [OK].





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 it is on the server except you do not need to install a database, run Database Setup, install a license, or install a hardware key (dongle). To install on a client machine refer to [Chapter 6: Installing OnGuard on a Server](#).

There are two ways to install OnGuard on client machines. The first is to manually install OnGuard on each computer and the second is to install OnGuard remotely from the server. Installing OnGuard remotely saves time by having you not go to each client computer to install it manually. It also insures that the same options are selected on every client during the installation.

If you are manually installing OnGuard on the client machines, then go to each machine and refer to [Chapter 6: Installing OnGuard on a Server](#).

If installing OnGuard remotely then refer to the Advanced Installation Topics guide.



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

- Systems with Oracle databases. For more information on Oracle, refer to the Advanced Installation Topics guide.
- Systems using browser-based OnGuard applications. There are two methods of authentication available:
  1. Authenticate Windows with the database.
    - [Configure Windows Authentication with SQL Server](#) on page 60.
  2. [Provide Credentials in the Protected File](#) on page 65

**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.

### Create a new Windows user

Create a new Windows user to run the LS Application Server according to your IT policy. You may also choose to utilize an existing Windows user for authentication.

### Add the Windows user to SQL Server

1. Click the Windows Start button, then select *Programs > Microsoft SQL Server 2008 > SQL Server Management Studio*. This launches 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 list select (check):
    - **db\_owner**
    - **public**

- c. Click [OK].

The new login will appear in the Logins folder.

### Verify the Integrated Security Setting

Verify that the **application.config** file is configured for Windows authentication.

1. Open the **application.config** file to edit.
  - On Windows XP or Windows Server 2003: Navigate to **C:\Documents and Settings\All Users\Application Data\Inl**
  - On Windows Vista or Windows Server 2008: Navigate to **C:\ProgramData\Inl**
2. Find the **<add key="ConnectionString" ...>** line and verify that Integrated Security is set to SSPI.

### Configure Authentication for Reports in Area Access Manager

If you want to use reports with Area Access Manager (Browser-based Client), additional steps are required for Windows authentication.

### Edit the Web.config File

1. Navigate to **C:\Inetpub\wwwroot\Inl.org.webservice** and edit the **Web.config** file.
2. Find the **<system.web>** line and add the following line below it:  
**<identity impersonate="true" />**
3. Find the **<add key="reportDSN" ... >** line and verify that the value is equal to the DSN name for connection to the database.
4. Find the **<add key="reportDatabase" ... >** line. By default this value is set to **<Server Name>len1**.
5. Find the **<add key="reportDatabaseUsername" ... >** line verify that the value is empty.
6. Find the **<add key="reportDatabasePassword" ... >** line and verify that the value is empty.
7. Save and exit the file.

## Disable Anonymous Access in Windows

1. Right-click My Computer and select *Manage*.
2. Expand *Services and Applications > Internet Information Services*.
3. Right-click Web Sites and select *Properties*.
4. On the Directory Security tab, click [Edit].
5. Deselect (uncheck) the **Enable anonymous access** check box.

## Edit the Machine.config File

Windows XP users must also modify the **machine.config** file.

1. Browse to the following folder:  
**C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG**

**Note:** The version folder name may vary depending on the version of .NET you have installed.

2. Open **machine.config** for editing.
3. Search for the following line:  
`<processModel autoConfig="true"`
4. Add the following immediately following `autoConfig="true"`:  
`userName="system" password="AutoGenerate"`
5. This should result in a string such as:  
`<processModel autoConfig="true"  
userName="system" password="AutoGenerate"/>`
6. Save and exit the file.

## Configure Windows Delegation for Remote Databases

If the OnGuard database is located on a different computer than the LS Application Server, Windows delegation must be configured. The following instructions are for domain controllers running on Windows Server 2003.

1. On the domain controller, open Active Directory Users and Computers.
2. In the console tree, under the domain name, click *Computers*.
3. Right-click the Web server, then click *Properties*.
4. On the Delegation tab, select the **Trust this computer for delegation to specified services only** radio button.

**Notes:** If the Delegation tab is not available on a Windows Server 2003 domain controller, you may need to raise the domain functional level. Consult your IT administrator for more information.

Windows Server 2000 does not have the option to specify specific services. Domain controllers running Windows Server 2000 should select **Trust this computer for delegation** on the General tab.

5. Select the **Use Kerberos only** radio button.
6. Click [Add], and add the service running the database. For example, the mssqlserver service and the computer name running the database server.
7. Click [OK].

## Restart IIS

After completing the above steps for configuring reports for Area Access Manager (Browser-based Client), restart IIS.

1. In Computer Management, expand **Services and Applications**.
2. Right-click **Internet Information Services** and select **All Tasks > Restart IIS**.

---

## *Windows Authentication with Oracle*

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

### Create a new Windows user

Create a new Windows user to run the LS Application Server according to your IT policy. You may also choose to utilize an existing Windows user for authentication.

### Add the Windows user to Oracle

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

1. Click the Windows **Start** button, then select *Programs > Oracle (this may be different depending on your installation) > Application Development > SQLPlus Worksheet*.
2. Log in using the **system** account.

**Important:** You must be logged in as SYSTEM to run the script!

3. Type or paste (with modifications) the following script into the worksheet:

**Important:** Modifications must be made in two places that the string OPS\$DOMAIN\DOMAINUSER is found. Replace both instances of DOMAIN with the name of the domain and DOMAINUSER with the name of a user that will be logged in to Windows when Database Setup is run. You must make sure that your DOMAINUSER and DOMAIN are both entirely in uppercase letters or you may encounter problems accessing certain applications.

```
CREATE USER "OPS$DOMAIN\DOMAINUSER" PROFILE
"DEFAULT" IDENTIFIED EXTERNALLY DEFAULT
TABLESPACE "LENEL_DATA"
TEMPORARY TABLESPACE "LENEL_TEMP" ACCOUNT
UNLOCK;

GRANT CONNECT, RESOURCE, DBA TO
"OPS$DOMAIN\DOMAINUSER" ;

COMMIT;
```

4. Execute the script.
5. Navigate to the **sqlnet.ora** file located at **\$ORACLE\_HOME\Network\Admin** and edit it.
6. Verify that authentication is set to "NTS" in the following line:



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

## Verify the Integrated Security Setting

Verify that the **application.config** file is configured for Windows authentication.

1. Open the **application.config** file to edit.
  - On Windows XP: Navigate to **C:\Documents and Settings\All Users\Application Data\Inl**
  - **On Windows Vista: Navigate to C:\ProgramData\Inl**
2. Find the `<add key="ConnectionString" ...>` line and verify that Integrated Security is set to True.

---

## *Provide Credentials in the Protected File*

Windows authentication with the non-embedded application server is the recommended method of configuration. Another method is to store the authentication information in the **application.config** file. When this method is used, additional steps are necessary to secure the file with Access Control Lists (ACL). When ACL is used the information within the file is very secure.

**Important:** 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. This is the default configuration unless the ODBC was manually created.

## 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 LS Application Service to determine where the database is and how to authenticate (by indicating integrated authentication or providing credentials).
- The **Web.config** file is used to store the Lenel user credentials when reports are used with Area Access Manager through a browser.

### Application.config

The **application.config** file can be used to store the Lenel user 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. The user account that runs the LS Application Server service must have read permission for the file.

### Web.config

The **Web.config** file contains user credentials only if reports are generated from the browser-based Area Access Manager.

Read permission must be configured for the account running the Web Service. This is the ASPNET account if running IIS 5.0 or the account configured as the Identity for the application pool that it is in if running IIS 6.0.

### Store the Lenel User Credentials

The following instructions are for storing the Lenel user credentials in the **application.config** file for authentication with the database.

**Note:** For information on storing Lenel user credentials for Crystal Reports, see [Browser-based Reports](#) on page 74.

1. Open the **application.config** file to edit.
  - On Windows XP: Navigate to **C:\Documents and Settings\All Users\Application Data\Inl**
  - On Windows Vista: Navigate to **C:\ProgramData\Inl**

2. Find the `<add key="ConnectionString" ... >` line and add the following to the existing information inside of the quotes (“”) in the value attribute where `<password>` is the LENEL user password:  
`User ID=LENEL; Password=<password>;`
3. On the same line, change the Integrated Security value to:  
`Integrated Security=No;`
4. Save and exit the file.

## 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)`

## Configure Authentication for Reports in Area Access Manager

If you want to use reports with Area Access Manager (Browser-based Client), credentials also must be provided and secured in the **Web.config** file.

1. Navigate to `C:\Inetpub\wwwroot\lnl.org.webservice` and edit the **Web.config** file.
2. Find the `<add key="reportDSN" ... >` line and verify that the value is equal to the DSN name for connection to the database.
3. Find the `<add key="reportDatabase" ... >` line. By default this value is set to `<Server Name>lenel`.
  - If you are using SQL with a different database name, edit the value to equal the name of the SQL database.
  - If you are using Oracle, the `reportDatabase` key is not required should not be specified. Remove `<Server Name>lenel` from the value and set it equal to `" "`.
4. Find the `<add key="reportDatabaseUsername" ... >` line and set the value to `"LENEL"`.

5. Find the `<add key="reportDatabasePassword" ... >` line and set the value to the LENEL account password.
6. The user that the Web Application Service is running under needs permission to create and delete files from the directory set in the `reportTemporaryFilePath` line.
  - a. Find the following line and either leave the default path or type a different directory location: `<add key="reportTemporaryFilePath" value="C:\Temp\LnlWebServiceReports\" ></add>`
  - b. Create the Windows directory specified in the `reportTemporaryFilePath` value.
  - c. Grant permission to create and delete files in the directory to the user that the Web Application Service is running under.
7. Save and exit the **Web.config** file.

## *Configuring the Web Application Server*

---

**Important:** When installing or upgrading OnGuard, you must choose to do a custom installation to install the Web Application Server, which is required on the server to use browser-based applications. The Web Application Server feature requires IIS running on Windows Server 2003 or Windows Server 2008; the Web Application Server is not supported on Windows XP or Windows Vista.

The instructions that follow are for Windows Server 2003; they may vary for Windows Server 2008.

The Web Application Server feature enables the use of browser-based applications on client machines that may not have OnGuard installed. The Web Application Server deploys the minimal software needed for the Web applications on first use, communicates with the OnGuard database, and provides streaming help to the client. Additional configuration steps are necessary to provide the Web Application Server with the credentials to access the OnGuard database.

IIS must be installed prior to the custom installation of the Web Application Server feature. IIS can be installed from **Control Panel > Add or Remove Programs > Add/Remove Windows Components**. The Windows installation disc may be required.

When used in this chapter, *single sign-on* refers to the use of a single log on to gain access to both Windows and the database. The application service runs under this Windows account and uses the same credentials to access the OnGuard database.

**Note:** The OnGuard server must have port 80 open for client connections.

---

## ***Custom Install the Web Application Server***

IIS must be installed prior to the OnGuard installation. IIS can be installed from **Control Panel > Add or Remove Programs > Add/Remove Windows Components**. The Windows installation disc may be required.

After IIS has been installed, use the OnGuard “Custom Installation” to install the Web Application Server component. This step can be performed during the initial installation of OnGuard or as a modification to an existing system. For more information, refer to [Appendix B: Custom Installation of OnGuard](#) on page 119.

---

## ***Running Form Translator***

The Form Translator utility must be run after the Web Application Server is installed. The Web Application Server enables the browser-based applications to be run.

**Note:** Form Translator must also be run after forms are modified using FormsDesigner. Form Translator is only installed on the server. If you are editing forms from a client, you must run Form Translator on the server for the browser-based and smart client-based applications to continue to function properly.

To run the Form Translator follow these steps:

1. Navigate to the OnGuard installation directory.
2. Run **Lnl.Tools.FormTranslator.exe**.

3. Log into Form Translator. Enter in the OnGuard “sa” login information for the fields, which include User Name, Password, and Directory. Click [OK]. If Form Translator happens to fail simply follow these instructions again and consult your Lenel representative.

---

## ***Internet Information Services (IIS)***

**Important:** Managing an Internet Information Services (IIS) Server requires an advanced IT understanding of security and IIS Application management. The installation guidelines offered in this manual are the minimum steps required to utilize IIS with OnGuard. As such, Lenel is not responsible for IIS configuration and maintenance other than the steps outlined for OnGuard functionality. Technical Support assistance will be provided specific to the installation, enablement, and base functionality of IIS per OnGuard requirements. Additional support services should be managed by the customer's IT department, and it is recommended that they are involved early in the implementation process to ensure corporate standards are met.

Default IIS directories and permissions are used. Consult your system administrator to ensure that your security requirements are met. For more information, refer to [Creating Virtual Directories](#) on page 72.

Use of SSL to ensure security across the network when using browser-based applications is highly recommended. Refer to IIS documentation for additional IIS and SSL configuration if desired. Once SSL has been configured, several files must be updated with the new URL. For more information, refer to [Configure SSL](#) on page 73.

### **.Net Configuration with SQL Server**

Systems running versions of OnGuard newer than 5.12.012 should update their .NET version. The exact version of .NET 3.5 SP1 will differ from system to system.

1. Right-click My Computer and select **Manage**.

2. In the Computer Management tree, expand *Services and Applications* > *Internet Information Services* > *Web Sites* > *Default Web Site*.
3. Right-click lnl.og.web and select **Properties**.
4. Select the ASP.NET tab.
5. In the **ASP.NET version** drop-down, select 2.0.
6. Repeat steps 3 through 5 for lnl.og.webservices.

## Serving Dynamic Content with Windows Server 2003

By default Windows Server 2003 only serves static content. If the Web Application Server is running Windows Server 2003, it must be configured to serve dynamic content. Consult your system administrator regarding the security implications of enabling dynamic content. The exact version of .NET 3.5 SP1 will differ from system to system.

1. Right-click My Computer and select **Manage**.
2. In the Computer Management tree, expand *Services and Applications* > *Internet Information Services* and select **Web Service Extensions**.
3. From the listing window, select ASP.NET v2.0 and click [Allow].

## Creating Virtual Directories

**Note:** This configuration is optional.

OnGuard browser-based applications are installed under the default IIS directory. Some system users may require that they be located in an alternate directory. Refer to IIS documentation for instructions on how to create new virtual directories. The following information is provided for configuration of new virtual directories.

Two virtual directories should be created: lnl.og.WebService and lnl.og.Web.

- lnl.og.WebService maps to the Local Path [Root-IIS-Path]\lnl.og.WebService\ and lnl.og.Web maps to the Local Path [Root-IIS-Path]\lnl.og.Web\.
- Each virtual directory should have the **Read**, **Log visits**, and **Index this resource** permissions selected.
- **Application name** should be Default Application.



- **Execute permissions** should have Scripts only selected.
- **Application pool** should be DefaultAppPool.
- Select the Directory Security tab. Under Anonymous access and authentication control, click [Edit]. **Integrated Windows authentication** should be selected.

## Configure SSL

Refer to IIS documentation for SSL configuration instructions. Once SSL has been configured with IIS, URLs need to be changed from `http` to `https`. Specifically, follow the procedures for updating the following files:

- [Updating the Preferences.js File for SSL](#) on page 74
- [Configuring the Services.config File](#) on page 81
- [Configuring the FlexApplicationConfiguration.xml File](#) on page 82
- [Configuring the SilverlightApplicationConfiguration.xml File](#) on page 82
- [Configuring the ClickOnce Files](#) on page 83

---

## Authentication

An authentication method with the database must be configured for browser-based applications to work properly. Create an account in both Windows and the database system for use with single sign-on authentication. For more information, refer to [Database Authentication for Web Applications](#) on page 59.

### Configure the LS Application Server Service Log On Account

Once the single sign-on account has been created in Windows and the database system, the Application Server service must be configured to run under the Windows account. This Windows user must also have read/write access to the OnGuard directory so that they can write to the log files.

1. Open the Windows services from *Control Panel > Administrative Tools > Services*.
2. Locate the LS Application Server service in the list. Right-click the service and select **Properties**.

3. On the Log On tab, select **This account** and click [Browse].
4. Type the user name of the Windows account in the **Enter the object name to select** text box and click [Check Names].
5. Click [OK] to exit the Select User dialog and [OK] to save the changes to the LS Application Server properties.

---

## *Area Access Manager and VideoViewer Browser-based Clients*

### **Updating the Preferences.js File for SSL**

For Area Access Manager and VideoViewer browser-based clients, the **preferences.js** file needs to be changed to use SSL.

1. Navigate to **C:\inetpub\wwwroot\lnl.og.web\** and edit the **Preferences.js** file.
2. Locate the line  

```
var g_lnl_pfx_webservice_serverAddress
```

and change `http` to `https`.

### **Browser-based Reports**

Area Access Manager has the ability to generate reports with a browser-based client. Additional configuration steps are necessary to enable reports in Internet Explorer:

- Crystal .NET Components must be installed on the Web Application Server.
- For Crystal Reports to access the database, the Lenel user credentials must be stored in the **Web.config** file and protected with security.
- By default, the Reports option is hidden from the browser-based Area Access Manager. The **Preferences.js** file must be edited to show the Reports button.
- Oracle users must grant full control of the Oracle folder to the user running the Web Service.

## Install the Crystal .NET Components

The Crystal .NET Components installation is located on the Supplemental Materials disc. This installation must be performed on the Web Application Server only. The Crystal .NET Components must be installed for the Windows user that the Web Application Service runs under.

## Configure Authentication for Reports in Area Access Manager

Authentication must be configured for reports in order to use them with Area Access Manager (Browser-based Client). Configuration steps vary depending on whether you are using Windows Authentication or providing credentials in a protected file. For more information, refer to [Database Authentication for Web Applications](#) on page 59.

## Enable the Reports Option

Use the following steps to display the [Reports] button in the browser-based Area Access Manager:

1. Navigate to **C:\inetpub\wwwroot\lnl.og.web\** and edit the **Preferences.js** file.
2. Add the following line to the file:  

```
var g_lnl_og_aam_showReportsTask = true;
```
3. Save and exit the file.

## Set Oracle Folder Permissions

Oracle database users must grant full control permissions for the Oracle root directory to the user running the Web Service.

1. Navigate to the Oracle root directory.
2. Right-click the directory and select **Sharing and Security**.
3. On the Security tab, select the user that runs the Web Service from the **Group or user names** list.
4. In the Permissions list, select the check box to allow **Full Control** to the user.
5. Click [Advanced].

6. Select the **Replace permission entries on all child objects with entries shown here that apply to child objects** check box.
7. Click [Apply].

## Configuration Download Service

The “configuration download service” (**LnlConfigDownloadService.exe**) is used to send updates to the controllers when changes are made to access level assignments using the Area Access Manager (Browser-based Client).

This service will check the database once a minute (the default setting) to see if there are any new changes to process and it will then send down these changes to the hardware. To change the default setting so the service checks the database at other time intervals, add the following lines to the **ACS.INI** file (the “LoopDelay” is in milliseconds):

```
[ConfigDownloadService]
LoopDelay=60000
```

This service needs to run if Area Access Manager (Browser-based Client) is being used.

Only one instance of the “configuration download service” can exist in a system.

## Configure the Configuration Download Service Host

1. In System Administration, navigate to **Administration > System options**.
2. On the General System Options form, click [Modify].
3. Select a workstation in the **Configuration Download Service** host drop-down box or browse for one in the system.

## OnGuard User Permissions

User accounts must be configured with permissions to access to the browser-based client applications.

## VideoViewer (Browser-based Client)

The following user permissions must be configured for each user account that will access the VideoViewer:

- System Permission Group > Video Hardware > Video Devices
- System Permission Group > Access Control Hardware > Alarm Panels
- System Permission Group > Users, Directories, Certification Authorities, Logical Access > Permission Groups
- Monitor Permission Group > Monitor > View
- Monitor Permission Group > Monitor > Live Video
- Monitor Permission Group > Control > Control
- Monitor Permission Group > Control > Camera PTZ (If you wish to grant permission to use PTZ)

### **Video Player Installation**

A file download and installation will be required the first time video is accessed through a browser on a client without OnGuard installed.

### **Viewing Reports in Area Access Manager**

Adobe Reader is required to view reports on a client workstation.

---

## ***Client Configuration***

Additional configuration steps are necessary for browser-based applications on the client.

### **Internet Browser Security Level**

The security level must be specified for the OnGuard server that the Web site is hosted on. A custom level must be defined with specific options.

1. From the **Tools** menu in Internet Explorer, select **Internet Options**.
2. Select the Security tab.
3. Select the Trusted sites icon and click [Sites].
  - a. Type the URL for the OnGuard server that the Web site is hosted on.
  - b. Click [Add].
  - c. Click [Close].
4. Set the **Security level for this zone** slider to Medium-low.

5. Click [Custom Level...].
  - a. Locate the following settings in the list and verify that they are set correctly:

Item	Setting
ActiveX controls and plug-ins > Automatic prompting for ActiveX controls	Enable
Downloads > File Download	Enable
Miscellaneous > Access data sources across domains	Prompt
Scripting > Active Scripting	Enable

- b. Click [OK].
6. On the Advanced tab, select **Multimedia > Play animations in web pages**.
7. Click [OK] to close the Internet Properties dialog.

### Configure Single Sign-on for Browser-based clients

Single sign-on can optionally be configured for browser-based clients. The following Internet Explorer settings must be configured on each client workstation that will use single sign-on authentication to connect to the browser-based applications. Additional steps must be performed on the server. For more information, refer to [Single Sign-On](#) on page 93.

1. From the **Tools** menu in Internet Explorer, select **Internet Options**.
2. On the Security tab, select the Trusted Sites icon and click [Sites...].
3. The Trusted sites dialog is displayed.
  - a. In the **Add this Web site to the zone** field, enter the domain name of the Web application server.
  - b. Click [Add].
  - c. Click [Close].
4. Click [Custom level...]
5. The Security Settings - Trusted Sites Zone dialog is displayed.
  - a. Set the **User Authentication > Logon** setting to **Automatic logon with current username and password**.

**Note:** Using Windows to store a username and password for the application will override the **Automatic logon with current username and password** setting in Internet Explorer.

- b. Click [OK].
6. Click [OK].

## Accessing the Browser-based Applications

To access browser-based applications from a client, it is necessary to know the server name and the location of the application on the Web Application Server. For the Area Access Manager and VideoViewer browser-based clients, the IP address is also acceptable in place of the server name. There is not a central log in location for all OnGuard browser-based applications. The following addresses should be used to access the browser-based applications from a client, where *<server-name>* equals the name or IP address of the Web application server.

Application	URL
Area Access Manager	http://<server name>/Inl.og.web/Inl_og_aam.aspx
VideoViewer	http://<server name>/Inl.og.web/Inl_og_videoviewer.aspx
Visitor Management Host	http://<server name>/ldvmHost Or, if manual sign-on is being used: http://<server-name>/ldvmhost/?useAutomaticSSO=false
Visitor Management Administration	http://<server name>/AdminApp

**Note:** If SSL is configured the Web address will begin with https.

For Visitor Management Host, additional steps are required to configure automatic single sign-on. The user logging in must be a cardholder. This cardholder must be paired with a user's directory account.

### Accessing ClickOnce

If you are using ClickOnce for Visitor Management Front Desk or Kiosk, the following URLs are also needed.

Application	URL
ClickOnce for Front Desk	http://<server name>/FrontDeskClickOnce
ClickOnce Kiosk	http://<server name>/KioskDeskClickOnce

### Create Bookmarks

Create favorites in Internet Explorer or shortcuts in the Start menu to enable users to easily access the browser-enabled applications.



---

Visitor Management Host, Administration, Front Desk, and Kiosk are installed with the Web Application Server.

---

## *Using SSL*

After installing the Web Application Server through a custom installation, additional configuration is needed to use SSL.

### **Security and Authentication**

For Visitor Management Host, the **services.config** file needs to be changed to use SSL. The **services.config** file is the default configuration, which is HTTP with Windows authentication.

### **Configuring the Services.config File**

If you do not plan to use SSL, then you do not have to perform this procedure.

1. Navigate to  
**C:\inetpub\wwwroot\lni.og.services\ldvmWebHost.**

2. There are four possible security policies, with corresponding files:

Security policy	File
No transport security, Windows Authentication not required	HttpServices.config
Transport security, Windows Authentication not required	HttpsServices.config
Transport security, Windows Authentication required	HttpsWithWindowsAuthenticationServices.config
No transport security, Windows Authentication required	HttpWithWindowsAuthenticationServices.config

- a. To configure transport security and require Windows Authentication, locate the file, **HttpsWithWindowsAuthenticationServices.config**.
  - b. Select the file name and rename it to `services.config`.
3. Save the file.

### Configuring the FlexApplicationConfiguration.xml File

For Visitor Management Host, the **FlexApplicationConfiguration.xml** file needs to be changed to use SSL.

1. Navigate to **C:\inetpub\wwwroot\Inl.org.services\WebHost** and edit the **FlexApplicationConfiguration.xml** file.
2. Locate the URL.
3. Change `http` to `https`.
4. Save the file.

### Configuring the SilverlightApplicationConfiguration.xml File

For Visitor Administration, the **SilverlightApplicationConfiguration.xml** file needs to be changed to use SSL.

1. Navigate to **C:\inetpub\wwwroot\AdminApp** and edit the **FlexApplicationConfiguration.xml** file.
2. Locate the URL.
3. Change `http` to `https`.

4. Save the file.

### **Configuring the ClickOnce Files**

Additional changes need to be made to the Front Desk and Kiosk ClickOnce files (serviceModelClient.config.deploy) to use SSL. For more information, refer to [ClickOnce Setup](#) on page 83.

---

## ***ClickOnce for Front Desk and Kiosk***

Visitor Management Front Desk and Kiosk can be deployed using ClickOnce. This facilitates simple installation or upgrade of the application. The applications can be deployed from the server or a shared network location.

### **Prerequisites**

Before using ClickOnce, make sure the computer has Microsoft .NET Framework 3.5 with Service Pack 1.

Additionally, the Kiosk requires Windows XP and the Touch-It Virtual Keyboard software.

**Note:** For more information, refer to the Kiosk documentation in the Visitor Administration User Guide.

---

## ***ClickOnce Setup***

To utilize ClickOnce, OnGuard must first be installed on the server. Doing so will install a folder, **FrontDeskClickOnce** for Front Desk, or **KioskClickOnce** for the Kiosk, with the required files. In most typical installations, the folder will be **C:\inetpub\wwwroot\FrontDeskClickOnce** or **C:\inetpub\wwwroot\KioskClickOnce**.

The Touch-It Virtual Keyboard is not installed with Clickonce. It must be installed separately.

## Methods of Deployment

One option for deployment is to make it available through a shared network location. To do this, move the ClickOnce directory to the appropriate location on your network.

Another option is to deploy through the server. With this method, the application can be installed on the computer by accessing the files with a browser.

## Server Name

The name of the server is usually configured during the installation process. However, if you wish to change it, this can be done in the **serviceModelClient.config.deploy** file. This is located in **C:\inetpub\wwwroot\FrontDeskClickOnce\config** for Front Desk or **C:\inetpub\wwwroot\KioskClickOnce\config** for Kiosk.

## Using SSL

The configuration files will also need to be changed when using SSL.

1. Locate the following file:  
Navigate to **C:\inetpub\wwwroot\FrontDeskClickOnce\config** and edit the **serviceModelClient.config.deploy** file for Front Desk.  
Navigate to **C:\inetpub\wwwroot\KioskClickOnce\config** and edit the **serviceModelClient.config.deploy** file for Kiosk.
2. Locate the section that states  

```
<!-- Points to the endpoint that supports a security policy with HTTP and Windows Authentication enabled-->
```

  - Comment markers `<!--` and `-->` are used to indicate a portion of the code that will be ignored.
3. Comment out the endpoint address section of code for http by surrounding it with comment markers.
  - a. Type `<!--` at the beginning of the section, before `<endpoint address="http...`
  - b. Type `-->` at the end of the section, after `"BasicHttpBinding_IIdvmService"></endpoint>`.
4. Locate the section that states

```
<!-- Points to the endpoint that supports a security policy with HTTPS and Windows Authentication enabled-->
```

The code for https is commented out by default.

5. Remove the comment markers `<!--` and `-->` surrounding that section to enable the code.
6. For the address in that same section, change `http` to `https`.

## Installation

Once the ClickOnce deployment site has been created and configured, it is possible to install the application.

### Installing the Application via Network

1. Obtain the location of the deployment site.
2. Navigate to the directory, **FrontDeskClickOnce** for Front Desk. Navigate to the directory, **KioskClickOnce** for Kiosk.
3. To install Front Desk, run **Lnl.OG.VM.FrontDesk.View.application**. To install Kiosk, run **Lnl.OG.VM.Kiosk.View.application**.
4. Click [Install].

### Installing the Application via Server

**Note:** To use this method of installation, JavaScript should be enabled for the browser. If it is not, contact your administrator for assistance.

1. Use a browser to go to the address,  
`http://<server name>/FrontDeskClickOnce` for Front Desk or `http://<server name>/KioskClickOnce` for the Kiosk,  
where `<server name>` is the name of the OnGuard server. If SSL has been configured, the URL will start with `https://...`
2. Click [Install].

The progress bar will indicate when installation is complete.

## ***Workaround for Security Policies***

A Front Desk or Kiosk error may occur, stating, “The HTTP request is unauthorized with client authentication scheme ‘Negotiate’. The authentication header received from the server was ‘Negotiate,NTLM’” This error occurs because only one security policy is typically supported by the Windows Communication Foundation (WCF) service for Visitor Management, regardless of the IIS setting to support both anonymous and Windows Authentication.

### **Support Two Security Policies**

Two security policies may be supported, requiring two webservices, two virtual directories, and two copies of the service file.

### **Creating Two Copies of the Service File**

1. Navigate to **C:\inetpub\wwwroot\LnI.OG.Services**. Copy the directory, **IdvmWebHost**.
2. Name the copied directory **IdvmAnonWebHost**.
3. In the **IdvmAnonWebHost** directory, locate the **HttpServices.config** file and rename it to **Services.config**.

### **Creating a New Virtual Directory**

1. In IIS, create a new virtual directory named **LnI.OG.AnonServices**.
2. For the path, browse to and select the new directory, **C:\inetpub\wwwroot\LnI.OG.Services\ldvmAnonWebHost**.

### **Updating the ClickOnce Deployment**

1. Navigate to **C:\inetpub\wwwroot**. Copy the directory, **FrontDeskClickOnce** for Front Desk. Copy the directory, **KioskDeskClickOnce** for Kiosk.
2. Name the copied directory **AnonFrontDeskClickOnce** for Front Desk or **AnonKioskClickOnce** for Kiosk.
3. Locate the following file:  
Navigate to **C:\inetpub\wwwroot\AnonFrontDeskClickOnce\config** and edit the **serviceModelClient.config.deploy** file for Front Desk.

Navigate to **C:\inetpub\wwwroot\AnonKioskClickOnce\config** and edit the **serviceModelClient.config.deploy** file for Kiosk.

4. Locate the section that states

```
<!-- Points to the endpoint that supports a
security policy with HTTP and Windows
Authentication enabled-->
```

- Comment markers `<!--` and `-->` are used to indicate a portion of the code that will be ignored.

5. Comment out the endpoint address section of code for http by surrounding it with comment markers.

- a. Type `<!--` at the beginning of the section, before `<endpoint address="http...`

- b. Type `-->` at the end of the section, after `"BasicHttpBinding_IIdvmService"></endpoint>`.

6. Locate the section that states

```
<!-- Points to the endpoint that supports a
security policy with HTTP and anonymous -->
This code is commented out by default.
```

7. Remove the comment markers `<!--` and `-->` surrounding that section to enable the code.

8. In IIS, create a new virtual directory named **AnonFrontDeskClickOnce** for Front Desk or **AnonKioskClickOnce** for Kiosk.

9. For the path, browse to and select the new directory, **C:\inetpub\wwwroot\AnonFrontDeskClickOnce** for Front Desk or **C:\inetpub\wwwroot\AnonKioskClickOnce** for Kiosk.

From a non-domain account, start Internet Explorer and go to:

- `http://<server name>/AnonFrontDeskClickOnce` for Front Desk or
- `http://<server name>/AnonKioskClickOnce` for Kiosk

Install the application. After doing so, you should be able to log in and use the application.

**Note:** For more information about configuring the system, refer to the Visitor Management Front Desk and Visitor Administration User Guides.





---

The following chapter deals with everything you need to know about logging into an 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.

---

### ***Passwords***

OnGuard<sup>®</sup> includes strong password enforcement, which 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 93.

The system's strong password enforcement also checks the Lenel database user's password when logging into applications. Database user passwords apply only to Oracle and SQL databases.

## 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 Lenel keywords.
- Although not required, your password should contain numbers, letters, and symbols. Spaces are also acceptable. (for example, August 18, 2002).
- OnGuard passwords are **not** case-sensitive.
- Database passwords conform to the rules of the specific database being used; passwords in SQL Server and Oracle are case insensitive.
- The maximum value for a strong password is 127 characters. The minimum value is 1.

**Note:** 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

## Enable/Disable Strong Password Enforcement

Strong password enforcement is enabled/disabled in System Administration or ID CredentialCenter. When you install OnGuard, by default strong password enforcement is enabled. When you upgrade, by default strong password enforcement is disabled. To manually enable or disable strong password enforcement:

1. Select **System Options** from the **Administration** menu.
2. Select the General System Options tab.
3. Click [Modify].
4. Select or deselect the **Enforce strong passwords** check box.

**Note:** If you disable the option to enforce strong passwords, you will no longer continue to receive a message stating your password is weak every time you log into an application until you

change your OnGuard password to meet the password standards.

5. Click [OK].

## 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 user password, select a password that meets the standards specified in [Password Standards](#) on page 90.

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
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, which you are strongly encouraged to do as soon as possible to discourage unauthorized use. The first time you log into OnGuard to configure the application, you should log in as **SA** and your password should be **SA**.

## 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 93. To log in using single sign-on, refer to [Configure Single Sign-On](#) on page 94.

1. Click the Start button, then select **All Programs > OnGuard 2009**. Choose an application to log in to.
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** check box 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).

**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.

## 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 XP Workstation, 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.

**Note:** *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. Click the Start button, then select **All Programs > OnGuard 2009 > [any OnGuard application]**.
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. Click the Start button, then select **All Programs > OnGuard 2009 > [any OnGuard application]**.
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** check box 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 for Browser-based Clients*

Additional steps are required to enable single sign-on with browser-based clients. Configuration must be performed at the Web Application Server and at each client workstation that will use single sign-on.

### **Configure the Web Server**

The following settings must be configured on the Web Application Server that hosts the web applications.

#### **Disable anonymous access in IIS**

1. Right-click My Computer and select **Manage**.
2. In the Computer Management tree, expand **Services and Applications > Internet Information Services > Web Sites**.
3. Right-click Default Web Site and select **Properties**.



4. Select the Directory Security tab.
5. In the Authentication and access control section, click [Edit].
  - a. Deselect the **Enable anonymous access** check box.
  - b. Select the **Integrated Windows Authentication** check box.
  - c. Click [OK].
  - d. Click [OK].
6. The Inheritance Overrides dialog is displayed.
  - a. Click [Select All].
  - b. Click [OK].

**Note:** If the Inheritance Overrides dialog is not displayed, repeat steps 3 through 5 for the `lnl.og.web` and `lnl.og.webservices` Web sites.

### **Edit the Preferences.js file**

1. Navigate to the `LnI.OG.Web\` directory and edit the `Preferences.js` file.
2. Locate the `var g_lnl_pfx_websevice_serverAddress` line and change `http` to `https`.
3. Locate the `g_lnl_useSingleSignOn` variable and change the value to `true`.
4. Save and exit the file.

### **Configure the Clients**

Additional configuration steps are necessary for the client. For more information, refer to [Configure Single Sign-on for Browser-based clients](#) on page 78.

---

## ***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 a correct user name/password and specified the correct directory.
- If your system is configured to display an authorization warning, you accepted the terms.
- A valid license is installed.
- You have permission to use the application.
- If you attempted to log into the server and the login failed, make sure that a properly coded, licensed dongle adapter is attached to your computer. Make sure that your dongle is securely attached.
- If you attempted to log into a client and failed, make sure the system has a valid software license. Client computers do not need a hardware dongle attached to the computer's parallel port. Instead, the system the client is installed on must have a valid software license, which is installed in the License Administration application.
- If you are using single sign-on, ensure that the directory you are authenticating against is operational and properly configured. When a directory is properly configured, the accounts are listed on the Select Account form when linking a user account to a directory.
- If you are using single sign-on, ensure that the directory account is properly linked to the user account.

---

OnGuard 2009 includes strong password enforcement, which checks the user's password against the OnGuard password standards. This functionality is designed to enhance password security as well as encourage users to implement single sign-on. If single sign-on is used (automatic or manual) OnGuard does not enforce password standards.

**Note:** The strong password enforcement feature in OnGuard also checks the Lenel database user's password when logging into applications. Database user passwords apply to SQL Server Express, SQL Server, and Oracle. For information on changing your database password refer to [Change the Database Password](#) on page 102.

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.	SA	SA	For more information, refer to <a href="#">About Accounts</a> on page 104.
OnGuard database. This is the actual OnGuard SQL Server Express, SQL Server, or Oracle database.	LENEL	MULTIMEDIA	For more information, refer to <a href="#">Change the Database Password</a> on page 102.
License Administration account. This is the account that is used initially to log into the License Administration application.	ADMIN	ADMIN	For more information, refer to <a href="#">Install Your OnGuard License</a> on page 48. For more information, refer to <a href="#">Install Your OnGuard License</a> on page 114.

## *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 Lenel keywords.
- Although not required, your password should contain numbers, letters, and symbols. Spaces are also acceptable. (for example, August 18, 1967)
- OnGuard user passwords are *not* case-sensitive.
- Database passwords conform to the rules of the specific database being used; passwords in SQL Server and Oracle 11g are case-sensitive. Passwords in Oracle 10g and earlier are case-insensitive.
- The maximum value for a strong password is 127 characters. The minimum value is 1.

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

System and Manager  
Internal and Oracle  
Sys and Change\_On\_Install

### **Enable/Disable Strong Password Enforcement**

Strong password enforcement is enabled/disabled in System Administration or ID CredentialCenter. When you install OnGuard, by default strong password enforcement is enabled. When you upgrade, by default strong password enforcement is disabled. To manually enable or disable strong password enforcement:

1. Select **System Options** from the **Administration** menu.
2. Select the General System Options tab.
3. Click [Modify].
4. Select or deselect the **Enforce strong passwords** check box.

**Note:** If you disable the option to enforce strong passwords, you will no longer continue to receive a message stating your password is weak every time you log into an application until you change your OnGuard password to meet the password standards.


## *Change the Database Password*

In addition to user accounts and passwords, your OnGuard system has a database password. During installation, this password is set to MULTIMEDIA. When you log on, the application checks your database server (SQL Server, Oracle, or SQL Server Express) for this password before allowing you to use the database. This is done “behind the scenes.”

It is highly recommended that this password be changed. Although all the machines in an Enterprise or Distributed ID system start out using the same database password (MULTIMEDIA), 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 the database is located on, and which options you choose to use. The SQL Server, Oracle, or SQL Server Express 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 100 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 102.
- e. Click [OK] to save the new password.
4. Exit the LS Login Driver application and restart the service.

## ***About 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 which screens, fields, and buttons the user can access.

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

<b>User name</b>	<b>Password</b>	<b>Type</b>
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, which you are strongly encouraged to do as soon as possible to discourage unauthorized use.

The first time you log into OnGuard to configure the application, you should log in as **SA** and your password should be **SA**.

## ***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 Express 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:



1. Change the system account password in the database using Database Setup.
2. Write down and inform administrators of the password change.

### **Change the SYSTEM Account Password Using Database Setup**

To change the SYSTEM account password using Database Setup, follow the same instructions listed in [Change the Lenel Account Password](#) on page 102, with the following exception: in step 3 on page 103, select the system account from the list (“SA” by default), then click [Change Password].

### **Write Down and Inform Administrators of the Password Change**

1. It is essential that you do NOT lose this password. If you do not have the system administration password, you can potentially lose your entire database since no one may gain access to the information.
2. Write down the password and store in a secure place that won't get lost.
3. Inform other system administrators of the password.
4. BE SURE to inform the customer that you have changed the system password.
5. Explain the importance of the password to the customer and recommend they keep it secure and not allow it to be “common knowledge.”



---

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

---

### ***Remove OnGuard 2009***

OnGuard can be removed by following these steps:

1. In the Control Panel:
  - a. Double-click “Add or Remove Programs”. In Windows Vista and Windows Server 2008 this is called “Programs and Features”.
  - b. In the Currently installed programs listing window, select “OnGuard 2009”.
  - c. Click [Remove].
2. You are asked if you’re sure you want to remove OnGuard. If you are, click [Yes].

## ***OnGuard Fixes and Maintenance***

### **Hot Fixes**

**Important:** A hot fix must be applied to all servers and workstations running OnGuard. Failure to apply the hot fix to all OnGuard computers will result in the inability for the user to log in to the OnGuard system. To ensure that this happens, versions of OnGuard 2009 will not allow you log into the system until all computers have the same hot fix installed.

A hot fix is a method in which the system is updated between OnGuard builds and contain software fixes and feature enhancements.

Hot fixes can be obtained by logging into [www.lenel.com](http://www.lenel.com) and navigating to the Technical Support page. Along the left side of the page you will find a “Hot Fixes” link that lists the ones available. Hot fixes can also be found on the Supplemental Materials disc.

Hot fixes do not have to be installed. Please read the hot fix release notes carefully before installing.

**Important:** You must stop all services with the prefix LS and LPS, and exit all applications before installing any hot fix.

**Important:** Hot fixes cannot be uninstalled. You should create a backup of your system before installing a hot fix. For more information, refer to [Chapter 3: Database Backup and Restoration](#) on page 15.

### **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 disc. See the release notes or [www.lenel.com](http://www.lenel.com) to see what latest updates have been approved.

The components requiring updates are:

Operating system (Operating system updates are not provided on the Supplemental Materials disc.)

- Windows XP
- Windows Server
- Windows Vista

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

#### Database

- SQL Server Express
- SQL Server
- Oracle

#### Miscellaneous

- MDAC
- DirectX
- Windows Internet Explorer
- Adobe Reader

### Language Packs

If you need a translated version of OnGuard you can request one by obtaining a login user name and ID, logging into [www.lenel.com](http://www.lenel.com) and navigating to the Technical Support page. Along the left side of the page you will find a “Language Packs” link that will show you how to request one.

### Log Files

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

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:

- SETUPDB.LOG

- LenelError.log
- DataExchange.log
- Replicator.Log
- LnLogError.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 to tape
- 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

# Appendices





---

The **application.config** file is an OnGuard configuration file that is used mainly to configure database information.

The **application.config** file is located in **C:\Documents and Settings\All Users\Application Data\Ln1** in Windows XP and Windows Server 2003 or **C:\ProgramData\Ln1** in Windows Vista and Windows Server 2008. By default, the **Application Data** folder is hidden in the operating system. If you need guidance in configuring your system to show hidden files and folders, please consult Microsoft Windows help.

You may use the Configuration Editor utility, located in the OnGuard directory, to edit the **application.config** file. You would use this utility if you feel more comfortable using a user interface instead of Notepad to edit configuration files. Editing the **application.config** file and using the Configuration Editor utility should only be done in extreme circumstances and ideally under the supervision of a Lenel representative.

### *Modifying the Application.config File*

1. Navigate to the **application.config** file. Do this by:

- On Windows XP and Windows Server 2003: Navigate to **C:\Documents and Settings\All Users\Application Data\InI**
- On Windows Vista and Windows Server 2008: Navigate to **C:\ProgramData\InI**
- Click the Start button, then select **All Programs > OnGuard 2009 > Configuration Editor**.

**Note:** You must show hidden files and folders to see the **application.config** file.

2. Open the **application.config** file. Do this by:
  - Using Notepad to open the **application.config** file and edit the desired settings.
  - Open the Configuration Editor utility. The **application.config** file opens automatically.
3. The settings most commonly edited in the **application.config** file are:

**Note:** If using the Configuration Editor utility: These settings are found in the **ConnectionString** section of the App Settings sub-tab. To change it, select [Edit] next to the **ConnectionString** field.

- **Initial Catalog:** This specifies the name of the database. If you installed OnGuard, you specified this name during the installation. By default, this is **AccessControl**.
- **ConnectionString:** This specifies the location of the database you will be using and the authentication method.
  - a. “Data Source=” for SQL Server, the Data Source points to the name of the machine that hosts the database. If the database resides on the same machine where database setup will be run from you can use the name of your machine (that is, **COMPUTER1-DT**). For Oracle, the Data Source reflects the SID Service Name.
  - b. “InitialCatalog=” is the name of the database. If you installed OnGuard, you specified this name during the installation. By default, this is **AccessControl**. If your

database is not called AccessControl you must change this line to have your database's name.

**Note:** If using the Configuration Editor utility: These settings are found in their corresponding sections of the App Settings sub-tab. To change them, edit their field text.

- **DatabaseType:** This specifies the type of database being used.
- **SchemaOwner:** The default is “dbo” for SQL, and “LeneI” for Oracle.
- **SRConnectionString:** This refers to the path to the .mdb file.

**Note:** If using the Configuration Editor utility: The Error Log settings are found on the Listeners sub-tab. To edit them, edit their corresponding field text.

- **Name:** Specifies the name of the listener and must be unique.
- **Filename:** Specifies the filename where the log messages are written.
- **Type:** Specifies the type of message to be written out in the log.
  - c. “Singleline” is used to produce a single line of text (usually for verbose or information type logs).
  - d. “Text” is used for logs that need more details including a stack trace (usually for error messages).
- **Severity** - Indicates what level of messages should be written to the log file
  - e. “Error” specifies that only errors will be written to the log file
  - f. “Warning” specifies that only warnings and errors will be written to the log file
  - g. “Information” specifies that informational messages as well as warnings and errors will be written to the log file
  - h. “Verbose” specifies that everything plus additional verbose tracing messages will be written to the log file. This generates a lot of output and should only be

enabled for troubleshooting purposes when instructed by technical support.

4. Save and close the **application.config** file. To save using the Configuration Editor utility, navigate to **File > Save**.

## *Application.config File Settings*

The following sections describe the most commonly changed settings in the **application.config** file in detail. If using the Configuration Editor utility the fields below may appear slightly different as only the pertinent information is shown.

### **ConnectionString**

ConnectionString is used to point to the correct database location. There must be only one uncommented ConnectionString entry in the **application.config** file.

By default, the line looks like this:

```
<add key="ConnectionString" value="Data Source=COMPUTER1-DT; Integrated Security=SSPI; Initial Catalog=AccessControl"></add>
```

The parameters for ConnectionString include the following:

### **Data Source**

Data Source specifies the name of the computer that hosts the database. If the database resides on the same computer where Database Setup will be run from you can use the name of your computer.

### **Integrated Security**

Integrated Security specifies how to authenticate with the database. This is done by indicating integrated authentication or by providing credentials.

For SQL Server users to use integrated authentication (single sign-on), the Integrated Security setting should be the following:

```
Integrated Security=SSPI
```

For Oracle users to use integrated authentication (single sign-on), the Integrated Security setting should be the following:

Integrated Security=True

If Lenel credentials for authentication with the database are stored in the **application.config** file then Integrated Security should be set to “No.” You must also specify the user name and password. In this case, the modified ConnectionString line would resemble the following:

```
<add key="ConnectionString" value="Data Source=COMPUTER1-DT; Integrated Security=No; User ID=LENEL; Password=<password>; Initial Catalog=AccessControl"></add>
```

Substitute the Lenel user password for <password>.

### **Initial Catalog**

Initial Catalog is the name of the database. If you installed OnGuard, you specified this name during the installation. By default, this is AccessControl.

### **DatabaseType**

The Database Type specifies the type of database that will be used with the OnGuard software. By default, the line resembles the following:

```
<add key="DatabaseType" value="SqlServer"></add>
```

### **Lnl.LicenseSystem.Client.Host**

Lnl.LicenseSystem.Client.Host is used to specify the host name of the machine running the License Server.

By default, the line looks like this:

```
<add key="Lnl.LicenseSystem.Client.Host" value="COMPUTER1-DT"></add>
```

### **Lnl.LicenseSystem.Client.Port**

Lnl.LicenseSystem.Client.Port is used to specify the port the License Server is listening on (8189 is the default).

By default, the line looks like this:

```
<add key="Lnl.LicenseSystem.Client.Port" value="8189"></add>
```

## SRConnectionString

SRConnectionString is used to specify the path to where the .mdb file is installed.

By default, the line looks like this:

```
<add key="SRConnectionString"
value="Provider=Microsoft.Jet.OLEDB.4.0; Data Source=C:\Program
Files\OnGuard\DBSetup\SR.mdb"></add>
```

## Data Source

The path specified in the Data Source must be consistent with where OnGuard is installed on the system.

## SchemaOwner

SchemaOwner is used to specify the path to where the .mdb file is installed.

By default, the line looks like this:

```
<add key="SchemaOwner" value="dbo"></add>
```

For SQL Server, the default setting is "dbo".

For Oracle, the default setting is "lenel".

## Error Log

The error log path is specified in the **application.config** file as well. It must be set to the path where the logs directory was installed. It is specified in the following line:

```
<add filename="C:\Program Files\OnGuard\logs\LnILogError.log"
name="StandardLog" output="file" severity="error" type="text"></add>
```

The default error log file for the browser-based client applications is **C:\Program Files\OnGuard\logs\LnILogError.log**. The **LnILogError.log** file is separate from the log file that the traditional OnGuard applications write to, which is **LenelError.log**.

# *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 on a Server](#) on page 41.
2. During the installation you are prompted to choose the system type. Select **Custom**.
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.

## ***Custom Features***

The following features are only available with a custom OnGuard installation.

### **Application Server**

This feature installs the Application Server components into your IIS Web server structure in order to serve Web versions of Area Access Manager, VideoViewer, Visitor Management, and Visitor Administration. This feature is only supported on systems running IIS.

Additional steps are required for the configuration of the Application Server. For more information, refer to [Chapter 9: Configuring the Web Application Server](#) on page 69.

### **Device Discovery Console**

This feature enables the discovery and maintenance of devices on a network or system. For more information, refer to the Device Discovery Console User Guide.

If the Device Discovery Console is selected for installation, WinPcap will also be installed. This is a third-party utility that is needed for the discovery of cameras. WinPcap has a separate license agreement.



## *Network Video over HTTP via Proxy*

---

This appendix describes the process by which video is displayed in the VideoViewer (Browser-based Client) and the network requirements for this setup.

---

### ***VideoViewer (Browser-based Client)***

The VideoViewer (Browser-based Client) supports viewing video over HTTP for connections outside of the internal network. This method of viewing video allows you to permit outside entities to view video while keeping the system secure. Viewing video over HTTP still enforces OnGuard user permissions; anyone that connects to VideoViewer must be authorized to login and view video.

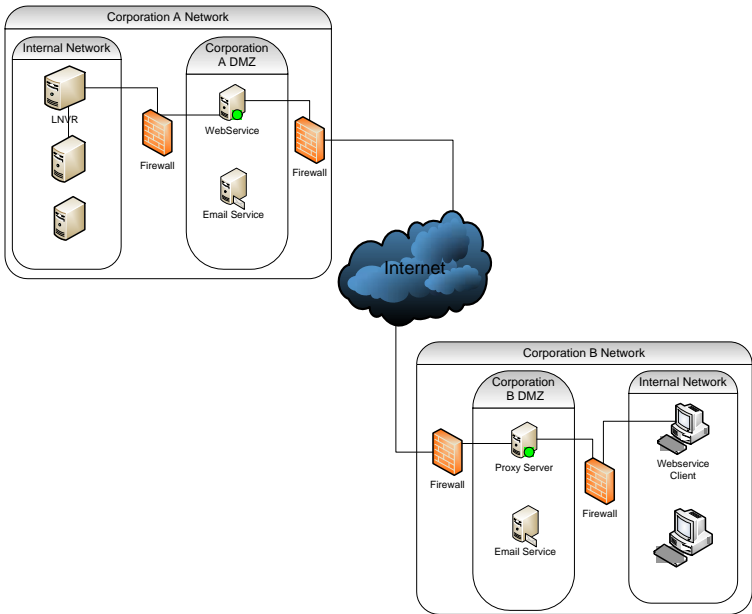
---

### ***Network Requirements***

VideoViewer (Browser-based Client) can connect directly to the Web Application Server or via proxy. The following diagram illustrates the scenario by which VideoViewer (Browser-based Client) retrieves LNVR video over HTTP via proxy.

In this diagram, the LNVR is located in Corporation A's internal network. VideoViewer can get video from the LNVR via the Web service located in Corporate A's demilitarized zone (DMZ). To support the VideoViewer through HTTP, Corporation A must expose the Web server's IP address to the external Internet and have port 80 (HTTP) and/or port 443 (HTTPS) open. If the Web service is running on Windows Vista, the client can have up to 10 connections depending on the proxy and firewall policy.

**Note:** A DMZ is a physical or logical sub-network that exposes an organization's external services to a larger, untrusted network.



---

# Index

---

## A

About accounts .....	104
Accounts .....	91
about .....	104
ADMIN .....	100
Lenel .....	100
SA .....	100
table of accounts .....	100
Application.config .....	113
file settings .....	116
modifying .....	113
Authentication .....	73

## B

Backup	
configure automatic file backup to tape .....	19
SQL Server database to file .....	16
SQL Server database to tape drive .....	19
SQL Server Express database to tape drive .....	19
Browser-based clients	
configuration .....	77
user permissions .....	77
Browser-based reports .....	74

## C

Change	
database password .....	102
Lenel account password .....	102
SYSTEM account password using Database Setup .....	105
system administrator password for the database .....	104
ClickOnce .....	83
Configuration Download Service .....	76
Configuration Editor utility .....	113
Configure	
automatic database file backup to tape drive .....	19
SQL Server 2008 .....	36
SQL Server for automatic database backup to file .....	16
Create	
database .....	36
login .....	37
Create the Lenel user	
SQL Server .....	37
Custom installation .....	119

## D

Daily maintenance	
-------------------	--

Server.....	110
Database authentication for the Web applications.....	59
Database backup overview .....	15
Database restoration .....	15
Database Setup	
change SYSTEM account password.....	105
Default accounts and passwords table... 100	
Deployment .....	84
Disable strong password enforcement .. ..	90, 101
DMZ.....	122
Dongle	
parallel port.....	43
USB .....	43

**E**

Enable strong password enforcement ... ..	90, 101
Enforce strong passwords check box.... ..	101
Error.....	86
Error logs.....	109
Error messages.....	91

**F**

Form Translator.....	70
----------------------	----

**H**

Hardware key	
parallel port.....	43
USB .....	43
Hot fix.....	108

**I**

IIS.....	71
Install	

Microsoft SQL Server 2008.....	29
OnGuard on a Client .....	57
OnGuard on a Server.....	41
OnGuard software .....	44
SQL Server (new installations)	
configuring SQL Server ..	36
SQL Server 2008 (new installations)	
create a login .....	37
run new query.....	38
Installation.....	85
custom .....	119
Installing	
license.....	48
OnGuard on a client .....	57
OnGuard on a server .....	41
Internet Information Services.....	71

**L**

Language Packs.....	109
Lenel account password	
change .....	102
License .....	48
License Administration	
logging into .....	49
Log Files.....	109
Logging in	
using automatic single sign-on ..	95
using manual single sign-on.....	95
without using single sign-on ....	92
Logging into License Administration	49
Login Driver.....	103
Login for SQL Server.....	37
Logs	
error logs .....	109

**M**

Maintenance	
daily.....	110
monthly .....	110
Monthly .....	110

**N**

New Query - running ..... 38

**O**

OnGuard ..... 100  
 client install..... 57  
 install..... 41  
 removing..... 107

**P**

Parallel port dongle..... 43

## Password

enable/disable strong password  
 enforcement ..... 90  
 overview ..... 89  
 SQL Server Express..... 47  
 standards ..... 90  
 weak database warning ..... 91

## Password change

inform administrators of the  
 password change ..... 105  
 write down ..... 105

## Passwords

case sensitivity ..... 101  
 change database password ..... 99  
 change Lenel account password ...  
 ..... 102  
 change the database password 102  
 change the SYSTEM account  
 password using Database  
 Setup ..... 105  
 change the system administrator  
 password for the database ...  
 104  
 disable strong password  
 enforcement ..... 101  
 enable strong password  
 enforcement ..... 101  
 Enforce strong passwords  
 checkbox ..... 101

enforcement when using single  
 sign-on ..... 99  
 Login Driver ..... 103  
 maximum length..... 101  
 minimum length..... 101  
 Oracle ..... 101  
 standards ..... 100  
 table of default passwords ..... 100

**R**

Remove..... 107

OnGuard ..... 107

## Run

New Query..... 38

**S**

Security policy..... 86

Security Utility ..... 47

## Software license

activate..... 52  
 repair..... 53  
 return..... 52

Software Licenses..... 48

## SQL Server

configure for automatic database  
 backup to file ..... 16  
 configure SQL Server..... 36  
 create database..... 36  
 create login ..... 37  
 create the Lenel user ..... 37

## SQL Server 2008

install ..... 29

## SQL Server Express

transfer database to new machine.  
 ..... 25  
 transferring ..... 25

## Strong password enforcement

disable..... 101  
 enable..... 101

SYSTEM account password - change...  
 ..... 105

**T**

Tape drive  
    backup..... 19  
Transfer a SQL Express database..... 25

**U**

USB devices  
    hardware key ..... 43  
User permissions  
    browser-based clients ..... 77

**V**

VideoViewer (Browser-based client)  
    user permissions ..... 76  
Visitor Management installation ..... 81  
VMware ..... 48

**W**

Weak database password warning..... 91  
Web Application Server  
    configuring ..... 69  
    custom install..... 70



Lenel Systems International, Inc.  
1212 Pittsford-Victor Road  
Pittsford, New York 14534 USA  
Tel 585.248.9720 Fax 585.248.9185  
[www.lenel.com](http://www.lenel.com)

[www.lenel.com](http://www.lenel.com)



A UTC Fire & Security Company

