# Table of Contents

## CHAPTER 1  About This Guide  ........................................ 9
- The Installation Guides ........................................... 10

## CHAPTER 2  Introduction  ........................................ 11
- Required Installations ........................................... 12
- Steps to Installing OnGuard .................................... 13
  - Installing OnGuard with SQL .................................. 13

## CHAPTER 3  Database Backup and Restoration  ................. 15
- Backing Up Your Database to File ............................... 15
  - Back Up to a File on SQL Server 2005 Database .......... 15
  - Back Up to a File on SQL Server 2005 Express Edition .. 17
- Backing Up to CD/DVD ........................................... 18
- Backing Up to Tape .............................................. 19
  - Back Up to Tape on SQL Server Database .................. 19
  - Back Up to Tape on SQL Server 2005 Express Edition ... 21
- Restoring Databases ............................................ 21
  - Restore the Database on SQL Server 2005 ................. 22
  - Restore the Database on SQL Server Express .............. 23

## CHAPTER 4  Transferring a SQL Server Express Database. 25
- Steps to Transfer a SQL Server Express Database .......... 25
  - Ensure Minimum Server Requirements are Met .......... 25
Table of Contents

Stop the SQL Server Service ........................................ 26
Copy Files from the Old Server to the New Server .............. 26
Restart the SQL Server Service ..................................... 26
Change the Database Owner ........................................... 27
Verify the Database Transfer was Successful ....................... 28

CHAPTER 5 Installing or Upgrading Microsoft SQL Server 29
Installing or Upgrading to SQL Server 2005 Express Edition .... 29
Installing SQL Server 2005 Express Edition ....................... 31
Installing or Upgrading to SQL Server 2005 Standard Edition .... 33
Installation Steps ....................................................... 34
Upgrade Steps ........................................................... 34
Installing SQL Server 2005 ............................................ 34
Configuring SQL Server 2005 .......................................... 36

CHAPTER 6 Installing OnGuard on a Server ................. 39
Install Prerequisites from the Supplemental Materials Disc .... 39
Configuring the Hardware Key ........................................ 40
Configure a Parallel Port Hardware Key ............................ 40
Configure a USB Hardware Key ....................................... 41
Install the OnGuard Software ......................................... 42
Running the Windows Security Utility ............................... 45
Install Your OnGuard License ........................................ 45
Log into the License Administration Application .................. 46
Changing Administrator Properties for the License Administration Application .................................................. 47
Install a New License ................................................. 48
Activate a Software License ......................................... 49
Return a Software License .............................................. 49
Repair a Software License ............................................. 50
Run Database Setup .................................................... 50

CHAPTER 7 Installing OnGuard on a Client Machine .... 53

CHAPTER 8 Database Authentication for the Web Applications ................................................................. 55
Windows Authentication with SQL Server .......................... 56
Configure Windows Authentication with SQL Server ............. 56
Configure Authentication for Reports in Area Access Manager .. 57
## Table of Contents

Windows Authentication with Oracle .......................... 60
  Configure Windows Authentication with Oracle .......... 60
Provide Credentials in the Protected File .................... 62
  Securing Files with the Access Control List. ............ 62
  Store the Lenel User Credentials .......................... 63

### CHAPTER 9  Configuring the Web Application Server . . . 65

Custom Install the Web Application Server .................. 66
Running Form Translator ........................................ 66
Internet Information Services (IIS) .......................... 67
  .Net Configuration with SQL Server ....................... 67
  Serving Dynamic Content with Windows Server 2003 ...... 68
  Creating Virtual Directories ................................ 68
  Configure SSL in Preferences.js ............................ 69
Authentication .................................................. 69
  Configure the LS Application Server Service Log On Account .. 69
Browser-based Reports ........................................ 70
  Install the Crystal .NET Components ...................... 70
  Configure Authentication for Reports in Area Access Manager. 70
  Enable the Reports Option .................................... 70
  Set Oracle Folder Permissions ............................... 71
Configuration Download Service ............................... 71
  Configure the Configuration Download Service Host ....... 72
OnGuard User Permissions ....................................... 72
  VideoViewer (Browser-based Client) ......................... 72
Client Configuration ........................................... 73
  Internet Browser Security Level ............................. 73
  Configure Single Sign-on for Browser-based clients ....... 73
  Accessing the Browser-based Applications .................. 74
  Video Player Installation ..................................... 75
  Viewing Reports in Area Access Manager .................... 75
  Create Bookmarks ............................................. 75

### CHAPTER 10  Logging Into the OnGuard System .............. 77

Windows User Permissions ....................................... 77
Passwords .......................................................... 77
  Password Standards ........................................... 78
  Enable/Disable Strong Password Enforcement ............... 78
  Error Messages ............................................... 79
  Accounts ...................................................... 79
# Table of Contents

Log In .................................................. 80  
Single Sign-On ......................................... 81  
  Directory Accounts ................................... 82  
  Automatic and Manual Single Sign-On ............ 82  
  Configure Single Sign-On ......................... 82  
  Log In Using Automatic Single Sign-On .......... 83  
  Log In Using Manual Single Sign-On ............. 83  
Single Sign-On for Browser-based Clients ........ 84  
  Configure the Web Server ......................... 84  
  Configure the Clients .............................. 85  
Troubleshoot Logging In .............................. 85  

## CHAPTER 11  Accounts and Passwords .............. 87  
Password Standards .................................... 88  
  Enable/Disable Strong Password Enforcement .... 89  
Change the Database Password ........................ 89  
  Change the Lenel Account Password .............. 90  
About Accounts ........................................ 92  
Change the System Administrator Password for the Database ........... 92  
  Step 1: Change the SYSTEM Account Password Using Database Setup .............................. 93  
  Step 2: Write Down and Inform Administrators of the Password Change ......................... 93  

## CHAPTER 12  Maintaining the OnGuard Installation .... 95  
Modify, Repair, or Remove OnGuard 2008 Plus .......... 95  
Remove OnGuard 2008 Plus ........................... 97  
OnGuard Fixes and Maintenance ......................... 97  
  Hot Fixes ............................................ 97  
  Third-Party Service Packs and Updates .......... 98  
  Language Packs .................................... 98  
  Log Files .......................................... 99  
  Server Maintenance ................................ 99  

## Appendices ........................................ 101  

**APPENDIX A  The Application.config File** .......... 103  
  Modifying the Application.config File ............ 103  

---  

6  

*Installation Guide*
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 installing 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.
The Installation Guides

The following table describes the different installation guides available.

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Item Number</th>
<th>Document Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Installation Topics</td>
<td>DOC-100</td>
<td>A guide that encompasses a variety of advanced topics including Oracle installation and configuration.</td>
</tr>
<tr>
<td>Installation Guide</td>
<td>DOC-110</td>
<td>A comprehensive guide that includes instructions for installing the OnGuard software. This guide also includes information on all supported SQL database systems and the browser-based client applications.</td>
</tr>
<tr>
<td>Upgrade Guide</td>
<td>DOC-120</td>
<td>A short and sequential guide on upgrading and configuring an OnGuard system that utilizes SQL Server or SQL Server Express.</td>
</tr>
</tbody>
</table>
Installing OnGuard® 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 2008 Plus disc.

**Important:** Lenel software requires certain security adjustments to operating systems using Windows Vista, Service Pack 2 or greater (Windows XP), or Service Pack 1 or greater (Windows Server 2003). For those who have installed the service packs a Lenel Windows Security Utility, which allows OnGuard to function properly, runs during installation. Please review the Lenel Windows 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, the OnGuard setup requires that you have administrative privileges.
- All prerequisite software, on the OnGuard 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.
- All workstations must be upgraded to the latest approved Windows service pack and Windows updates. See the release notes for specifics.
- 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 OnGuard 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 2008 Plus 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 to 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

1. Make sure you have the proper hardware requirements. For more information, refer to Install Prerequisites from the Supplemental Materials Disc on page 39.

2. Install IIS [Only if using the OnGuard browser-based applications]. For more information, refer to Internet Information Services (IIS) on page 67.

3. Install and configure SQL or SQL Server Express. For more information, refer to Chapter 5: Installing or Upgrading Microsoft SQL Server 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 39.

5. Configure the Hardware Key. For more information, refer to Configuring the Hardware Key on page 40.

6. Install the OnGuard software. For more information, refer to Install the OnGuard Software on page 42.


8. Install the OnGuard license. For more information, refer to Install Your OnGuard License on page 45.

9. Configure authentication with the database [Only if using the OnGuard browser-based applications]. For more information, refer to Chapter 8: Database Authentication for the Web Applications on page 55.

10. Run Database Setup. For more information, refer to Run Database Setup on page 50.

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 65.
12. Configure the client [Only if using the OnGuard browser-based applications]. For more information, refer to Client Configuration on page 73.

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

- http://<machinename>/IdvmHost
  Or, if you are using automatic single sign-on for the Visitor Management Host:
- http://<machinename>/idvmhost/Main.html?useAutomaticSSO=true
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.

**Backing Up Your Database to File**

This section includes information on how to:

- **Back Up to a File on SQL Server 2005 Database** on page 15
- **Back Up to a File on SQL Server 2005 Express Edition** on page 17

**Back Up to a File on SQL Server 2005 Database**

The following section will show you how to back up your SQL Server 2005 database to a file.
Configure Microsoft SQL Server for Automatic Database Backup to File

1. Click the Windows Start button, then select All Programs > Microsoft SQL Server 2005 > 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. 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].


7. The SQL Server Maintenance Plan Wizard is launched. 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 list.

13. In the Databases drop-down popup:
   a. Select the ACCESSCONTROL check box.
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 list, select “Overwrite”.
   c. Click [Add].

15. In the Select Backup Destination window, click [...].

16. In the Locate Database Files window:
   a. Type ACCESSCONTROL.bak in the File name field.
   b. Click [OK].
   c. Click [OK] in the Select Backup Destination window.
   d. 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 list, select “Automatic”.
   b. Click [OK].

**Back Up to a File on SQL Server 2005 Express Edition**

1. Click the Windows Start button, then select All Programs > OnGuard 2008 > 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. Name this file `AccessControlBackup`. 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 2005 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 file 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 2005 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, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**.
2. Click the Backup tab.
3. Navigate to the file that you wish to back up.
4. In the **Backup media or file name** drop-down list, select “Accesscontrol Backup”.
5. Select “Travan” in the **Backup destination** drop-down list.
   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].
6. A message is displayed. Click [Yes] to save the backup selections now.
7. 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].
8. 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].

9. The Scheduled Job Options window opens.
   a. In the **Job name** field, type *AccessControl* or any other name you would like to use.
   b. Click [Properties].

10. The Properties are displayed in the Schedule Job window.
    a. In the **Schedule task** drop-down list, 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].

11. In the Schedule Job window, click [OK].

12. 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 the Windows Control Panel, and then double-click “Scheduled Tasks”.

2. Right-click on the Accesscontrol task, and then select **Run**.

3. After a short delay, the backup runs.

4. To verify that the backup ran:
   a. Start the Windows Backup software. To do this, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Back up**. On Windows Vista, the backup software is called Backup Status and Configuration.
   b. Click the Restore and Manage Media tab.
   c. The backup is listed, as shown.
Back Up to Tape on SQL Server 2005 Express Edition

If you are using SQL Server 2005 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 2005 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, click the Start button, and then navigate to All Programs > Accessories > System Tools > Backup.
2. Click the Backup tab.
3. Navigate to the file that you wish to back up. In most cases, this will be the accesscontrol_backup file that is in the C:\Program Files\OnGuard\database_backup directory.
4. Select “Accesscontrol Backup” in the Backup media or file name drop-down list.
5. Select “Travan” in the Backup destination drop-down list.
6. Click [Start Backup].
7. 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.
8. Click [Start Backup].
9. 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 2005 on page 22
Restore the Database on SQL Server 2005

To restore a SQL Server 2005 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 22. 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 2005 Database From a File on page 22.

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, click the Start button, and then navigate to All Programs > Accessories > System Tools > Backup.

3. The Backup or Restore Wizard opens.

4. Click the Advanced Mode link.

5. Click the Restore and Manage Media tab.

6. Select “Travan”, and then navigate to the database that you wish to restore.

7. Click [Start Restore].

Restore Microsoft SQL Server 2005 Database From a File

1. Click the Windows Start button, then select All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio.

2. The SQL Server Management Studio window displays.
   a. Navigate to ACCESSCONTROL database.
b. Right-click on the ACCESSCONTROL database and select **Tasks > Restore > Database**.

3. The Restore database window displays.
   a. For the **To database** and **From database** drop-down lists, select “ACCESSCONTROL”.
   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 2005 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 22. 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 23.

**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 Lenel 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.
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 machine.

**Steps to Transfer a SQL Server Express Database**

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

- Ensure Minimum Server Requirements are Met on page 25.
- 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 navigate to the All Programs >
   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\MSSQL.1\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 navigate to the Start > 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, navigate to Prerequisite Software\Microsoft SQL Server 2005 Express on the Supplemental Materials disc and run SQLServer2005_SSMSEE.msi.

Change the Database Owner Using SQL Express Management Studio

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

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.

**Important:** The latest approved SQL Server 2005 service pack should also be installed. See the OnGuard release notes for specifics.

The following sections will show you how to install and upgrade your specific version of SQL Server.

- Installing or Upgrading to SQL Server 2005 Express Edition on page 29.
- Installing or Upgrading to SQL Server 2005 Standard Edition on page 33.

---

**Installing or Upgrading to SQL Server 2005 Express Edition**

**Important:** SQL Server 2005 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 2005 Express Edition. It is highly recommended that you install SQL Server 2005 Express Edition automatically. However, manual instructions are presented in the following section.

Microsoft SQL Desktop Edition (MSDE) has been replaced with SQL Server 2005 Express Edition.

To have SQL Server 2005 Express install automatically, use the .bat files (Express.bat/ExpressUpgrade.bat) found on the Supplemental Materials disc. The files can be found by navigating to Prerequisite Software\Microsoft SQL Server 2005 Express on the Supplemental Materials disc. It is vital that you read the instructions in this directory for specifics on how to run the files correctly.

If you would rather install SQL Server 2005 Express manually, follow the instructions presented in this section.

The installation and upgrade steps for SQL Server 2005 Express are very similar. Differences between installations and upgrades are noted in the appropriate steps.

When performing an upgrade, there should be nothing connected, i.e. 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.

If the SQL Server Native Client is installed on a system with MSDE, it can cause the upgrade to SQL Server 2005 Express to fail. Use Add or Remove Programs (or Programs and Features if using Windows Vista) to completely remove it prior to performing the upgrade.

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

**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.
Installing SQL Server 2005 Express Edition


1. On the Supplemental Materials disc, navigate to the Prerequisite Software > Microsoft SQL Server 2005 Express directory and run the SQLEXPR.EXE file.

2. In the End User License Agreement window:
   a. If you agree with the license terms, select I accept the licensing terms and conditions.
   b. Click [Next].

3. The Installing Prerequisites 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 >].

4. Click [Next] to begin the installation wizard.

5. The System Configuration Check will examine your system for prerequisites. After it has finished, click [Next].

6. In the Registration Information window:
   a. Enter the name and company information.
   b. Deselect Hide advanced configuration options.
   c. Click [Next].

7. In the Feature Selection window:
   a. Expand Client Components and select Entire feature will be installed on local hard drive for the Connectivity Components feature.
   b. Click [Next].

8. In the Instance Name window, select Default instance and click [Next].

9. Upgrade only: In the Existing components window, select the existing SQL Server installation and click [Next].

Important: The existing SQL Server component will be grayed out if you are running a version of MSDE that is not compatible with the
upgrade. You must install the most recent MSDE service packs prior to upgrading to SQL Server Express.

10. Upgrade only: In the Upgrade Logon Information window, select Windows Authentication Mode and click [Next].

11. Upgrade only: In the Service Account window:
   a. Select **Use the built-in System account**.
   b. Select **Local system** from the drop-down list.
   c. Deselect **SQL Browser**.

12. Installation only: In the Service Account window:
   a. Select **Use the built-in System account**.
   b. Select **Local system** from the drop-down list.
   c. Select **SQL Server** and deselect **SQL Browser**.
   d. Click [Next].

13. Installation only: In the Authentication Mode window:
   a. Select the **Mixed Mode** radio button.
   b. Choose and confirm a secure sa logon password.
   c. Click [Next].

14. Installation only: In the Collation Settings window click [Next].

15. In the User Instances window, deselect **Enable User Instances**. If using Windows Vista, select **Add user to the SQL Administrator role** and click [Next].

16. In the Error and Usage Report Settings window, deselect both options. Click [Next].

17. In the Ready to Install window, click [Install] to begin the installation.

18. After all of the Setup Progress items have been completed, click [Next].

19. In the Completing Microsoft SQL Server 2005 Setup window, click **Surface Area Configuration tool**. The Surface Area Configuration Tool is displayed.

   a. On the **Available privileges** section, select the user that you wish to grant administrator rights to.
b. Click the double-arrow button to move them to the **Privileges that will be granted to** section.

c. Click [OK].

21. The Surface Area Configuration Tool is displayed. Click **Surface Area Configuration for Services and Connections**.

22. In the SQL Server 2005 Surface Area Configuration window:

   a. Click **Remote Connections** in the navigation tree.

   b. Select the **Local and remote connections** and **Using both TCP/IP and named pipes** radio buttons.

   c. Click [OK].

23. A message is displayed instructing you to restart the Database Engine Service.

24. Windows Vista installations only: You must install SQL Server Service Pack 2 now. SP2 is optional for operating systems other than Vista.

25. Reboot the computer, even if you are not prompted to do so. This completes the installation of SQL Server 2005 Express edition. You are now ready to install OnGuard.

26. Upgrades only: You must synchronize the Lenel password with the Login Driver prior to logging in to OnGuard.

---

**Installing or Upgrading to SQL Server 2005 Standard Edition**

The instructions that follow are for the Standard edition. The installation and upgrade steps for SQL Server 2005 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 2005 on page 34.
   a. Create the Database on page 36.
   b. Create a Login on page 37.
   c. Run Query Analyzer on page 38.
   d. Set Memory Usage on page 38

Upgrade Steps

- Installing SQL Server 2005 on page 34
- Set Memory Usage on page 38

Installing SQL Server 2005


1. Insert the SQL Server 2005 disc.
   • If autorun is enabled, the Microsoft SQL Server 2005 splashscreen is automatically opened.
   • If the Microsoft SQL Server 2005 splashscreen does not automatically appear, click the Windows Start button, then select Run... In the Run window, browse for splash.hta on the disc drive. Alternatively, you can run splash.hta from Explorer. The Microsoft SQL Server 2005 splashscreen is displayed.

2. Click Server components, tools, Books Online, and samples.

3. In the End User License Agreement window:
   a. If you agree with the license terms, select I accept the licensing terms and conditions.
   b. Click [Next]

4. The Installing Prerequisites step will install any of the listed components that are missing from your system. Click [Install].
5. Click [Next] to begin the installation wizard.

6. The System Configuration Check will examine your system for prerequisites. After it has finished, click [Next].

7. In the Registration Information window, enter the name, company, and Product Key. Click [Next].

8. In the Components to Install window:
   a. Select SQL Server Database Services.
   b. Click [Advanced].

9. In the Feature Selection window, select **Entire feature will be installed on local hard drive** for the Database Services feature and Management Tools component under the Client Components feature. Click [Next].

10. In the Instance Name window, select **Default instance** and click [Next].

11. Upgrade only: The Existing components window is displayed.
   a. Select the check box for the version of SQL Server you are upgrading from.
   b. Click [Next].

12. Upgrade only: The Upgrade Logon Information window is displayed.
   a. Select the **SQL Server Authentication Mode** radio button.
   b. Enter the SQL Server account **Username** and **Password**.
   c. Click [Next].

13. In the Service Account window:
   a. Select **Use the built-in System account**
   b. Select **Local system** from the drop-down list.
   c. Select **SQL Server** and deselect **SQL Server Agent** and **SQL Browser**.
   d. Click [Next].

14. In the Authentication Mode window:
   a. Select the **Mixed Mode** radio button.
   b. Choose and confirm a secure sa logon password.
   c. Click [Next].

Upgrades: This screen will not be displayed.
15. In the Collation Settings window click [Next].
   Upgrades: This screen will not be displayed.

16. In the Error and Usage Report Settings window, deselect both options. Click [Next].

17. In the Ready to Install window, click [Install] to begin the installation.

18. After all of the Setup Progress items have been completed, click [Next].

19. In the Completing Microsoft SQL Server 2005 Setup window, click [Finish].

20. Windows Vista installations only: You must install SQL Server Service Pack 2 now. SP2 is optional for operating systems other than Vista.

21. Reboot the computer, even if you are not prompted to do so. This completes the installation of SQL Server 2005. You can now go on to configure SQL Server 2005.

Configuring SQL Server 2005

Create the Database

1. Click the Windows Start button, then select All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio. This launches the SQL Server Management Studio.

2. In the Object Explorer pane, expand the Databases folder. Right click on the Databases folder and select New Database.

3. The New Database window is displayed. On the General page:
   a. In the Database name field, type ACCESSCONTROL (this is case insensitive).
   b. Verify the Use full-text indexing check box is not selected.
   c. Set the Initial Size (MB) of the Data file to 50.
   d. Set the Initial Size (MB) of the Log file to 10.

4. Select the Options page from the Select a page pane.
   a. Change the Recovery model drop-down to Simple.
   b. Verify the Compatibility level drop-down is set to SQL Server 2005 (90).
c. In the Other options list view, set Auto Shrink, Auto Update Statistics, Auto Create Statistics, and Recursive Triggers Enabled 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
Installing or Upgrading Microsoft SQL Server

- tempdb
  b. Click [OK].

6. The new login will appear in the Logins folder.

Run Query Analyzer

1. In the Object Explorer pane of the SQL Server Management Studio, right-click on the ACCESSCONTROL database and select New Query.

2. The Query tab is displayed.
   a. In the text window, type `sp_changedbowner lenel`
   b. Press <F5> to execute the command you typed.
   c. The message “The command(s) completed successfully” is displayed in the Messages tab window.
   d. Press <F5> to execute the command you typed.
   e. The message “The 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.

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.
CHAPTER 6

Installing OnGuard on a Server

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 OnGuard 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 OnGuard 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
• 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.

• Microsoft XML Parser - required for the Video Player application

• Microsoft .NET Framework 2.0 and 3.5 - Required if installing the browser-based applications. This is not necessary for Windows Vista Installation.

3  Install your database system.

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. For information on activating a software license, refer to Install Your OnGuard License on page 45.

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

There are two types of hardware security 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, no special configuration is needed for the hardware key; simply attach the hardware key to the parallel port.
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 Rainbow USB hardware key driver by doing the following:
   a. Navigate to the Rainbow directory on the OnGuard 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/Rainbow.
   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 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 installation wizard begins. Click [Install] to begin installation. Microsoft .NET Framework 3.5 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 65.

7. Choose your database.
Install the OnGuard Software

Note: SQL Server 2005 Express Edition is 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 2005 Express Edition. It is highly recommended that you install SQL Server 2005 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.
   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.

   • 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 operating systems using Windows Vista, Service Pack 2 or greater (Windows XP) or Service Pack 1 or greater (Windows Server 2003). For those who have installed the service packs a Windows Security Utility, which allows OnGuard to function properly, runs during installation. Please review the Windows Security Utility release notes provided prior to running this utility, which then makes these adjustments automatically. Upon agreeing to the 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.

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 Windows Security Utility**

Lenel software requires certain security adjustments to operating systems using Windows Vista, Service Pack 2 or greater (Windows XP) or Service Pack 1 or greater (Windows Server 2003). For those who have installed the service packs a Windows Security Utility, which allows OnGuard to function properly, runs during installation. Please review the Windows 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 Windows Security Utility also needs to be run whenever any update to the operating system takes place.

To run the Windows Security Utility manually:

1. Click **Start > All Programs > OnGuard 2008 > Windows Security Utility**.
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...
Installing OnGuard on a Server

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. Software licenses can only be used on a physical computer or in a VMware ESX virtual environment.

**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.

**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 the License Administration Application**

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 2008 > 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 the License Administration Application**

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

1. Log into the License Administration application.

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 the License Administration application.
4. Log into the License Administration application.
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 49.
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 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:** 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 103.

1. Click the Windows Start button, then select **All Programs > OnGuard 2008 > 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 66.
Installing OnGuard on a Server
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 it on each computer and the second is to install it remotely from the server. Installing it 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 56
     - Configure Windows Authentication with Oracle on page 60
  2. Provide Credentials in the Protected File on page 62

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. You may also choose to utilize an existing Windows user for authentication and skip this step.

1. From the Start menu, select Settings > Control Panel > User Accounts.
2. Select the Advanced tab and click [Advanced].
3. Right-click the Users folder and select New User.
4. Enter the User name and choose and confirm a password for the new user.
5. Deselect User must change password at next logon.
7. Click [Create].

Add the Windows user to SQL Server

1. Click the Windows Start button, then select Programs > Microsoft SQL Server 2005 > 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 username.
   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 ACCESSCONTROL database from the Users mapped to this login list.
   b. In the Database role membership for: ACCESSCONTROL list select (check):
      • db_owner
      • public
   c. Click [OK].

7. 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: 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 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.log.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 AccessControl.

4. Find the `<add key="reportDatabaseUsername" ... >` line verify that the value is empty.

5. Find the `<add key="reportDatabasePassword" ... >` line and verify that the value is empty.

6. 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*.


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.

Note: 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.

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.

Windows Authentication with Oracle

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

Create a new Windows user

Create a new Windows user to run the LS Application Server. You may also choose to utilize an existing Windows user for authentication and skip this step.

1. From the Start menu, select *Settings > Control Panel > User Accounts.*
2. Select the Advanced tab and click [Advanced].
3. Right-click the Users folder and select *New User.*
4. Enter the *User name* and choose and confirm a password for the new user.
5. Deselect *User must change password at next logon.*
6. Select *Password never expires.*
7. Click [Create].

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 and edit it.
   • Oracle 10g: \oracle\product\10.1.0\Db_1\NETWORK\ADMIN
   • Oracle 9i: \oracle\ora92\Network\Admin
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\lnl
   • On Windows Vista: Navigate to C:\ProgramData\lnl
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.

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 70.

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.
3. 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>;
   ```
4. On the same line, change the Integrated Security value to:
   ```
   Integrated Security=No;
   ```
5. 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.og.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 AccessControl.
   • 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 AccessControl 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 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 Service is running under.

7. Save and exit the Web.config file.
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 XP or Windows Server 2003; the Web Application Server is not supported on Windows Vista.

Note: The instructions that follow are for Windows Server 2003; they may vary for other versions of Windows. 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.

Use a 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 109.

---

**Running Form Translator**

The Form Translator must be run after the Web Application Server is installed. The Web Application Server enables the browser-based applications to be run. To run the Form Translator follow these steps:

1. Navigate to the OnGuard installation directory.
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 68.

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, the Preferences.js file must be updated with the new URL. For more information, refer to Configure SSL in Preferences.js on page 69.

.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 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.
4. Select the ASP.NET tab.
5. In the ASP.NET version drop-down list, select 2.0.
6. Repeat steps 3 through 5 for ln1.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 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.Web-Service\ 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 Protection should be medium.
- Directory Security > Anonymous access and authentication control should have Integrated Windows authentication selected.
Configure SSL in Preferences.js

Refer to IIS documentation for SSL configuration instructions. Once SSL has been configured with IIS, complete the following steps:

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

2. Locate the var g_lnl_pfx_webservice_serverAddress line and change http to https.

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 the Web Applications on page 55.

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 username 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.
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 Windows 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 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 the Web Applications on page 55.

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:

   ```javascript
   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)
**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 [OK].
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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveX controls and plug-ins &gt; Automatic prompting for ActiveX controls</td>
<td>Enable</td>
</tr>
<tr>
<td>Downloads &gt; File Download</td>
<td>Enable</td>
</tr>
<tr>
<td>Miscellaneous &gt; Access data sources across domains</td>
<td>Prompt</td>
</tr>
</tbody>
</table>

   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 81.

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 or IP address and the location of the application on the web application server. 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.

<table>
<thead>
<tr>
<th>Application</th>
<th>URL</th>
</tr>
</thead>
</table>
Note: If SSL is configured the web address will begin with https.

**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.

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

<table>
<thead>
<tr>
<th>Application</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor Management</td>
<td>http://&lt;server-name&gt;/IdvmHost/</td>
</tr>
<tr>
<td>Host</td>
<td>Or, if automatic single sign-on is enabled:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;server-name&gt;/idvmhost/</td>
</tr>
<tr>
<td></td>
<td>Main.html?useAutomaticSSO=true</td>
</tr>
</tbody>
</table>
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® 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 81.

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 (e.g. SA, SA).
- Passwords cannot be Lenel keywords.
- Although not required, your password should contain numbers, letters, and symbols. Spaces are also acceptable. (e.g. 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 78.

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

**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:

<table>
<thead>
<tr>
<th>User name</th>
<th>Password</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa</td>
<td>sa</td>
<td>system account</td>
</tr>
<tr>
<td>admin</td>
<td></td>
<td>sample</td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>sample</td>
</tr>
<tr>
<td>badge</td>
<td></td>
<td>sample</td>
</tr>
</tbody>
</table>

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 81. To log in using single sign-on, refer to Configure Single Sign-On on page 82.

1. Click the Start button, then select **All Programs > OnGuard 2008**. 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** (Light-weight 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 2008 > [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 2008 > [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.
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].
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.log.web and lnl.log.webservices web sites.

**Edit the Preferences.js file**

1. Navigate to the Lnl.OG.Web directory and edit the Preferences.js file.
2. Locate the `var g_lnl_pfx_webservice_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 73.

---

**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 2008 Plus 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 89.
The following table summarizes the OnGuard default accounts and passwords:

**OnGuard Default Accounts and Passwords**

<table>
<thead>
<tr>
<th>Description</th>
<th>User name</th>
<th>Password</th>
<th>How to change the password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default system administrator account. This is the account that is used initially to log into the main OnGuard applications, such as System Administration.</td>
<td>SA</td>
<td>SA</td>
<td>For more information, refer to About Accounts on page 92.</td>
</tr>
<tr>
<td>OnGuard database. This is the actual OnGuard SQL Server Express, SQL, or Oracle database.</td>
<td>LENEL</td>
<td>MULTIMEDIA</td>
<td>For more information, refer to Change the Database Password on page 89.</td>
</tr>
<tr>
<td>License Administration account. This is the account that is used initially to log into the License Administration application.</td>
<td>ADMIN</td>
<td>ADMIN</td>
<td>For more information, refer to Install Your OnGuard License on page 45.</td>
</tr>
</tbody>
</table>

**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 (e.g. SA, SA)
- Passwords cannot be Lenel keywords.
- Although not required, your password should contain numbers, letters, and symbols. Spaces are also acceptable. (e.g. august 18, 1967)
- 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 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 deselected 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 program (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. How the database password is changed depends whether the Login Driver is running on the same computer that the database is on, and what options you choose to use. The SQL Server Express, Oracle, or SQL Server password and the password in the Login Driver must be the same or you will not be able to log into any OnGuard applications. SQL Server Express, Oracle, and SQL Server passwords case-insensitive, but the password in the Login Driver is case-sensitive.

- If the Login Driver and the database are on different computers, you have two options: (For more information, refer to step d on page 91.)
  - Change the database password, and change the password in the Login Driver manually later
  - Change the database password in the Login Driver as well. If you choose this option, be aware that 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**.
   
   d. Proceed to step 2.

2. If the password is considered weak, the Database Server Account Passwords window is displayed. Refer to **Password Standards** on page 88 to determine a secure password.

3. Click [Continue]. If you wish to change the password for a database server account now, i.e., “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 90.

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:

<table>
<thead>
<tr>
<th>User name</th>
<th>Password</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa</td>
<td>sa</td>
<td>system account</td>
</tr>
<tr>
<td>admin</td>
<td></td>
<td>sample</td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>sample</td>
</tr>
<tr>
<td>badge</td>
<td></td>
<td>sample</td>
</tr>
</tbody>
</table>

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.

**Step 1: 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 90, with the following exception: in step 3 on page 90, select the system account from the list (“SA” by default), then click [Change Password].

**Step 2: 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.

Modify, Repair, or Remove OnGuard 2008 Plus

Note: OnGuard can be removed more quickly by following Remove OnGuard 2008 Plus on page 97.

Note: If you choose to repair OnGuard you will need to reset your DSN name, license server name, and any other custom setting made to the ACS.INI and/or application.config file. You may want to back up the ACS.INI and/or application.config before doing any maintenance.

1. To modify, repair, or remove your existing OnGuard installation, go to Windows Control Panel, select Add or Remove Programs (or Programs and Features if using Windows Vista), select OnGuard 2008, and click [Change].
   • If autorun is enabled, the Installation & Configuration window will automatically be opened.
• If the Installation & Configuration window does not automatically appear, click the Windows Start. Click the Run... popup menu choice.

• In the Run window, select setup.exe from the disc drive. Alternatively, you can run Setup from Explorer.

2. The Maintenance Wizard opens. Click [Next].

3. The Maintenance Type window opens. Click one of the following radio buttons:

• Modify – to add or remove programs from the existing build. Select if you want to install components that were previously left uninstalled or remove components that are no longer needed.

• Repair – to automatically attempt to repair shortcuts, deleted files, etc., that were deleted by the user.

• Remove – to remove OnGuard and all of its components from the hard drive.

If you chose the Modify or Repair option, click [Next] to continue. If you chose the Remove option, the [Next] button is replaced by a [Remove] button. Click [Remove] to remove OnGuard 2008 from your computer.

4. What happens next depends on what option you chose.

• If you chose the Repair option, click [Install] to repair the program.

• If you chose the Modify option, the Custom Setup window is displayed. Select the OnGuard features you wish to have installed or those you want to remove.

  a. 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 OnGuard feature are displayed.

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

  c. Click [Next] to continue.

  d. The Ready to Modify the Program window is displayed. Click [Install].

5. A status meter will indicate the progress of the installation or removal.

6. Click [Finish].

7. Reboot the computer if you are prompted to do so.
Remove OnGuard 2008 Plus

OnGuard can be removed by following these steps:

1. In the Control Panel:
   a. Double-click “Add or Remove Programs”. In Windows Vista this is called “Programs and Features”.
   b. In the Currently installed programs listing window, select “OnGuard 2008 Plus”.
   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 2008 Plus 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 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 OnGuard 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 OnGuard Supplemental Materials disc. See the release notes or 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 2003
- Windows Vista

Note: The Windows 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
- Microsoft 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 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
- LnILogError.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 (i.e., 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\Ln\ in Windows XP or C:\ProgramData\Ln\ in Windows Vista. 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\lnl
• On Windows Vista: Navigate to C:\ProgramData\lnl
• Click the Start button, then select All Programs > OnGuard 2008 > 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 2005, 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 (i.e. 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
Application.config File Settings

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 "Lenel" for Oracle.
- **SRCConnectionString**: This refers to the path to the .mdb file.
- **Error Log**: This refers to the path to logs directory.

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.

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:

```xml
<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:

```xml
<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:

```xml
<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:

```xml
<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:

```xml
<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:

```xml
<add filename="C:\Program Files\OnGuard\logs\LnlLogError.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\LnlLogError.log`. The `LnlLogError.log` file is separate from the log file that the traditional OnGuard applications write to, which is `LenelError.log`. 
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 Installation**

1. Begin installing the OnGuard software. For more information, refer to Chapter 6: Installing OnGuard on a Server on page 39.
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.

**Existing OnGuard Installation**

1. Navigate to Windows Control Panel.
2. Click **Add or Remove Programs**.
3. In the list of currently installed programs, select OnGuard and click [Change].
4. The OnGuard maintenance wizard opens. Click [Next].
5. Select Modify and click [Next].
6. In the custom setup screen, select which features you wish to install.

**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, and Visitor Management. 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 65.

**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.
Index

A
About accounts .................................. 92
Accounts ............................................. 79
about ......................................... 92
ADMIN..................................... 88
Lenel ......................................... 88
SA ............................................. 88
table of accounts ....................... 88
Application.config ........................... 103
file settings.............................. 105
modifying ......................... 103
Authentication ........................................ 69

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............................. 73
user permissions ....................... 72
Browser-based Reports...................... 70

C
Change
database password ..................... 89
Lenel account password ......... 90
SYSTEM account password using Database Setup .......... 93
system administrator password for the database .......... 92
Configuration Download Service ..... 71
Configuration Editor utility .......... 103
Configure
automatic database file backup to tape drive ................. 19
SQL Server 2005 ...................... 36
SQL Server for automatic database backup to file .......... 16
Create
database ......................... 36
login.......................................... 37
Create the Lenel user
SQL Server ......................... 37
Custom installation........................ 109

D
Daily maintenance
Server........................................ 99
Database Authentication for the Web Applications.......................... 55
Database backup overview ........................................... 15
Database restoration ........................................... 15
Database Setup
change SYSTEM account password.................................. 93
Default accounts and passwords table 88
Disable strong password enforcement.............................. 78, 89
Dongle
parallel port........................................... 40
USB ........................................... 41
Enable strong password enforcement.............................. 78, 89
Enforce strong passwords check box 89
Error logs ........................................... 99
Error messages ........................................... 79
Form Translator ........................................... 66
Hardware key
parallel port........................................... 40
USB ........................................... 41
Hot fix........................................... 97
IIS ........................................... 67
Install
Microsoft SQL Server ........................................... 29
OnGuard on a Client ........................................... 53
OnGuard on a Server ........................................... 39
OnGuard software ........................................... 42
SQL Server 2005 (new installations) ................................ 33
configure SQL Server 2005 ........................................... 36
create a login ........................................... 37
run SQL Query Analyzer ........................................... 38
SQL Server Express ........................................... 29
Installation
custom ........................................... 109
Installing
license ........................................... 45
OnGuard on a client ........................................... 53
OnGuard on a server ........................................... 39
Internet Information Services ........................................... 67
Language Packs ........................................... 98
Lenel account password change ........................................... 90
License ........................................... 45
License Administration
logging into ........................................... 46
Log Files ........................................... 99
Logging in
using automatic single sign-on ........................................... 83
using manual single sign-on ........................................... 83
without using single sign-on ........................................... 80
Logging into License Administration 46
Login Driver ........................................... 91
Login for SQL Server ........................................... 37
Logs
erorr logs ........................................... 99
Maintenance
daily ........................................... 99
monthly ........................................... 99
Monthly ........................................... 99
OnGuard ........................................... 88
client install ........................................... 53
install......................................... 39
removing..................................... 97

P
Parallel port dongle............................ 40
Password
  enable/disable strong password
    enforcement .......................... 78
  overview ................................ 77
  standards ............................... 78
  weak database warning .............. 79
Password change
  inform administrators of the
    password change ....................... 93
  write down ................................ 93
Passwords
  case sensitivity ......................... 88
  change database password ............ 87
  change Lenel account password ....... 90
  change the database password ....... 89
  change the SYSTEM account
    password using Database Setup ... 93
  change the system administrator
    password for the database .......... 92
  disable strong password
    enforcement .......................... 89
  enable strong password
    enforcement .......................... 89
Enforce strong passwords
  checkbox .................................. 89
  enforcement when using single
    sign-on ................................. 87
Login Driver .................................. 91
  maximum length .......................... 89
  minimum length .......................... 89
Oracle........................................ 89
  standards ................................ 88
  table of default passwords .......... 88

Q
Query Analyzer - running.................. 38

R
Remove........................................... 97
  OnGuard ..................................... 97
Run
  Query Analyzer ............................ 38

S
SQL Server
  configure for automatic database
    backup to file .......................... 16
  configure SQL Server 2005 ............ 36
  create database .......................... 36
  create login ............................. 37
  create the Lenel user ................... 37
  install ..................................... 29
  new installations ....................... 33
  upgrade .................................... 29
SQL Server 2005 Express
  transfer database to new machine ......... 25
SQL Server Express
  install ....................................... 29
  transferring ............................. 25
Strong password enforcement
  disable ..................................... 89
  enable ...................................... 89
SYSTEM account password - change 93

T
Tape drive
  backup ...................................... 19
Transfer a SQL 2005 Express database
  ............................................ 25

U
Upgrade
Index

SQL Server ........................................ 29
USB devices
  hardware key .......................... 41
User permissions
  browser-based clients ............ 72

V

VideoViewer (Browser-based client)
  user permissions ............... 72

W

Weak database password warning.... 79
Web Application Server
  configuring .......................... 65
  custom install ...................... 66
Windows Security Utility .......... 45