ReadykeyPRO Unlimited
Upgrade Guide

BOSCH

Bosch ReadykeyPRO® Unlimited Upgrade Guide, product version 6.5. This guide is item number DOC-120-2-023, revision 2.023, July 2012.

Table of Contents

CHAPTER 1 About This Guide

This guide will walk you through the processes for upgrading your ReadykeyPRO system. It also includes steps to upgrade SQL Server and SQL Server Express. You can also find information on maintaining your ReadykeyPRO installation. The vocabulary used:

Database System
Refers to the database program that you are using. SQL Server databases can be found in this document.

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 ReadykeyPRO software is installed.

Hardware Key
Commonly referred to as a "dongle." It is used on the server as part of the license.

Software License

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

The Installation Guides

The following table describes the different installation guides available.

Document Name	Item Number	Document Description
Advanced Installation Topics	DOC-100-2-032	A guide that encompasses a variety of advanced topics.
Installation Guide	DOC-110-2-029	A comprehensive guide that includes instructions for installing the ReadykeyPRO software. This guide also includes information on all supported SQL Server database systems and the browser-based client applications.
Upgrade Guide	DOC-120-2-023	A short and sequential guide on upgrading and configuring an ReadykeyPRO system that utilizes SQL Server or SQL Server Express.

CHAPTER 2 *Introduction*

Upgrading ReadykeyPRO® involves only three general steps: upgrading the system database, installing the upgraded license, and upgrading the ReadykeyPRO software.

Before beginning 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 ReadykeyPRO installation. Please refer to the release notes for those requirements, which are located on the root of the ReadykeyPRO Unlimited installation disc.

Direct upgrades can be performed for all versions of ReadykeyPRO that are currently supported. To check your software version log into any ReadykeyPRO application and click, **Help > About** in the menu bar. For more information please contact your Bosch representative.

Important: Bosch software requires certain security adjustments to the operating system to function more securely. If needed, the Security Utility runs during installation. Please review the Security Utility release notes provided prior to running this utility, which then makes these adjustments automatically. Upon agreeing to this disclaimer, the user is assuming

responsibility for any security issues that may occur due to these adjustments.

Required Installations

The following must be installed before installing ReadykeyPRO:

- If using Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, the ReadykeyPRO setup requires that you have administrative privileges.
- All third-party requirements on the Supplemental Materials disc must be installed.
- Each ReadykeyPRO computer must be configured for the TCP/IP network protocol prior to installation of the ReadykeyPRO software.
- All workstations must be upgraded to the latest approved Windows service pack. See the release notes for specifics.
- All database systems must be upgraded to a supported version with the latest approved service pack. Refer to the ReadykeyPRO release notes for specific information.
- The latest approved drivers are required for any video capture devices and printers you have installed on workstations.
- ReadykeyPRO 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 Upgrading ReadykeyPRO

The following steps will show you how to upgrade your ReadykeyPRO installation. Read the instructions carefully and use them as a guide while you upgrade. Upgrades can be performed by a member of the Administrators Group.

Upgrading ReadykeyPRO with SQL Server

Important: The ReadykeyPRO database must be backed up. It is ***CRITICAL*** that you have an up-to-date backup of the database before you begin the upgrade process.

1. Manually decommision End of Life hardware. For more information, refer to End of Life Hardware and Data Considerations on page 12.
2. If you manually decommisioned any hardware, back up the database. The backup should not contain decommisioned hardware.
3. Stop all of the Bosch services.
4. If you are using any custom .dll files you must back these up prior to upgrading the ReadykeyPRO software. Back up the custom .dll files now.
5. Install IIS (only if using the ReadykeyPRO browser-based applications). For more information, refer to Internet Information Services (IIS) for Windows Server 2003 on page 64. This is not necessary for Windows Vista, Windows 7, or Windows Server 2008 R2 installations as these operating systems do not support running the browser-based applications.
6. Upgrade SQL Server or SQL Server Express. For more information, refer to Upgrading to SQL Server 2008 Express Edition on page 16.
7. Upgrade the ReadykeyPRO software. For more information, refer to Upgrading ReadykeyPRO on page 51.
8. The upgrade process assumes your ReadykeyPRO 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 Appendix A: The application.config File on page 93.
9. Start the Login Driver in application mode from the ReadykeyPRO menu and sync the Lenel password by clicking **Edit > Change Password**. You might need to know the SA password to do this, as you are asked for it during the process in some configurations. For more information, refer to the *Accounts and Passwords* chapter in the Installation guide.
10. Configure authentication with the database. For more information, refer to Chapter 6: Database Authentication for Web Applications on page 41.

11. If your ReadykeyPRO database is called anything other than "AccessControl" and the Database Setup portion of Setup Assistant did not run successfully, you must run Database Setup and Form Translator manually. For more information, refer to Run Database Setup on page 60.
12. Install the Web Application Server (only if using the ReadykeyPRO browser-based applications). For more information, refer to Chapter 8: Configuring the Web Application Server on page 63. The system is now upgraded.

    To access the browser-based applications, the link syntax is as follows (where *<machinename>* is the location of the Web Application Server):

    - For Area Access Manager — http://*<machinename>*/lnl.og.web/lnl_og_aam.aspx
    - For VideoViewer — http://*<machinename>*/lnl.og.web/lnl_og_videoviewer.aspx
    - For Visitor Management Host — http://*<machinename>*/IdvmHost

      Or, if manually logging into Visitor Management Host — http://*<machinename>*/IdvmHost/?useAutomaticSSO=false
    - For Visitor Administration — http://*<machinename>*/AdminApp

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

    - For Front Desk installation — http://*<machinename>*/FrontDeskClickOnce
    - For Kiosk installation — http://*<machinename>*/KioskClickOnce

End of Life Hardware and Data Considerations

Refer to the following:

- "Hardware that must be removed manually" on page 13 lists hardware that you must decommission in the field and delete manually from the ReadykeyPRO system using System Administration.

- "Smart Card formats that must be removed manually" on page 13 lists the Smart Card formats that you must delete manually from the ReadykeyPRO system using System Administration.
- "Data that will be removed automatically" on page 14 lists data that Database Setup will remove automatically during the upgrade process.

Hardware that must be removed manually

- AAD Readers
- AMD-12 Input Panels
- Apollo Hardware
- Asset Reader Interfaces
- Cisco AIC Hardware
- Digitize CAPSII Receivers
- Identix Fingerscan V20 Readers
- LNVS Hardware

Smart Card formats that must be removed manually

- Cartographer Smart Card Format
- CombiSmart Smart Card Format
- GSC (DESFire) Smart Card Format
- GuardDog Smart Card Format
- IE Smart Touch Smart Card Format
- Offline Guest Smart Card Format
- TI Access Control Smart Card Format
- UltraScan Smart Card Format

- Windows Certificate Smart Card Format

Data that will be removed automatically

- Identix Fingerprint Templates
- Ultrascan Fingerprint Templates
- Biocentric Fingerprint Templates

CHAPTER 3 *Microsoft SQL Server 2008*

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

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

Important: If you have SQL Server 2005 Express installed on your system, the database software will not be automatically upgraded during the ReadykeyPRO upgrade. If you want to upgrade your database software, instructions for upgrading from SQL Server 2005 Express to SQL Server 2008 Express are provided in this chapter.

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

Prerequisites

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

- Microsoft .NET Framework 4.0
- Microsoft Windows Installer 4.5 or later
- Microsoft Windows PowerShell 1.0

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

SQL Server 2008 Express Edition

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

Upgrading to SQL Server 2008 Express Edition

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

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

When performing an upgrade, there should be nothing connected, that is, no clients logged on. There can be no software connections to the database when the upgrade is performed, so all ReadykeyPRO 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 ReadykeyPRO applied.

1. On the ReadykeyPRO disc, navigate to the **Temp\SQLExpress** directory and run:
   - **SQLEXPR_x86_ENU.exe** for 32-bit systems or
   - **SQLEXPR_x64_ENU.exe** for 64-bit systems.
2. The SQL Server Installation Center is displayed. Click **Installation** from the left pane, then click **Upgrade from SQL Server 2000 or SQL Server 2005**.

3. The Setup Support Rules window will identify potential problems that might occur during installation. You must correct any failures before setup can continue. If no problems are identified, click [OK].
4. In the Product Key window, click [Next].
5. In the License Terms window:
   a. If you agree with the license terms, select **I accept the license terms**.
   b. Click [Next].
6. In the Setup Support Files window, click [Install].
7. After the setup files have been installed, the Setup Support Rules will run again to identify potential issues. You must resolve any failures before setup can continue. Once the check has completed successfully, click [Next].
8. In the Select Instance window, select the existing SQL Server installation from the drop-down and click [Next].
9. In the Select Features window, click [Next].
10. In the Instance Configuration window, click [Next].
11. Review the Disk Space Requirements information and click [Next] if you have sufficient space.
12. In the Error and Usage Report Settings window, deselect both options. Click [Next].
13. The Upgrade Rules window will determine if there are any barriers to the installation process. If there are no failures, click [Next].
14. In the Ready to Upgrade window, click [Upgrade] to begin the installation.
15. Once the setup process is complete, you will be notified that you need to restart your computer to complete the process. Click [OK] to close the message, then click [Next].
16. In the Complete window, click [Close] to exit.
17. You will receive another message to remind you to restart your computer. Your computer will not automatically be restarted; you must manually restart your computer to complete the upgrade process.

Installing SQL Server Management Tools

SQL Server Management Studio is required if the server intends to use Database Authentication or Windows single sign-on. The SQL Server Management Studio software and instructions for installation are available on the Supplemental Materials disc.

SQL Server 2008 Standard Edition

The instructions that follow are for the Standard edition. The installation and upgrade steps for SQL Server 2008 are very similar. Special considerations for upgrades are noted in the appropriate steps. When performing an upgrade, there should be nothing connected, that is: no clients logged on. There can be no software connections to the database when the upgrade is performed, so all ReadykeyPRO LS and LPS services including the LS Communication Server must be stopped.

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

Installation Steps

To perform the installation, complete the following steps:

1. Installing SQL Server 2008 on page 19.
2. Configuring SQL Server 2008 on page 21.
    a. Create the Database on page 21.
    b. Create a Login on page 22.
    c. Set Memory Usage on page 24.
    d. Set Memory Usage on page 24.

Upgrade Steps

- Installing SQL Server 2008 on page 19.
- Set Memory Usage on page 24.

Installing SQL Server 2008

Note: SQL Server 2008 setup requires Microsoft .NET Framework 4.0 and Windows Installer 4.5. If you do not have these prerequisites prior to installing SQL Server 2008, the setup will prompt you before installing them.

1. Insert the SQL Server 2008 disc.
   - If autorun is enabled, the SQL Server Installation Center is automatically opened.
   - If the SQL Server Installation Center does not automatically appear, click the Windows Start button, then select **Run**. In the Run window, browse for **setup.exe** on the disc drive. Alternatively, you can run **setup.exe** from Windows Explorer.
2. The SQL Server Installation Center is displayed. Click **Installation** from the left pane, then:
   - For new installations, click **New SQL Server stand-alone installation or add features to an existing installation**.
   - For upgrades, click **Upgrade from SQL Server 2000 or SQL Server 2005**.
3. The Setup Support Rules window is displayed. You must correct any failures before setup can continue. If no problems are identified, click [OK].
4. The Product Key window is displayed. Enter your product key and click [Next].
5. In the License Terms window:
   a. If you agree with the license terms, select **I accept the license terms**.
   b. Click [Next].
6. The Setup Support Files step will install any of the listed components that are missing from your system.
   a. Click [Install].
   b. Once the prerequisite installation is complete, click [Next].
7. Upgrade only: In the Select Instance window, select the **Instance to upgrade** from the drop-down and click [Next].
8. In the Feature Selection window:

a. Under Instance Features, select **Database Engine Services**, **SQL Server Replication**, and **Full-Text Search**.

b. Under Shared Features, select **Management Tools - Basic** and **Management Tools - Complete**.

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

c. Click [Next].

9. In the Instance Configuration window:
   - For new installations, select **Default instance** and click [Next].
   - For upgrades, the **Named instance** should already be selected. Click [Next].
10. Review the Disk Space Requirements information and click [Next] if you have sufficient space.
11. The Server Configuration window is displayed.
    - For new installations, select "NT AUTHORITY\SYSTEM" from the **Account Name** column drop-down for SQL Server Agent and SQL Server Database Engine. Click [Next].
    - For upgrades, click [Next].
12. Upgrade only: In the Full-text Upgrade window, click [Next].
13. Installation only: In the Database Engine Configuration window:
    a. Select the **Mixed Mode** radio button.
    b. Enter and confirm a password for the SQL Server system administrator account.
    c. Click [Add].
    d. In the Select Users or Groups window, click [Advanced].
    e. Change the **From this location** field to the local machine by clicking [Locations] and selecting the local machine from the list.
    f. Click [Find Now], then select Administrators from the Search results listing window.
    g. Click [OK], then click [OK] again to close the Select Users or Groups window.
    h. The BUILTIN\Administrators group should now appear in the Specify SQL Server administrators listing window. Click [Next].

14. In the Error and Usage Report Settings window, deselect both options. Click [Next].
15. The Installation Rules or Upgrade Rules window will determine if there are any barriers to the installation process. If there are no failures, click [Next].
16. In the Ready to Install or Ready to Upgrade window, click [Install] or [Upgrade] to begin the installation.
17. After all installation progress has completed, click [Next].
18. In the Complete window, click [Close].
19. Reboot the computer, even if you are not prompted to do so. This completes the installation of SQL Server 2008. You can now go on to configure SQL Server 2008.

Configuring SQL Server 2008

Create the Database

1. Click the Windows Start button, then select **All Programs** > **Microsoft SQL Server 2008** > **SQL Server Management Studio** to start the SQL Server Management Studio.
2. Select your method of authentication, provide credentials if required, and click [Connect].
3. In the Object Explorer pane, expand the Databases folder. Right-click the Databases folder and select **New Database**.
4. The New Database window is displayed. On the General page:
   a. In the **Database name** field, type `ACCESSCONTROL` (this is case-insensitive).
   b. Set the Initial Size (MB) of the Data file to 50.
   c. Set the Initial Size (MB) of the Log file to 10.
   d. Scroll to the right in the Database files listing window and click the browse button in the Autogrowth column of the log file row.
   e. Select the **Restricted File Growth (MB)** radio button and set a maximum log file size. The recommended maximum log file size is 2048.
   f. Click [OK].

5. Select the Options page from the **Select a page** pane.
   a. Change the **Recovery model** drop-down to “Simple”.
   b. Verify that the **Compatibility level** drop-down is set to “SQL Server 2005 (90)” or “SQL Server 2008 (100)”.
   c. In the Other options list view, set the **Auto Shrink**, **Auto Update Statistics**, **Auto Create Statistics**, and **Recursive Triggers Enabled** drop-downs to “True”.
   d. Click [OK].

Create a Login

1. In the Object Explorer pane of the SQL Server Management Studio, expand the Security folder.
2. Right-click the Logins folder and select **New Login**.
3. In the General page of the Login window:
   a. In the **Login name** field, type `LENEL`.
   b. Select the **SQL Server authentication** radio button.
      - For **Password**, type `MULTIMEDIA`.
      - For **Confirm password**, type `MULTIMEDIA`.

Note: The SQL Server password is case-sensitive.

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

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

4. Recommended settings for user:

Note: For advanced users who do not want the database owned by **Bosch**, proceed to step 5 on page 23.

a. Select **Server Roles** from the **Select a page** pane, and then select (check) the following:
   - dbcreator
   - serveradmin

b. Select **User Mapping** from the **Select a page** pane, and then select the following databases from the Users mapped to this login list:
   - master
   - tempdb

c. Click [OK].

d. The new login appears in the **Logins** folder.

e. In the **Object Explorer** pane of SQL Server Management Studio, right-click on the ReadykeyPRO database and select **New Query**. A query tab is shown.

f. In the text window, type `sp_changedbowner lenel`.

g. Press <F5> to execute the command.

h. The message **Command(s) completed successfully** is shown in the **Messages** tab.

i. Click the close ("X") button to close the query tab, then click [No] when prompted if you want to save the changes.

j. Proceed to "Set Memory Usage" on page 24.

5. For advanced users, the minimum required user settings are:

a. In the **Object Explorer** pane of SQL Server Management Studio, right-click on the ReadykeyPRO database and select **New Query**. A query tab is shown.

b. In the text window, type:
   - `CREATE ROLE db_executor`
   - `GRANT EXECUTE TO db_executor`

c. Press <F5> to execute the command.

d. The message **Command(s) completed successfully** is displayed in the **Messages** tab.

e. Click the close ("X") button to close the query tab, then click [No] when prompted if you want to save the changes.

f. Select **Server Roles** from the **Select a page** pane, and then select (check) the following:
   - public

g. Select **User Mapping** from the **Select a page** pane, and then select the ACCESSCONTROL database.

h. Select (check) the following roles:
   - public
   - db_datareader
   - db_datawriter
   - db_ddladmin
   - db_executor

i. Click [OK].

j. The new login appears in the **Logins** folder.

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

Set Memory Usage

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

Truncate the Log File

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

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

CHAPTER 4

Database Backup and Restoration

Important: If upgrading, the ReadykeyPRO database must be backed up. It is ***CRITICAL*** that you have an up-to-date backup of the database before you begin the upgrade process.

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

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

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

Note: Some of the procedures in this chapter require the use of SQL Server Management Studio. If have SQL Server 2008 Express Edition and you do not have the SQL Server Management Studio Express application, you can install the application from the Supplemental Materials disc.

Backing Up Your Database to File

This section includes information on how to:

Back Up to a File on SQL Server 2008 Database

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

Configure Microsoft SQL Server for Automatic Database Backup to a File

1. Click the Windows Start button, then select ***All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio***.
2. Log into SQL Server Management Studio.
3. Navigate to the SQL Server Agent in the Object Explorer.
   a. Right-click the SQL Server Agent and select **Start**.
   b. You will be asked whether you are sure that you want to start the service, click [Yes].
   c. Right-click the SQL Server Agent and select **Properties**.
4. The SQL Server Agent Properties window is displayed.
   a. Select the **Auto restart SQL Server if it stops unexpectedly** and **Auto restart SQL Server Agent if it stops unexpectedly** check boxes.
   b. Click [OK].
5. Expand the Management folder in the Object Explorer.
6. Right-click on the Maintenance Plans folder and select **Maintenance Plan Wizard**.
7. The SQL Server Maintenance Plan Wizard is displayed. Click [Next].
8. On the Select Plan Properties window:
   a. In the **Name** field, enter a name for the maintenance plan.
   b. Click [Change].
9. The Job Schedule Properties window is displayed.

a. For **Name**, enter a name for the schedule.
b. Set the frequency for the backup to occur.
c. Click [OK].
d. Click [Next] in the Select Plan Properties window.

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

Back Up to a File on SQL Server Express Edition

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

Backing Up to CD/DVD

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

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

1. Back up your database to a file. For more information, refer to Backing Up Your Database to File on page 28.
2. Right-click on the file(s) to be backed up and click [Send to]. Choose the CD or DVD writable drive on your computer.
3. You receive a message that files are waiting to be backed up.
4. Click on the My Computer icon on your desktop and double-click the CD or DVD drive that you saved the files to. You should see the files you want to burn.
5. Make sure the proper media is in the drive and click **File** in the menu bar and select **Write these files to CD/DVD**.

6. The CD/DVD writing wizard opens. Follow the on screen instructions to burn your files to CD/DVD.

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

Backing Up to Tape

This section includes:

Back Up to Tape on SQL Server Database

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

1. Start the Windows Backup software. To do this:
   - In Windows XP and Windows Server 2003, click the Start button, and then navigate to ***All Programs > Accessories > System Tools > Backup***.
   - In Windows 7 or Windows Server 2008 R2 open Control Panel and open the Backup and Restore Center.
   - In Windows Server 2008, open Control Panel and navigate to **Admin Tools > Windows Server Backup**.
2. If the Wizard starts, click the Advanced Mode link.
3. Click the Backup tab.
4. Navigate to the file that you want to back up.
5. In the **Backup media or file name** drop-down, select “Accesscontrol Backup”.
6. Select “Travan” in the **Backup destination** drop-down.
   a. Click [Start Backup].

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

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

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

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

Verify that the Backup Ran

1. Start the Windows Backup software. To do this:
   a. In Windows XP and Windows Server 2003, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**. In Windows 7 or Windows Server 2008 R2, open Control Panel and open the Backup and Restore Center. In Windows Server 2008, open Control Panel and navigate to **Admin Tools** > **Windows Server Backup**.
   b. Click the Restore and Manage Media tab.
   c. The backup is listed.

Back Up to Tape on SQL Server 2008 Express Edition

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

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

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

1. Start the Windows Backup software. To do this:
   - In Windows XP and Windows Server 2003, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**.
   - In Windows 7 or Windows Server 2008 R2, open Control Panel and open the Backup and Restore Center.

- In Windows Server 2008, open Control Panel and navigate to **Admin Tools** > **Windows Server Backup**.

2. If the wizard starts, click the Advanced Mode link.
3. Click the Backup tab.
4. Navigate to the file that you want to back up. In most cases, this will be the **accesscontrol_backup** file that is in the **C:\Program Files\ReadykeyPRO\database_backup** directory.
5. Select "Accesscontrol Backup" in the **Backup media or file name** drop-down list.
6. Select "Travan" in the **Backup destination** drop-down.
7. Click [Start Backup].
8. The Backup Job Information window opens.
   a. In the **Backup description** field, type `Accesscontrol Backup`.
   b. In the **If the media is overwritten, use the label to identify the media** field, type `Accesscontrol Backup`.
9. Click [Start Backup].
10. The backup will run. The Backup Progress window displays, and the backup is complete.

Restoring Databases

This section includes:

Restore the Database on SQL Server 2008

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

1. Restore the database in the tape drive to a file by running the Windows Backup software. For more information, refer to Restore the Database

from a Tape Drive on page 35. If you backed up to a CD or DVD then you can skip this step and go on to the next step.

2. Restore the file to the database via the SQL Server Management Studio. For more information, refer to Restore Microsoft SQL Server 2008 Database from a File on page 35.

Restore the Database from a Tape Drive

1. Insert the tape that contains the database that you wish to restore into the proper drive.
2. Start the Windows Backup software. To do this:
   - In Windows XP and Windows Server 2003, click the Start button, and then navigate to **All Programs > Accessories > System Tools > Backup**.
   - In Windows 7 or Windows Server 2008 R2, open Control Panel and open the Backup and Restore Center.
   - In Windows Server 2008, open Control Panel and navigate to **Admin Tools** > **Windows Server Backup**.
3. If the wizard starts, click the Advanced Mode link.
4. Click the Restore and Manage Media tab.
5. Select "Travan", and then navigate to the database that you wish to restore.
6. Click [Start Restore].

Restore Microsoft SQL Server 2008 Database from a File

1. Click the Windows Start button, then select **All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio.**
2. The SQL Server Management Studio window displays.
   a. Navigate to ReadykeyPRO database.
   b. Right-click on the ReadykeyPRO database and select **Tasks > Restore > Database**.
3. The Restore database window displays.
   a. For the **To database** and **From database** drop-downs, select the ReadykeyPRO database.

   b. Click the Options page from the Select a page list view.
4. The Options page is displayed.
   a. Select the **Overwrite the existing database** check box.
   b. Click [OK].
5. A success message is displayed. Click [OK].

Restore the Database on SQL Server Express

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

1. Restore the database in the tape drive to a file by running the Windows Backup software. For more information, refer to Restore the Database from a Tape Drive on page 35. 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 ReadykeyPRO Database Backup utility. For more information, refer to Restore the File to the Database on page 36.

Restore the File to the Database

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

CHAPTER 5

Transferring a SQL Server Express Database

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

Steps to Transfer a SQL Server Express Database

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

- Back up the SQL Server Express database. Refer to Back Up to a File on SQL Server Express Edition on page 30 or Back Up to Tape on SQL Server 2008 Express Edition on page 33.
- Ensure Minimum Server Requirements are Met on page 37.
- Stop the SQL Server Service on page 38.
- Copy Files from the Old Server to the New Server on page 38.
- Restart the SQL Server Service on page 38.
- Change the Database Owner on page 39.
- Verify the Database Transfer was Successful on page 40.

Ensure Minimum Server Requirements are Met

Make sure that the new server meets the specifications that are listed in the current release notes. Although the server MUST meet

the minimum specifications listed, your system will perform much better if the server also meets the recommended specifications.

Stop the SQL Server Service

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

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

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

Copy Files from the Old Server to the New Server

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

Restart the SQL Server Service

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

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

Change the Database Owner

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

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 ReadykeyPRO database and select **New Query**.
2. The Query tab is displayed.
   a. In the text window, type `sp_changedbowner`
   b. Press <F5> to execute the command you typed.
   c. The message "Command(s) completed successfully" is displayed in the Messages tab window.
3. Click the close ("X") button to close the Query tab, then click [No] when prompted if you want to save the changes.

Change the Database Owner Manually

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

1. On the taskbar, click the Start button, and then click **Run**.
2. Click [Browse], navigate to the ReadykeyPRO 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.
   b. Type the following: `sp_changedbowner sa`
   c. Click [OK]. If the command gets highlighted in blue, then it completed without error, and you are ready to enter the next command.
   d. Type the following: `sp_changedbowner`
   e. 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.

CHAPTER 6 *Database Authentication for Web Applications*

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

- Systems using browser-based ReadykeyPRO applications.

There are two methods of authentication available:

1. Authenticate Windows with the database.
   - Refer to Configure Windows Authentication with SQL Server on page 41, or
   - Windows Authentication with Oracle on page 70.
2. Provide Credentials in the Protected File on page 46

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

Windows Authentication with SQL Server

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

Configure Windows Authentication with SQL Server

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

Create a new Windows user

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

Add the Windows user to SQL Server

1. Click the Windows Start button, then select ***Programs > Microsoft SQL Server 2008 > SQL Server Management Studio***. This launches the SQL Server Management Studio.
2. In the Object Explorer pane of the SQL Server Management Studio, expand the Security folder.
3. Right-click the Logins folder and select **New Login**.
4. In the General page of the Login window:
   a. In the **Login name** field, type *server-name**username*, where *server-name* is the name of the server and *username* is the name of the Windows user.
   b. Select the **Windows authentication** radio button.
5. Click [Search] to launch the Select User or Group dialog. This dialog is used to verify that the Login name is correct.
   a. In the **Enter the object name to select** text box, enter the user name.
   b. Click [Check Names]. If the user is found it will appear underlined.
   c. Click [OK].
6. Select User Mapping from the Select a page pane.
   a. Select (check) the `<Server Name>` database from the Users mapped to this login list.
   b. In the Database role membership for `<Server Name>`, the recommended settings are (check):
      - db_owner
      - public

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

- db_datawriter
- db_ddladmin
- db_executor

Note: If the db_executor role does not already exist, refer to step 5a through step 5e on page 23.

c. Click [OK].

The new login will appear in the Logins folder.

Verify the Integrated Security Setting

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

1. Open the **application.config** file to edit.
   - On Windows XP or Windows Server 2003: Navigate to **C:\Documents and Settings\All Users\Application Data\lnl**
   - On Windows 7, Windows Server 2008, or Windows Server 2008 R2: Navigate to **C:\ProgramData\lnl.** You may need to show hidden folders.
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.

Note: If you do not want to use Windows authentication you can also store the Bosch credentials in the **Web.config** file. For more information, refer to Provide Credentials in the Protected File on page 46.

Edit the Web.config File

1. Navigate to ***C:\Inetpub\wwwroot\lnl.og.webservice*** and edit the **Web.config** file.
2. Find the `<system.web>` line and add the following line below it:
   `<identity impersonate=“true” />`

3. Find the `<add key="reportDSN" ... >` line and verify that the value is equal to the DSN name for connection to the database.
4. Find the `<add key="reportDatabase" ... >` line and verify it is set to the correct database name. By default this value is set to AccessControl.
5. Find the `<add key="reportDatabaseUsername" ... >` line and set the value to `"LENEL"`.
6. Find the `<add key="reportDatabasePassword" ... >` line and set the value to the LENEL account password.
7. Save and exit the file.

Disable Anonymous Access in Windows

1. Right-click My Computer and select ***Manage***.
2. Expand ***Services and Applications > Internet Information Services***.
3. Right-click Web Sites and select ***Properties***.
4. Select the Directory Security tab.
5. In the Authentication and access control section, click [Edit].
   a. Deselect (uncheck) the **Enable anonymous access** check box.
   b. Select the **Integrated Windows Authentication** check box.
   c. Click [OK].
   d. Click [OK].
6. The Inheritance Overrides dialog is displayed.
   a. Click [Select All].
   b. Click [OK].

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 ReadykeyPRO 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.

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

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 7: Navigate to **C:\ProgramData\Inl**
2. Find the `<add key="ConnectionString" ...>` line and verify that Integrated Security is set to True.

Provide Credentials in the Protected File

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

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

Important: When providing credentials in a protected file, the ODBC authentication method must not be set to Windows authentication. This is the default configuration unless the ODBC was manually created.

Securing Files with the Access Control List

The Access Control List (ACL) is a highly secure method of protecting information stored within a file. ReadykeyPRO 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 can be used to store the user credentials when reports are used with Area Access Manager through a browser. This is only necessary if you are not using Windows authentication.

Application.config

The **application.config** file can be used to store the 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 and Windows authentication is not being used.

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 User Credentials

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

Note: For information on storing 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\lnl**
   - On Windows 7 or Windows Server 2008 R2: Navigate to **C:\ProgramData\lnl**
2. Find the `<add key="ConnectionString" ...>` line and add the following to the existing information inside of the quotes ("") in the `value` attribute where *<password>* is the LENEL user password:

`User ID=LENEL;Password=`*<password>*`;`

3. On the same line, change the Integrated Security value to:
   `Integrated Security=No;`
4. Save and exit the file.

Configure Authentication for Reports in Area Access Manager

If you want to use reports with Area Access Manager (Browser-based Client) without using Windows authentication, credentials also must be provided and secured in the **Web.config file**.

Note: If you are using Windows authentication this procedure is not necessary for browser-based reports.

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 and verify it is set to the correct database name. 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.
4. Find the `<add key="reportDatabaseUsername" ... >` line and set the value to `"LENEL"`.
5. Find the `<add key="reportDatabasePassword" ... >` line and set the value to the LENEL account password.
6. The user that the Web Application Service is running under needs permission to create and delete files from the directory set in the reportTemporaryFilePath line.
   a. Find the following line and either leave the default path or type a different directory location: `<add key="reportTemporaryFilePath" value="C:\Temp\LnlWebServiceReports\"></add>`
   b. Create the Windows directory specified in the reportTemporaryFilePath value.

c. Grant permission to create and delete files in the directory to the user that the Web Application Service is running under.

7. Save and exit the **Web.config** file.

CHAPTER 7 *Upgrading ReadykeyPRO*

Important: For information on hardware and data that must be decommisioned from the system prior to upgrading ReadykeyPRO, refer to "End of Life Hardware and Data Considerations" on page 12.

Upgrading ReadykeyPRO consists of upgrading the software, the licenses (if a major upgrade) and the database. The following chapters will show you how to upgrade the software, install a new license, and upgrade the database.

This is just one step in the upgrade process. Please refer to the Introduction chapter for a list of processes that must be completed before attempting an ReadykeyPRO upgrade.

Install Prerequisites

Before you install ReadykeyPRO you must first install the third-party requirements from the Supplemental Materials disc. Windows Service Packs are also required but are not provided on the Supplemental Materials disc. See the ReadykeyPRO 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 ReadykeyPRO documentation.

1. 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. This is not necessary for Windows Vista installations as Vista does not support running the browser-based applications.
2. Insert the Supplemental Materials disc.
3. Install the components that are needed from the prerequisites section:
   - Adobe Reader - required to read the ReadykeyPRO help documentation
   - Microsoft DirectX - required on all machines running ReadykeyPRO
4. Install your database system.
5. Restart your computer.

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 Installing Your ReadykeyPRO License on page 57.

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

USB hardware keys are available for use with ReadykeyPRO. Remember to physically attach the hardware key (“dongle” adapter) directly to the USB port on the computer that has License Server installed in order for the software to run properly.

A hardware key is only needed on the server running License Server.

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

Configure a USB Hardware Key

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

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

To configure a USB hardware key:

1. Install the SafeNet USB hardware key driver by doing the following:
   a. Navigate to the **SafeNet** directory on the Supplemental Materials disc and then double-click the .exe file. This can be found by navigating through the following folders on the Supplemental Materials disc: **/License Key Drivers/SafeNet**.
   b. The InstallShield Wizard starts. Click [Next].
   c. The wizard continues, and the License Agreement window opens. Select the **I accept the terms in the license agreement** radio button, and then click [Next].
   d. The wizard continues, and the Setup Type window opens. Select the **Custom** radio button, and then click [Next].
   e. On the custom screen 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. A message warning that you must not have the hardware key attached to the computer displays. Make sure that the hardware key is not attached to the computer, and then click [Install].
   g. The wizard completes. Click [Finish] to exit the wizard.
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.

Upgrading ReadykeyPRO

Note: Before beginning the upgrade process, make sure that you have an up-to-date backup of the ReadykeyPRO database.

ReadykeyPRO services should be stopped on all computers. These services must not be restarted until the upgrade is complete. For those services that are configured for automatic start up, temporarily change them to manual start up. All services with the prefix LS or LPS should be shut down. Users should not run any ReadykeyPRO applications during the installation process.

Important: Be sure all ReadykeyPRO applications are closed on all client computers. Failure to do so will result in the Communications Server to function improperly.

The ReadykeyPRO database server should be upgraded first. This must be done before upgrading any client computers.

All ReadykeyPRO client computers can be upgraded once the database server has been upgraded. This includes all Archive Servers. Software must not be restarted on a client computer until it has been upgraded. As client computers are upgraded, ReadykeyPRO software (including Bosch services) can be restarted. It is not necessary to wait until ALL clients are upgraded to restart software on a client computer that has been upgraded.

Upgrading between major releases may require the installation of a new license. For more information, refer to Installing Your ReadykeyPRO License on page 57.

Your upgrade procedure may vary slightly depending on what build of ReadykeyPRO you have installed. After the software is upgraded the Database Setup program must be run to upgrade the ReadykeyPRO database. For more information, refer to Run Database Setup on page 60.

Upgrade ReadykeyPRO

1. Insert the ReadykeyPRO Unlimited disc into a computer running the Windows operating system.
   - Click the Windows Start button on the taskbar. Click the **Run...** popup menu choice. In the Run window, select **setup.exe** from the disc drive. Alternatively, you can run **setup.exe** from Explorer.
2. You may be asked to install Microsoft .NET Framework 4.0. Click [Install] to begin installation. Microsoft .NET Framework 4.0 must be installed for some ReadykeyPRO features to work correctly.
3. 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 [Next].
4. A check is performed to see if your system contains any unsupported hardware, custom reports and/or DataExchange scripts. If your system contains custom reports or scripts then they may not work correctly after you upgrade. You are prompted as to whether you would like to continue with the upgrade process.

   ReadykeyPRO now uses Coordinated Universal Time (UTC) for events, user transactions, visits and alarm acknowledgments. You must run the Universal Time Conversion utility after your system has been fully upgraded to convert these times to the UTC format so that reports and visits will work correctly. For more information, refer to Appendix D: Universal Time Conversion Utility on page 105. If you choose not to run the conversion utility then older data will not report the time in UTC. All new data will be reported correctly.

   If you choose to continue be aware that any custom reports and/or DataExchange scripts may no longer work correctly. Please refer to Appendix C: Deprecated Fields for a list of columns that are affected by the new use of UTC.
5. Click [Install]. Before the installation begins you will be asked to stop the Windows Management Instrumentation (WMI) service. This is done automatically after you confirm that you wish to stop the service. If any other services depend on the WMI service, they must also be stopped.

6. After Windows configures ReadykeyPRO, ReadykeyPRO will be upgraded, and the status and progress bar will be updated as the upgrade progresses.

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

7. Depending on the components that were installed, you may need to reboot the computer. If you are prompted to do so, reboot the computer.

Running the Security Utility

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

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

To run the Security Utility manually:

1. Click **Start > All Programs > ReadykeyPRO Unlimited > System Tools > Security Utility**.
2. Click [More Info] to review the Security Utility release notes.
3. Click [Agree] if you agree with the disclaimer notice.
4. Follow the on screen instructions and click [Apply] when ready.

Installing Your ReadykeyPRO License

You must have a license to run the ReadykeyPRO software. The license comes to you from Bosch 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.

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.

Log into the License Administration Application

1. Make sure that the License Server is running. The License Server must run on the server specified in the **ACS.INI** file.
2. Click the Windows Start button, then select **All Programs** > **ReadykeyPRO Unlimited** > **System Tools > 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.
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.

Note: 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.

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.

Install a New License

1. Obtain a new license file from Bosch. 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 the license 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.
11. Select the **Yes** radio button if you agree with the terms of the license.
12. 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.

Sync the Login Driver and Database Passwords

When performing an upgrade, the Bosch password used by the Login Driver and the database must be synchronized prior to running Database Setup.

1. Stop the LS Login Driver service.

Note: It may take a few additional moments for the service to stop completely.

2. Start the Login Driver as an application. Click the Windows Start button, then select **All Programs > ReadykeyPRO Unlimited > Service and Support > Login Driver**.
3. Open the Login Driver application by double clicking the Login Driver icon in the System Tray.
4. Use the Change Password dialog to synchronize the passwords:
   a. From the **Edit** menu, select **Change Password**.
   b. A message should be displayed indicating that the passwords are out of sync. Click [Yes] to change the password.
5. The Change Password dialog is displayed.
   a. Type the Bosch password in the **Old password**, **New password**, and **Confirm password** text boxes to sync the passwords. By default the Bosch password is “MULTIMEDIA”.
   b. Click [OK].
6. After the passwords have been synchronized the system will perform a weak password scan. Click [Close].
7. From the **File** menu, select **Exit** to close the Login Driver application.
8. Start the LS Login Driver service.

Configure Windows Authentication

This step only needs to be completed if you plan on using the browser-based applications.

For more information, refer to Chapter 6: Database Authentication for Web Applications on page 41.

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: If upgrading a database from versions of ReadykeyPRO earlier than ReadykeyPRO 2005 Second Edition (5.11.216), the installation utility notifies you that it cannot perform the upgrade because the database is too old. The solution is to go to http://www.boschsecurity.us/en-us/readykeypro and then click Support > Downloads. Under Software > Legacy Database Setup, read the Readme file, and then download and unzip the 5.11.216 Database Setup file. Run the StpDB.exe file, and then run Database Setup again..

Important: The installation and upgrade process assumes your ReadykeyPRO 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 Appendix A: The application.config File on page 93.

1. Click the Windows Start button, then select **All Programs > ReadykeyPRO Unlimited > Service and Support > 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 4: Database Backup and Restoration on page 27. If your database is backed up click [Yes].
4. The database will install. If upgrading the database, the system will be checked for anomalies. Anomalies are database features that are

unknown to ReadykeyPRO 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. If you are uncertain on how to proceed please contact your Bosch representative.

5. Run Form Translator. To run Form Translator, follow these steps:
   a. Navigate to the ReadykeyPRO installation directory.
   b. Run **Lnl.Tools.FormTranslator.exe**.
   c. If Form Translator fails, simply perform these steps again.

Upgrading Other Bosch Components

- If the new release contains updated Bosch controller firmware, this can be downloaded to the Bosch controllers. It is not necessary to do this immediately, but it should be done as soon as it is convenient. New features will not be available until the firmware is updated. Sites with a large number of controllers may find it useful to schedule firmware downloads via the Scheduler application.
- If the new release contains updated Bosch interface gateway firmware, this can be downloaded to the interface gateways. It is not necessary to do this immediately, but it should be done as soon as it is convenient.

CHAPTER 8 *Configuring the Web Application Server*

Important: When installing or upgrading ReadykeyPRO, you must choose to do a custom installation to install the Web Application Server, which is required on the server to use browser-based applications. The Web Application Server feature requires IIS running on Windows Server 2003 or Windows Server 2008; the Web Application Server is not recommended for use on Windows XP or Windows 7 because the number of client connections to IIS is limited.

The Web Application Server feature enables the use of browser-based applications on client machines that may not have ReadykeyPRO installed. The Web Application Server deploys the minimal software needed for the Web applications on first use, communicates with the ReadykeyPRO 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 ReadykeyPRO database.

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 ReadykeyPRO database.

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

Custom Install the Web Application Server

After IIS has been installed, use the ReadykeyPRO “Custom Installation” to install the Web Application Server component. This step can be performed during the initial installation of ReadykeyPRO or as a modification to an existing system. For more information, refer to Appendix B: Custom Installation of ReadykeyPRO on page 99.

Running Form Translator

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

To run the Form Translator follow these steps:

1. Navigate to the ReadykeyPRO installation directory.
2. Run **Lnl.Tools.FormTranslator.exe.**
3. If Form Translator fails, simply perform these steps again.

Internet Information Services (IIS) for Windows Server 2003

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 ReadykeyPRO. As such, Bosch is not responsible for IIS configuration and maintenance other than the steps outlined for ReadykeyPRO functionality. Technical Support assistance will be provided specific to the installation, enablement, and base functionality of IIS per ReadykeyPRO 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 65.

Use of SSL to ensure security across the network when using browser-based applications is highly recommended. Refer to IIS documentation for additional IIS and SSL configuration if desired. Once SSL has been configured, several files must be updated with the new URL. For more information, refer to Configure SSL on page 66.

.NET Configuration with SQL Server

1. Right-click My Computer and select **Manage**.
2. In the Computer Management tree, expand ***Services and Applications > Internet Information Services > Web Sites > Default Web Site***.
3. Right-click lnl.og.web and select **Properties**.
4. Select the ASP.NET tab.
5. In the **ASP.NET version** drop-down, select 4.0.
6. Repeat steps 3 through 5 for lnl.og.webservices.

Serving Dynamic Content with Windows Server 2003

By default Windows Server 2003 only serves static content. If the Web Application Server is running Windows Server 2003, it must be configured to serve dynamic content. Consult your system administrator regarding the security implications of enabling dynamic content.

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 v4.0 and click [Allow].

Creating Virtual Directories

ReadykeyPRO browser-based applications are installed under the default IIS directory. This step is optional; some system users may require that they be located in an alternate directory and must follow this procedure. Refer to IIS documentation for instructions on how to create new virtual directories. The following information is provided for configuration of new virtual directories.

Two virtual directories should be created: Lnl.OG.WebService and Lnl.OG.Web.

- Lnl.OG.WebService maps to the Local Path [Root-IIS-Path]\Lnl.OG.WebService\ and Lnl.OG.Web maps to the Local Path [Root-IIS-Path]\Lnl.OG.Web\.
- Each virtual directory should have the **Read**, **Log visits**, and **Index this resource** permissions selected.
- **Application name** should be Lnl.OG.Web for the Lnl.OG.Web VD and should be blank for the Lnl.OG.Webservice VD.
- **Execute permissions** should have Scripts only selected.
- **Application pool** should be DefaultAppPool.
- Select the Directory Security tab. In Windows XP, under Anonymous access and authentication control, click [Edit]. **Integrated Windows authentication** should be selected. In Windows 2003, under Authentication and access control, click [Edit]. **Integrated Windows authentication** should be selected.

Configure SSL

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

- Updating the Preferences.js File for SSL on page 69
- Configuring the Services.config File on page 77
- Configuring the FlexApplicationConfiguration.xml File on page 78
- Configuring the SilverlightApplicationConfiguration.xml File on page 78
- Configuring the ClickOnce Files on page 79

Internet Information Services (IIS) for Windows Server 2008

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 ReadykeyPRO. As such, Bosch is not responsible for IIS configuration and maintenance other than the steps outlined for ReadykeyPRO functionality. Technical Support assistance will be provided specific to the installation, enablement, and base functionality of IIS per ReadykeyPRO 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 65.

Use of SSL to ensure security across the network when using browser-based applications is highly recommended. Refer to IIS documentation for additional IIS and SSL configuration if desired. Once SSL has been configured, several files must be updated with the new URL. For more information, refer to Configure SSL on page 66.

.NET Configuration with SQL Server

Systems running versions of ReadykeyPRO newer than 5.12.012 should update their .NET version. By default for Windows Server 2008 the ASP.NET version is already set to 4.0. To check if it is 4.0:

1. Right-click My Computer and select **Manage**.
2. In the Server Manager tree, expand ***Roles > Web Server (IIS) > Internet Information Services (IIS) Manager***.
3. On The Internet Information Services (IIS) Manager window, expand ***Server Name > Sites > Default Web Site*** and click lnl.og.web.
4. Make sure that the **ASP.NET** version is set to 4.0 which it should be by default. To check:
   a. Double-click **.NET Compilation**.
   b. Expand ***Assemblies***. The system version should be 4.0.

Serving Dynamic Content with Windows Server 2008

By default Windows Server 2008 serves static and dynamic content. There is no configuration needed.

Creating Virtual Directories

ReadykeyPRO browser-based applications are installed under the default IIS directory. This step is optional; some system users may require that they be located in an alternate directory and must follow this procedure. 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 Physical Path [Root-IIS-Path]\Lnl.OG.WebService\ and Lnl.OG.Web maps to the Physical Path [Root-IIS-Path]\Lnl.OG.Web\.
- Once the virtual directories is created, right-click the virtual directory in the tree and select **Convert to Application** and click **[OK]**.
- **Application pool** should be LSAppPool32bit.
- On The Internet Information Services (IIS) Manager window, double-click **Authentication** and make sure that the status of **Anonymous Authentication** and **Integrated Windows authentication** is set to "Enabled."

Configure SSL

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

- Updating the Preferences.js File for SSL on page 69
- Configuring the Services.config File on page 77
- Configuring the FlexApplicationConfiguration.xml File on page 78
- Configuring the SilverlightApplicationConfiguration.xml File on page 78
- Configuring the ClickOnce Files on page 79

Authentication

An authentication method with the database must be configured for browser-based applications to work properly. Create an account in both Windows and the database system for use with single sign-on authentication. For more

information, refer to Database Authentication for Web Applications on page 41.

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 ReadykeyPRO directory so that they can write to the log files. This is also part of the Setup Assistant. For more information, refer to Setup Assistant on page 48.

1. Open the Windows services from ***Control Panel > Administrative Tools > Services***.
2. Locate the LS Application Server service in the list. Right-click the service and select **Properties**.
3. On the Log On tab, select **This account** and click [Browse].
4. Type the user name of the Windows account in the **Enter the object name to select** text box and click [Check Names].
5. Click [OK] to exit the Select User dialog and [OK] to save the changes to the LS Application Server properties.

Area Access Manager and VideoViewer Browser-based Clients

Updating the Preferences.js File for SSL

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

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

```
var g_lnl_pfx_webservice_serverAddress
 and change http to https.
```

Browser-based Reports

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

- Additional steps are required for Crystal Reports to access the database. Either NT authentication must be configured or the user credentials must be stored in the **Web.config** file and protected with security. For more information, refer to Configure Authentication for Reports in Area Access Manager on page 43.
- 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.
- The IIS user must be able to access the temp folder (typically **C:\Windows\temp**).

Configure Authentication for Reports in Area Access Manager

Authentication must be configured for reports in order to use them with Area Access Manager (Browser-based Client). Configuration steps vary depending on whether you are using Windows Authentication or providing credentials in a protected file. For more information, refer to Database Authentication for Web Applications on page 41.

Enable the Reports Option

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

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

   ```
   var g_lnl_og_aam_showReportsTask = true;
   ```

3. Save and exit the file.

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) or when active badges are being used in Visitor Management Front Desk.

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 or if active badges are being used in Visitor Management Front Desk.

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

Important: To make changes in the **ACS.INI** file on a Windows 7 computer you must right-click on the **ACS.INI** file and run it as the Administrator.

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.

ReadykeyPRO User Permissions

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

Viewing Reports in Area Access Manager

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

Client Configuration

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

Internet Browser Security Level

The security level must be specified for the ReadykeyPRO 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 then click [Sites].
   a. Type the URL for the ReadykeyPRO server on which the Web site is hosted.
   b. Click [Add].
   c. Click [Close].
4. Click [Custom level].

a. Locate the following settings in the list and verify that they are set correctly:

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

   a. Set the **Reset to** drop-down menu to **Medium-low**.
   b. Click [Reset].
   c. Click [OK].
   d. A warning dialog opens. Click [Yes].

5. On the **Advanced** tab, select **Multimedia > Play animations in web pages**.
6. Click [OK] to close the Internet Options 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.

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 opens.
   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 user name and password**.

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

b. Click [OK].

c. A warning dialog opens. Click [Yes].

6. Click [OK].

Accessing the Browser-based Applications

To access browser-based applications from a client, it is necessary to know the server name and the location of the application on the Web Application Server. For the Area Access Manager and VideoViewer browser-based clients, the IP address is also acceptable in place of the server name. There is not a central log in location for all ReadykeyPRO 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.

Important: If accessing with an IP address, IDVM may not work properly.

Application	URL
Area Access Manager	http://<*server name*>/lnl.og.web/lnl_og_aam.aspx
VideoViewer	http://<*server name*>/lnl.og.web/lnl_og_videoviewer.aspx
Visitor Management Host	http://<*server name*>/IdvmHost Or, if manual sign-on is being used: http://<*server-name*>/idvmhost/?useAutomaticSSO=false
Visitor Management Administration	http://<*server name*>/AdminApp

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

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

Accessing ClickOnce

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

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

Create Bookmarks

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

CHAPTER 9 *Visitor Management Installation*

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

Using SSL

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

Security and Authentication

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

Configuring the Services.config File

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

1. Navigate to **C:\Inetpub\wwwroot\lnl.og.services\ldvmWebHost**.
2. There are four possible security policies, with corresponding files:

Security policy	File
No transport security, Windows Authentication not required	HttpServices.config

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

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

3. Save the file.

Configuring the FlexApplicationConfiguration.xml File

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

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

Configuring the SilverlightApplicationConfiguration.xml File

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

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

Configuring the ClickOnce Files

Additional changes need to be made to the Front Desk and Kiosk ClickOnce files (serviceModelClient.config.deploy) to use SSL. For more information, refer to ClickOnce Setup on page 79.

ClickOnce for Front Desk and Kiosk

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

Prerequisites

Before using ClickOnce, make sure the computer has Microsoft .NET Framework 4.0.

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

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

ClickOnce Setup

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

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

Methods of Deployment

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

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

Server Name

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

Using SSL

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

1. Locate the following file:

   Navigate to **C:\inetpub\wwwroot\FrontDeskClickOnce\config** and edit the **serviceModelClient.config.deploy** file for Front Desk.

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

2. Locate the section that states

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

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

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

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

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

4. Locate the section that states

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

   The code for https is commented out by default.

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

6. For the address in that same section, change `http` to `https`.

Installation

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

Installing the Application via Network

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

Installing the Application via Server

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

1. Use a browser to go to the address,

   http://*<server name>*/FrontDeskClickOnce for Front Desk or http://*<server name>*/KioskClickOnce for the Kiosk,

   where *<server name>* is the name of the ReadykeyPRO server. If SSL has been configured, the URL will start with https://...

2. Click [Install].

The progress bar will indicate when installation is complete.

Workaround for Security Policies

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

Support Two Security Policies

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

Creating Two Copies of the Service File

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

Creating a New Virtual Directory

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

Updating the ClickOnce Deployment

1. Navigate to **C:\Inetpub\wwwroot**. Copy the directory, **FrontDeskClickOnce** for Front Desk. Copy the directory, **KioskClickOnce** for Kiosk.

2. Name the copied directory **AnonFrontDeskClickOnce** for Front Desk or **AnonKioskClickOnce** for Kiosk.
3. Locate the following file:

   Navigate to **C:\inetpub\wwwroot\AnonFrontDeskClickOnce\config** and edit the **serviceModelClient.config.deploy** file for Front Desk.

   Navigate to **C:\inetpub\wwwroot\AnonKioskClickOnce\config** and edit the **serviceModelClient.config.deploy** file for Kiosk.
4. Locate the section that states

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

   - Comment markers `<!--` and `-->` are used to indicate a portion of the code that will be ignored.
5. Comment out the endpoint address section of code for http by surrounding it with comment markers.

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

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

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

   This code is commented out by default.
7. Remove the comment markers `<!--` and `-->` surrounding that section to enable the code.
8. In IIS, create a new virtual directory named **AnonFrontDeskClickOnce** for Front Desk or **AnonKioskClickOnce** for Kiosk.
9. For the path, browse to and select the new directory, **C:\Inetpub\wwwroot\AnonFrontDeskClickOnce** for Front Desk or **C:\Inetpub\wwwroot\AnonKioskClickOnce** forKiosk.

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

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

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

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

CHAPTER 10

Maintaining the ReadykeyPRO Installation

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

Modify ReadykeyPRO Unlimited

ReadykeyPRO can be modified by following these steps:

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

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

   - **This feature will be installed on local hard drive**
   - **This feature, and all subfeatures, will be installed on local hard drive**
   - **This feature will not be available.**

5. After making your choices, click [Next] and then click [Install].

Repair ReadykeyPRO Unlimited

ReadykeyPRO can be repaired by following these steps:

1. Insert the ReadykeyPRO installation disc into the workstation.
2. The installation wizard should launch automatically. If it doesn't, browse the contents of the disc and double-click **setup.exe**.
3. The Welcome dialog opens. Click [Next].
4. Select Repair, and then click [Next].
5. The installation wizard provides a workstation-specific list of files you should back up before continuing the repair. Back up these files.
6. Click [OK].
7. Click [Install].
8. When the installation wizard completes, click [Finish].
9. Restore the backed-up files from step 5.

Remove ReadykeyPRO Unlimited

ReadykeyPRO can be removed by following these steps:

1. In the Control Panel:
   a. Double-click "Add or Remove Programs". In Windows 7, Windows Server 2008, or Windows Server 2008 R2 this is called "Programs and Features".
   b. In the **Currently installed programs** list, select "ReadykeyPRO Unlimited".
   c. Click [Remove].
2. You are asked if you are sure you want to remove ReadykeyPRO. If you are, click [Yes].

Upgrade from Older Versions of ReadykeyPRO

Check the release notes for the versions of ReadykeyPRO that are supported for upgrade. If you need to upgrade a version that is older than what's supported, contact your ReadykeyPRO Certified Dealer for specific information about upgrading to the newest edition.

ReadykeyPRO Fixes and Maintenance

Hot Fixes

Important: A hot fix must be applied to all servers and workstations running ReadykeyPRO. Failure to apply the hot fix to all ReadykeyPRO computers will result in the inability for the user to log in to the ReadykeyPRO system. To ensure that this happens, versions of ReadykeyPRO Unlimited 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 ReadykeyPRO builds and contain software fixes and feature enhancements.

Hot fixes can be obtained by contacting technical support. Hot fixes can also be found on the Supplemental Materials disc.

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

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

Important: Hot fixes cannot be uninstalled. You should create a backup of your system before installing a hot fix. For more information, refer to Chapter 4: Database Backup and Restoration on page 27.

Third-Party Service Packs and Updates

Third-party service packs and updates should only be installed after they have been fully tested with the ReadykeyPRO system. Approved updates can be found on the Supplemental Materials disc.

The components requiring updates are:

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

- Windows XP
- Windows Server
- Windows 7

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

Database:

- SQL Server Express
- SQL Server

Miscellaneous:

- MDAC
- DirectX
- Windows Internet Explorer
- Adobe Reader

Log Files

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

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

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

The most frequently used log files are:

- LenelError.log
- DataExchange.log

- Replicator.Log
- LnlLogError.log

Server Maintenance

Daily

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

Monthly

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

Appendices

APPENDIX A The application.config File

The **application.config** file is an ReadykeyPRO 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\Lnl** in Windows XP and Windows Server 2003 or **C:\ProgramData\Lnl** in Windows 7, Windows Server 2008, and Windows Server 2008 R2. 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 ReadykeyPRO 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 Bosch 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 7, Windows Server 2008, and Windows Server 2008 R2: Navigate to **C:\ProgramData\lnl**
- Click the Start button, then select **All Programs** > **ReadykeyPRO Unlimited** > **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 ReadykeyPRO, 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.
  - "Data Source=" for SQL Server, the Data Source points to the name of the machine that hosts the database. If the database resides on the same machine where database setup will be run from you can use the name of your machine (that is, COMPUTER1-DT).
  - "InitialCatalog=" is the name of the database. If you installed ReadykeyPRO, you specified this name during the installation. By default, this is AccessControl. If your database is not called AccessControl you must change this line to have your database's name.

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

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

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

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

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

application.config File Settings

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

ConnectionString

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

By default, the line looks like this:

```
<add key="ConnectionString" value="Data
Source=COMPUTER1-DT; Integrated Security=SSPI; Ini-
tial 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

Integrated Security=True

If 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 Connection-String 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 ReadykeyPRO, 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 ReadykeyPRO software. By default, the line resembles the following:

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

Lnl.LicenseSystem.Client.Host

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

By default, the line looks like this:

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

Lnl.LicenseSystem.Client.Port

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

By default, the line looks like this:

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

SRConnectionString

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

By default, the line looks like this:

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

Data Source

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

SchemaOwner

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

By default, the line looks like this:

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

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

Error Log

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

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

APPENDIX B

Custom Installation of ReadykeyPRO

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

Performing a Custom Installation

First Time and Existing ReadykeyPRO Installation

1. Begin installing the ReadykeyPRO software.
2. During the installation you are prompted to choose the system type. Select **Custom.**
3. You will be prompted with the custom setup screen. Choose which features to install.
4. Continue with the installation by following the installation steps.

Custom Features

The following features are only available with a custom Readykey-PRO installation.

Application Server

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

Additional steps are required for the configuration of the Application Server. For more information, refer to Chapter 8: Configuring the Web Application Server on page 63.

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.

Note: By choosing to install the Device Discovery Console, you automatically accept the WinPcap license agreement.

APPENDIX C *Deprecated Fields*

The following is a list of column changes that can potentially impact your custom reports and custom DataExchange scripts. Old columns store local time while the new columns store time in Coordinated Universal Time (UTC).

The Column (Old) represents the old deprecated fields that should not be used, whereas the Column (New) represents the new fields that replaced the old deprecated fields.

Table	Column (Old)	Column (New)
ACCTRANS	ACCDATE	TIMESTAMP
ACCTRANS_REPL	ACCDATE	TIMESTAMP
ACCTRANS_RESTORED	ACCDATE	TIMESTAMP
ASSET_LASTLOCATION	EVENTIME	EVENT_TIME_UTC
EVENTS	EVENTIME	EVENT_TIME_UTC
EVENTS_REPL	EVENTIME	EVENT_TIME_UTC
EVENTS_RESTORED	EVENTIME	EVENT_TIME_UTC
EVENTS_GUARANTEE	EVENTIME	EVENT_TIME_UTC
LASTLOCATION	EVENTIME	EVENT_TIME_UTC
LASTLOCATION_REPL	EVENTIME	EVENT_TIME_UTC

LASTLOCATION_REPL_STAGE	EVENTIME	EVENT_TIME_UTC
QUEUED_EVENTS	EVENTIME	EVENT_TIME_UTC
SAVEDEVENTS	SAVTIME	EVENT_TIME_UTC
EVENTS_VIDEO	STARTTIME	START_TIME_UTC
EVENTS_VIDEO	ENDTIME	END_TIME_UTC
EVENTS_VIDEO_REPL	STARTTIME	START_TIME_UTC
EVENTS_VIDEO_REPL	ENDTIME	END_TIME_UTC
EVENTS_VIDEO_RESTORED	STARTTIME	START_TIME_UTC
EVENTS_VIDEO_RESTORED	ENDTIME	END_TIME_UTC
CONTINUOUS_VIDEO	STARTTIME	START_TIME_UTC
CONTINUOUS_VIDEO	ENDTIME	END_TIME_UTC
CONTINUOUS_VIDEO_REPL	STARTTIME	START_TIME_UTC
CONTINUOUS_VIDEO_REPL	ENDTIME	END_TIME_UTC
CONTINUOUS_VIDEO_RESTORED	STARTTIME	START_TIME_UTC
CONTINUOUS_VIDEO_RESTORED	ENDTIME	END_TIME_UTC
ALARMSACK	ACKTIME	ACK_TIME_UTC
ALARMSACK	FORWARDED_TIME	FORWARDED_TIME_UTC
ALARMSACK_RESTORED	ACKTIME	ACK_TIME_UTC
ALARMSACK	IN_PROGRESS_ACKTIME	IN_PROGRESS_ACKTIME_UTC
ALARMSACK_RESTORED	IN_PROGRESS_ACKTIME	IN_PROGRESS_ACKTIME_UTC
ALARM_ACK_HISTORY	ACKTIME	ACKTIME_UTC

ALARM_ACK_HISTORY_RESTORED	ACKTIME	ACKTIME_UTC
ALARMSACK_RESTORED	FORWARDED_TIME	FORWARDED_TIME_UTC
** *VISIT* (**VISIT_EVENT** in New Table)	SCHEDULED_TIMEIN	SCHEDULED_TIMEIN
** *VISIT* (**VISIT_EVENT** in New Table)	SCHEDULED_TIMEOUT	SCHEDULED_TIMEOUT
VISIT	TIMEIN	TIMEIN_UTC
VISIT	TIMEOUT	TIMEOUT_UTC
VISIT	LASTCHANGED	LASTCHANGED_UTC
** VISIT_RESTORED (**VISIT_EVENT_RESTORED** in New Table)	SCHEDULED_TIMEIN	SCHEDULED_TIMEIN
** VISIT_RESTORED (**VISIT_EVENT_RESTORED** in New Table)	SCHEDULED_TIMEOUT	SCHEDULED_TIMEOUT
VISIT_RESTORED	TIMEIN	TIMEIN_UTC
VISIT_RESTORED	TIMEOUT	TIMEOUT_UTC
VISIT_RESTORED	LASTCHANGED	LASTCHANGED_UTC
VISIT_EVENT	LAST_CHANGED	LASTCHANGED_UTC
VISIT_EVENT_RESTORED	LAST_CHANGED	LASTCHANGED_UTC

Note: ** VISIT.VISIT_EVENTID *----> VISIT_EVENT.VISIT_EVENTID

APPENDIX D

Universal Time Conversion Utility

Important: Before running the Universal Time Conversion Utility you should create a backup of your database. For more information, refer to Chapter 4: Database Backup and Restoration on page 27.

Important: Due to limitations regarding data collected during Daylight Saving Time, the Universal Time Conversion Utility cannot be guaranteed to be 100% accurate for those dates that fall within Daylight Saving Time. Any inaccuracies, however, should not cause any problems for your system.

The purpose of the Universal Time Conversion (UTC) Utility is to collect non-UTC dates and times that are contained in reports and convert them to use the new standard UTC time.

Converting reports to use UTC Time allows users in multiple time zones to see the same data but in their local time.

The conversion process should be the last step in the upgrade process. If you do not run the utility then data collected in prior versions of ReadykeyPRO will not display the correct time until the conversion is completed.

The setup process for the UTC Utility occurs after your system and database has been completely upgraded and after any replication has been completed.

If you restore any archive prior to when the UTC Utility was first run, you will have to run the utility again.

Universal Time Conversion Utility Enterprise Considerations

Before running the Universal Time Conversion Utility on an Enterprise system you must:

- Complete all replication.
- Make sure that all of your regional node information has been uploaded to the master node.

Once replication is complete you must run the UTC utility on the master node and then perform a system download to the regional nodes.

On the regional nodes you can configure the linkage server and default system time zone after the system download is complete. If user replication is enabled, all user time zone data must be collected at the master node and downloaded to the regional nodes. If user replication is not enabled, you can configure the user time zones on the regional nodes as well.

Run the Universal Time Conversion Utility

1. Click the Start button, then select **All Programs > ReadykeyPRO Unlimited > Universal Time Conversion Utility**. The Universal Time Conversion Utility starts.
2. Enter your System Administrator login credentials used to access ReadykeyPRO.
3. On the Welcome screen, read the warning regarding database backups and select a radio button for your response. If you have created a backup, click [Next]. To begin the conversion process.
4. On the System screen, use the drop-down to select the World Time Zone that will be used as the default time zone in the system. Click [Next].

5. If you have a Linkage Server host configured, then, on the Linkage Server screen, select the World Time Zone that will be used by the items associated with the Linkage Server and click [Next]. You will only see the Linkage Server screen if your system has the Linkage Server host configured. Click [Next].
6. If you have segmented system then, on the Segments screen, choose the World Time Zone that will be used for the segments.
7. On the Workstations screen, select the World Time Zone that will be used for each of the system's workstations. The options are:
   - **Use the system world time zone for all workstations -** sets the World Time Zone on all workstations to match the one set as the default System World Time Zone.
   - **Use the associated segment world time zone for all workstations -** sets the World Time Zone on all workstations to match the one set on the segment.

   Click [Next].
8. On the Controllers screen, select the World Time Zone that you intend to associate with each of the system's controllers. You may be asked to restart the communication server before the changes take effect. Click [Next].
9. If you have a segmented system then proceed to step 10. If you do not have a segmented system then proceed to step 12.
10. On the Multi-segmented Users screen, select the World Time Zone to associate with multi-segmented system users. Optionally you can use the **Find User** field to search for a specific system user to change. You can also use the check box to assign the system world time zone to all users. Click [Next].
11. On the Single Segment Users screen, select the World Time Zone that you intend to associate with each of the single-segmented system users. These include the administrator, badge operator, system account, and user. You can also use the check boxes to assign the system or segment world time zone to all users.

    Optionally you can use the **Find User** field to search for a specific system user to change. You can also use the segment drop-down to associate users with the time zone associated with a specific segment. Click [Next].

12. (For non-segmented systems only) On the Users screen, select the World Time Zone that you intend to associate each of the system's users with. These include the administrator, badge operator, system account, and user. You can also use the check box to assign the system World Time Zone to all users.

    Optionally you can use the **Find User** field to search for a specific system user to change. Click [Next].

13. On the Save screen, the collected data is saved to the database. Select whether you would like to run the conversion process now or at a later time. If you choose to run the conversion process immediately, click [Next]. Otherwise, click [Close].

    Optionally, you can generate a report of the collected World Time Zone data by clicking [Generate Report]. This report is exported as a Comma Separated Value (CSV) file which is best opened in Microsoft Excel.

14. On the Conversion screen, click [Close] once the conversion process has completed.

Index

T

U

V

W

Bosch Security Systems, Inc.
130 Perinton Parkway
Fairport, NY 14450
1-800-289-0096
www.boschsecurity.us