

MainBoss Advanced 3.4, Update 2 Installation and Administration

Copyright © 2013, Thinkage Ltd.

Permission granted to reproduce all or part of this document
provided that Thinkage's copyright notice is included in the reproduction.
No money may be charged for such reproductions except
to recover all or part of the cost of reproduction.

Table of Contents

MainBoss Advanced Installation and Administration Guide	1
Software and Hardware Requirements.....	1
Microsoft SQL Server	2
Microsoft Report Viewer.....	3
Privileges.....	4
Installation Locations for MainBoss Software.....	4
ClickOnce Deployment	5
Manual Installation.....	5
Manual Installation Overview	5
Manually Installing MainBoss Software	7
Creating a Maintenance Organization.....	7
Entering License Keys.....	9
Users.....	13
Registering New Users with MainBoss.....	15
Security Roles	17
Testing Security Roles.....	19
Roles for Administering MainBoss	20
Installing MainBoss on Other Computers.....	20
MainBoss Service.....	22
Installing MainBoss Service.....	22
Configuring MainBoss Service	25
Allowing MainBoss Service to Access the MainBoss Database.....	29
Starting and Stopping MainBoss Service	30
Uninstalling MainBoss Service	31
The MainBoss Service Event Log.....	31
Transferring a Database to a New Computer	33
MainBoss Service and MainBoss Upgrades.....	34
Using Multiple Maintenance Organizations	34
Start Modes.....	35
Command Line Options.....	36
Backups	38
Backups within MainBoss	39
Restoring a Backup Within MainBoss	41
The MBUtility Command	44
Getting Help for MBUtility	45
Listing MainBoss Organizations	45
Built-In Data Schemas.....	45
Exporting Data from Your Database	46

An Example of Exporting to Excel 2007	47
Importing Data into Your Database.....	48
Adding Organizations.....	50
Backing Up Your Database with MBUtility.....	51
Adding an Administrator to a Database	51
Appendix A: Setting Up SQL Server	53
Instances	53
SQL Server Installation	54
Backups with SQL Server	54
Using SQL Server to Restore a Database from Backup	55
SQL Express Considerations.....	56
Installing SQL Express	56
Backups with SQL Express	58
SQL Server Maintenance	58
Appendix B: Troubleshooting.....	60
General Advice.....	60
File-Sharing.....	61
Testing for the Server's Machine Presence.....	62
Testing That a User Can Connect with the Server Machine	62
Comparing the DNS Name and Active Directory Name	65
SQL Server Configuration	66
Adjusting the Firewall.....	68
Granting Access to a Program through the Firewall.....	69
Firewall Off and On.....	70
Local Security Settings.....	71
Authorizing Users in SQL Server	72
Testing Whether a User Has Access to SQL Server and the MainBoss Database...	74
Testing Database Access with Microsoft Excel.....	75
Testing Database Access with SQL Server Management Studio Express	75
Testing POP3/IMAP4 Permissions for MainBoss Service	76
Testing Access to the MainBoss Service Event Log.....	78
Testing that You Can Start and Stop MainBoss Service.....	78
General Troubleshooting.....	79
Appendix C: MainBossRemote.....	80
MainBossRemote System Requirements	80
Minimum Server Configuration	80
License Keys	82
Initial Set-Up.....	82
Security Considerations.....	82
Application Pools	84
Giving Folder Permissions to Network Service or the Application Pool	

Identity	86
Giving SQL Server Permissions to Network Service or the Application Pool Identity	86
Web Sites vs. Applications	87
Adding and Configuring an Application	87
Adding and Configuring a Web Site	88
Authentication Settings	89
Application Settings	90
Software Initialization	91
Accessing SQL Server on a Different Computer	91
Integrating MainBoss Remote with MainBoss Service	92
MainBossRemote Troubleshooting.....	93
Cookie Usage	93

Introduction

MainBoss Advanced Installation and Administration Guide

This guide provides information about installing, configuring and managing MainBoss Advanced. The first chapter gives a quick guide that should be sufficient for many users. Later chapters give more details for those with advanced needs.

This guide is aimed at providing a reasonable path to getting MainBoss up and running. The procedures and settings we describe are not the only possibilities; some sites may have good reason to take different approaches (e.g. in setting up permissions over your local area network). However, if you don't follow our suggestions and you contact MainBoss Technical Support for help, we will probably recommend that you change your configuration to match what is described in this guide.

Important Note: You will obtain MainBoss software from a page on our web site (mainboss.com). The web page will provide primary instructions for installing the software. This manual provides additional information that may be useful during the installation process, beginning with *Installation Locations for MainBoss Software on page 4*. **If there is any disagreement between the download web page and this manual, follow the instructions on the download web page.**

Software and Hardware Requirements

Operating System: MainBoss Advanced will run on any of the following operating systems:

- Windows XP Pro or better (with Service Pack 3 or later):
 - XP Pro should provide satisfactory performance with one or two simultaneous users, provided that both users aren't on external machines
- Windows Server 2003 (with Service Pack 2 or later), including Windows Server 2003 R2; or
- Windows Vista Business or better (with Service Pack 3 or later); or
- Windows Server 2008 (with Service Pack 2 or later); or
- Windows Server 2008 R2 or later; or
- Windows 7 Pro or better.

We do not recommend the 64-bit versions of Windows XP or Windows Server 2003. For other systems, both 32-bit or 64-bit versions are acceptable.

We do not recommend Windows XP Home, Windows Vista Home, Windows Vista Basic, or Windows 7 Home.

If you will be running the **Web Access** and/or the **Web Requests** module, you must have Windows Server 2008, Windows Server 2008 R2, or better.

.NET Framework and Report Viewer: Every computer where MainBoss will run must have the .NET framework installed (version 4.0 or later). If you attempt to install MainBoss on a computer which doesn't have an appropriate of .NET, the MainBoss installation procedure will automatically attempt to download and install the latest .NET software from Microsoft's web site.

Every computer that runs MainBoss will also need Microsoft Visual Studio 2010 Report Viewer. This software will be included in the MainBoss distribution.

Hardware: We recommend that any computer running MainBoss Advanced should have:

- Windows XP and Windows Server 2003: at least a 3 GHz P4 processor with 1 GB of RAM
- Windows Vista, Windows Server 2008, and Windows 7: at least dual 2.5 GHz processors with 2 GB of RAM

In both cases, get the fastest RAM available. Ideally, the monitor screen should have a resolution of 1280 by 1024 or better; however, it is possible to get by with 1024 by 768 if you use the "hide details panel" button:



Since MainBoss requires SQL Server, you should also check the hardware requirements of the SQL Server package you intend to use. SQL Server will run on a single computer; if you also intend to use this computer to run MainBoss, the computer's hardware and operating system should satisfy the requirements of both SQL Server and MainBoss. Every other computer where you intend to run MainBoss has to satisfy MainBoss's hardware and software requirements, but doesn't have to satisfy SQL Server's.

If you intend to run MainBoss on multiple computers, we strongly recommend that MainBoss users should belong to a domain. A domain lets MainBoss users sign on with the same login name and password on different computers. You can create a domain with Microsoft Server software, or with a Linux network running Samba.

Microsoft SQL Server

MainBoss Advanced uses Microsoft's SQL Server 2005, 2008, or 2008 R2 to read and write all data. SQL Server must be installed at your site before you can begin using MainBoss Advanced. Specifically, you must have:

- SQL Server 2005 SP3 (Version 9.00.4035.00 or greater), or
- SQL Server 2008 SP1 or SQL Server 2008 R2

MainBoss doesn't work with earlier versions of SQL Server.

If you've installed MainBoss, you can determine what version of SQL Server you have by going to **Help** → **About** in the MainBoss menus.

While this *Installation and Administration Guide* offers suggestions of how to work with SQL Server, SQL Server is a Microsoft product and Thinkage has no control over its behavior. If you have any difficulties with SQL Server, contact Microsoft, not MainBoss support.

SQL Server is actually a family of compatible software products, with different members of the family designed for different work loads. If you have a small organization, you can use SQL Express, a free version of SQL Server available from Microsoft. For more information, see *SQL Express Considerations on page 56*.

SQL Express will likely be adequate if you intend to run the SQL Server on Windows XP Windows XP Pro (which supports fewer than five simultaneous users). The same applies to Windows 7 and Vista. If you will have more than five simultaneous users, you should run SQL Server on Windows Server 2003 or Server 2008 and buy a version of SQL Server whose size is appropriate to your needs.

If you intend to have multiple people using MainBoss, or you intend to access MainBoss from multiple machines, you should install SQL Server Management Studio and the configuration tools at the same time that you install SQL Server. This is discussed in the Appendix.

Microsoft Report Viewer

MainBoss prepares reports using Microsoft's Report Viewer. Before you install MainBoss, you should install the correct version of this software.

Because Microsoft occasionally changes the web page location of the Report Viewer software, we recommend going to

<http://www.mainboss.com/info/microsoft.shtml>

which will direct you to the correct location.

Note: SQL Server and Report Viewer are independent of MainBoss, including language support. In particular, reporting facilities will be in the language of your report viewer, which may or may not be the same language used by MainBoss. Similarly, diagnostic messages generated by SQL Server may or may not be in the same language as MainBoss.

Since Report Viewer is Microsoft software, Thinkage takes no responsibility for any problems you might encounter with the Report Viewer software package.

Privileges

Windows Administrator Privileges: Normally, you do not need Windows Administrator privileges to run MainBoss. However, you do need such privileges in the following cases:

- When you manually install MainBoss on a computer
- When you install MainBoss Service (see *Installing MainBoss Service on page 22*) and when you start or stop the service
- When you set up MainBoss Remote (see *Appendix C: MainBossRemote on page 80*)
- In order to look at the event logs in **Administration | MainBoss Service** (if you don't have privileges, the Event Log list will have an error message rather than log messages)

SQL Server Administrator Privileges: SQL Server Administrator privileges are needed to perform backups and restores of the MainBoss database. SQL Server Administrator privileges are also needed to add new users to the list of recognized MainBoss users (**Administration | Users**). This is because the new user must be given appropriate permissions to use SQL Server to access the database. However, there is a way around this; for details, see *Registering New Users with MainBoss on page 15*.

MainBoss Administration Security Role: You need the MainBoss Administration security role in order to use anything in the **Administration** section of the MainBoss control panel. This security role only applies to the use of features within MainBoss itself, and has no effect on any other software.

The person who creates a MainBoss database is automatically granted the MainBoss Administration security role. That person must then authorize other users, or else authorize one user and then give that user the Administration security role so that he/she may authorize other users.

Important: If you have Windows Administrator privileges and you use “Run as administrator” to start MainBoss (on Windows 7 or Vista), MainBoss will behave as if you have the Administration security role. In this case, you don't really have to have that role, nor does your login name have to appear in MainBoss's list of authorized users. This allows IT personnel to upgrade software and perform other software maintenance tasks without being recognized MainBoss users.

Installation Locations for MainBoss Software

When setting up MainBoss, it's important to distinguish between where you store the data and where you store the software:

- MainBoss *data* will be stored on a computer where SQL Server is running. There is only one copy of the data; this is shared by all users at your site.

- MainBoss *software* should be installed on every computer where people wish to work with MainBoss. In other words, you may have many copies of the software.

The software for MainBoss Advanced doesn't have to be installed on the server system if people won't be using MainBoss from that system. However, a number of administrative operations are more straightforward if MainBoss *is* installed on the server system.

Problems may arise if you store the MainBoss executable program on one computer and try to run it on another computer. (This is a known problem with the Microsoft .NET framework.) As a result, you must either:

- Install the MainBoss software on every computer where you intend MainBoss to run; or
- Use ClickOnce deployment, as discussed in the next section

ClickOnce Deployment

This version of MainBoss supports *ClickOnce Deployment*. This is a Microsoft technique which eliminates the need to install MainBoss updates on user's computers. Essentially, you create a web page that non-privileged users can use to invoke MainBoss, even if MainBoss hasn't been installed on the user's system.

Note that non-privileged users can't run MainBoss using ClickOnce unless they have prerequisite Microsoft software installed on their systems (the correct versions of .NET and Report Viewer).

For more about installing the ClickOnce version of MainBoss, see the information provided on the download web page that you use to get the MainBoss ClickOnce software.

Manual Installation

The sections that follow deal with manual installation, as opposed to ClickOnce Deployment.

Manual Installation Overview

To install and configure MainBoss, some operations must be done by someone who has Windows Administration privileges (typically someone from the IT department). Other operations must be done by someone with SQL Server Administration privileges. Finally, some operations must be done within MainBoss by someone with the MainBoss Administration security role. (In some organizations, this will be the same person.)

As noted previously, someone with Windows Administration privileges can start MainBoss with "Run as administrator" (on Windows 7 or Vista), in which case MainBoss behaves as if you are an authorized user with the Administration security role.

Below we list the recommended order of operations for installation and initial set-up, as well as the privileges needed for each step (if any).

1. Install SQL Server first. This should be on a computer that is accessible to all other computers where you wish to use MainBoss Advanced. We will call this the *Server computer*. [Windows Administration privileges]
2. Install the MainBoss Advanced software on a single computer first. Ideally, this should be the computer where SQL Server is running; this eliminates any issues that may arise when accessing SQL Server over your local area network. [Windows Administration privileges]
3. Start MainBoss on the computer where you just installed it, and create a maintenance organization database as described in [Creating a Maintenance Organization on page 7](#). [SQL Server Administration privileges; anyone who creates a MainBoss database is automatically granted the MainBoss Administration security role on that database.]
4. If you intend to import data from MainBoss Basic (MainBoss 2.9), follow the instructions given in the guide [Migration from MainBoss Basic to MainBoss Advanced](#). [SQL Server Administration privileges]
5. Enter the license keys you were given when you licensed MainBoss Advanced. For more information, see [Entering License Keys on page 9](#). [MainBoss Administration security role]
6. If multiple people will be using MainBoss Advanced, you must add those people to MainBoss's table of authorized users, as described in [Users on page 13](#). [MainBoss Administration security role]
7. Once you have MainBoss Advanced working correctly on one computer, either set up ClickOnce deployment or install the MainBoss software on all other computers where you wish to use MainBoss. [Windows Administration privileges]
8. Once the software is installed on a given computer, each person who will be using MainBoss on that computer must start MainBoss and add the MainBoss database to their personal list of known maintenance organizations. For more information, see [Installing MainBoss on Other Computers on page 20](#). [Any user can add a MainBoss database to his/her list of known databases. However, a user's access to a database is controlled by the user's security roles.]
9. If you have licensed the **MainBoss Service** module, install MainBoss Service as described in [Installing MainBoss Service on page 22](#). [Windows Administration privileges]
10. If you have licensed the **Web Access** and/or **Web Request** modules, install MainBoss Remote as described in [Appendix C: MainBossRemote on page 80](#). [Windows Administration privileges]

The Windows operating system is full of pitfalls, especially if your IT department has set up a customized environment. For help on dealing with difficulties during the installation process, see *Appendix A: Setting Up SQL Server on page 53* and *Appendix B: Troubleshooting on page 60*, especially if you'll be using SQL Express.

Manually Installing MainBoss Software

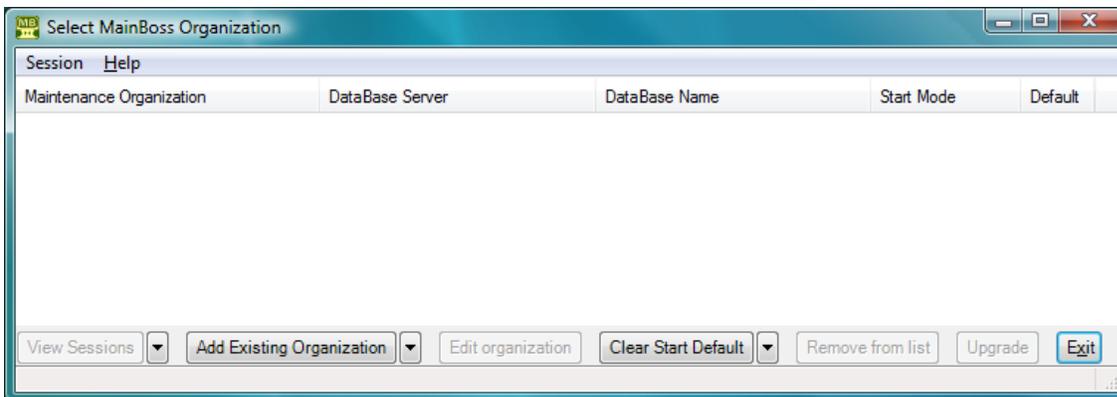
MainBoss Advanced is currently available through download from the MainBoss web site. Make sure you get the most up-to-date version of the software. To install the software, follow the instructions given on the download web page.

Once you've installed the MainBoss software on a user's system, the software can be started through the standard Windows program menu. Typically, however, you should create a desktop icon that starts the program.

Read Permission: Wherever you install the software, you should make sure that the folder has read permission for everyone who will be running MainBoss from that particular copy of the software. For example, if you are an administrator who installs MainBoss on a regular user's computer, make sure that the user has read permission on the installation folder. Similarly, if you intend for users to run MainBoss from a shared network folder, make sure that your MainBoss users all have read permission on that folder.

Creating a Maintenance Organization

When you first start MainBoss, the software displays a window that lets you create a new maintenance organization (database).



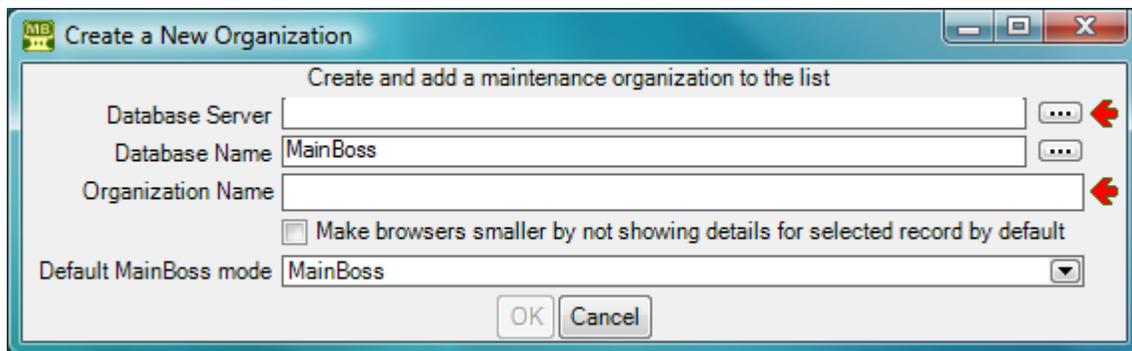
In order to create a MainBoss database, you must be logged into an account that has SQL Server Administrator privileges on the SQL Server that will manage the MainBoss database.

Important: MainBoss’s language support mostly adapts to the personal preferences of each individual user, as expressed in the user’s “Regional Settings”. However, a few key terms are generated and stored in the database at the time the database is created. If possible, these terms are translated into the preferred language of the person who creates the database; for example, if the database creator has set “Regional Settings” to English, the key terms will be stored in English. Once this happens, the terms are difficult to change. Therefore, it’s important for the person who creates the database to set his or her “Regional Settings” to whatever language will best suit the needs of the whole organization. (Note that you can override your existing “Regional Settings” using the /CultureInfo option on the MainBoss command line. For more, see *Command Line Options* on page 36.)

Changing Regional Settings may also change the currency symbol (e.g. from “\$” for dollars to “£” for pounds). However, MainBoss cannot handle multiple currencies; it assumes that all money values are in the same currency. For example, if you enter 33 in a “Unit Cost” field, MainBoss may display the result as \$33.00 or £33.00 depending on your Regional Settings...but internally, MainBoss simply record 33.00. Therefore, it is important that all MainBoss users use the same currency for all money values.

□ **To create a new maintenance organization database:**

1. Drop the arrow on [Add Existing Organization](#) and click [Create New Organization](#). This opens a window like this:



2. In “Database Server”, specify the name of the SQL Server that you will use.

If you click the “...” button after “Database Server”, MainBoss will attempt to determine what servers are available to you. However, this list may be incomplete—certain firewall settings and SQL Server configurations can prevent servers from appearing in the list, even though the servers may be available for use.

3. In “Database Name”, enter the name of the new database. This will be the name used by SQL Server; it must be different from all other databases controlled by the server. We recommend that this name should *not* contain any spaces or special characters—just letters and digits. (The default database name is MainBoss; this name is recommended, unless your organization has multiple MainBoss databases.)

If you click the “...” button after “**Database Name**”, MainBoss will attempt to display all databases already managed by the specified “**Database Server**”. You cannot choose any of these names (because the databases already exist), but the list may help you see what names are not already in use. (Depending on your permissions, you may not be allowed to see the list.)

4. In “**Organization Name**”, enter the name of your company or organization. Your “**Organization Name**” can contain spaces and special characters if you wish.
5. Click **OK**. MainBoss will proceed to create the database.

Entering License Keys

When you license MainBoss, you will be given a set of license keys for the software. Once you have installed MainBoss and created a new maintenance organization, MainBoss enters a special mode where you can enter these keys. You must have a separate set of license keys for each organization you use; for more information, contact your dealer or Thinkage Ltd.

License keys have the format

AAAAA-AAAAA-AAAAA-AAAAA-AAAAA

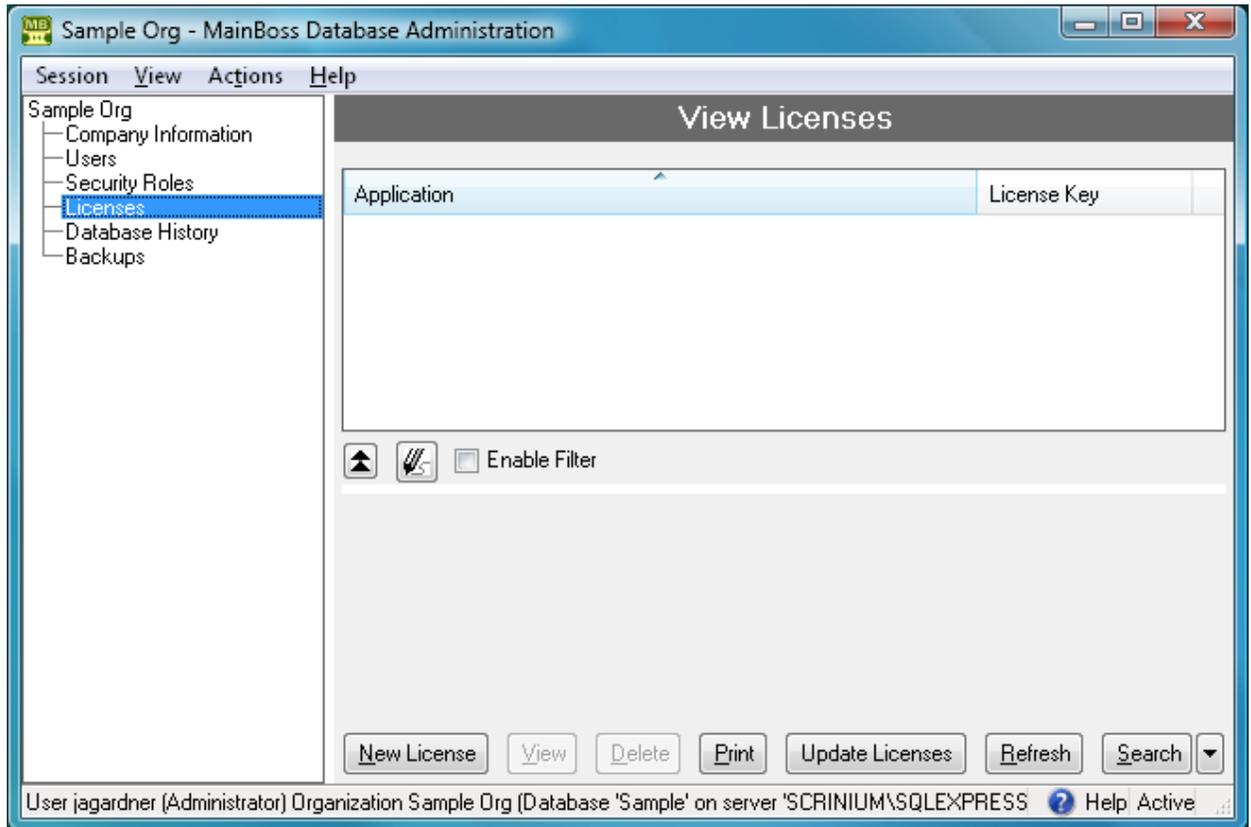
where each A is a letter or number.

The presence or absence of license keys will change the appearance of many MainBoss windows. For example, if you have not licensed the **Purchasing** module, you will not see functions related to purchase orders in the control panel and in other parts of MainBoss.

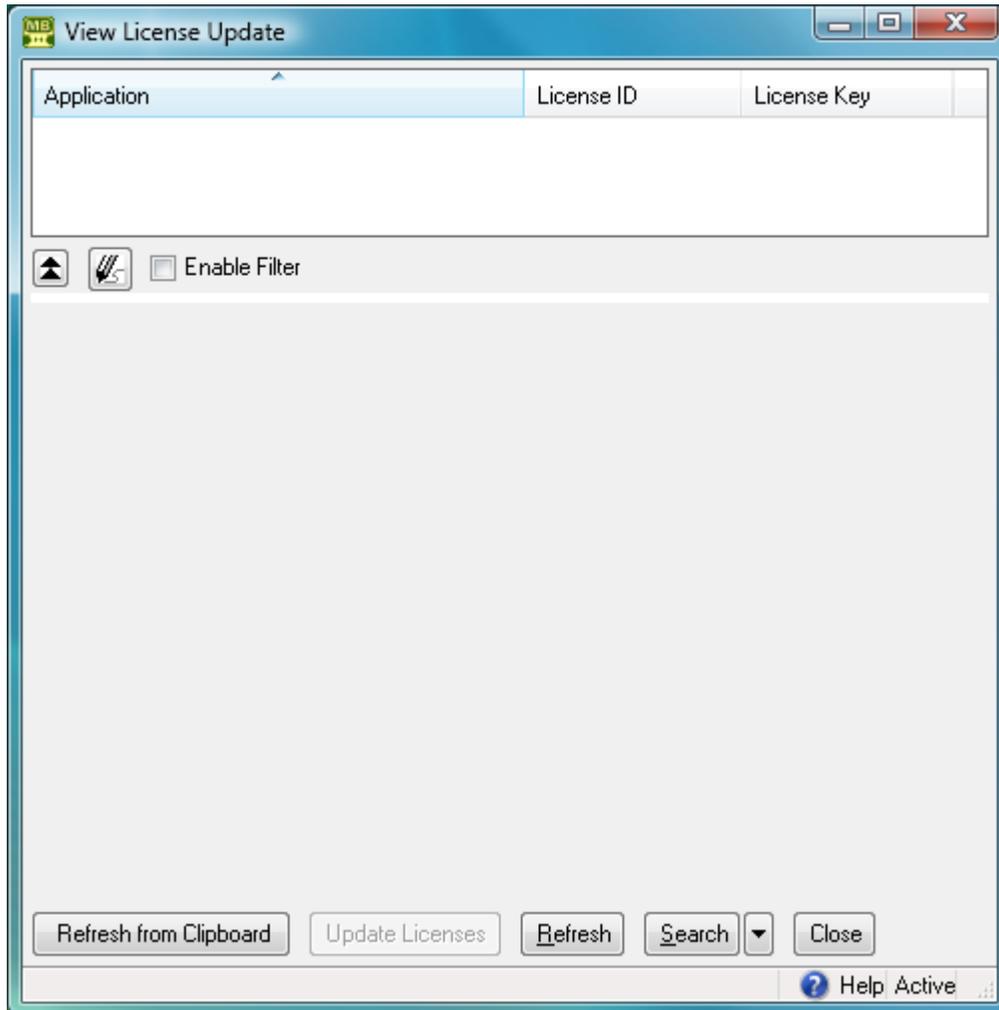
Thinkage gives you the option of receiving new license keys by e-mail. This makes it possible to enter all the keys you receive by copying them from the e-mail message and “pasting” them into MainBoss. To do so, follow these steps:

-
- **To enter your license keys by copying from an e-mail message:**
 1. Select the *entire* e-mail message that contains the new license keys. You do not have to select individual keys.
 2. Copy the message. In most e-mail programs, you can do this by pressing **<Ctrl+C>**.

3. In the MainBoss control panel, go to **Administration | Licenses:**



4. Click **Update Licenses**. MainBoss opens a window where you can enter the licenses:



5. Click **Refresh from Clipboard**. MainBoss scans through the e-mail message that you copied in Step 2, and extracts the license keys. MainBoss displays these keys in the upper part of the window.
6. Click **Update Licenses**. This uses the new license keys to replace the corresponding old ones, subject to the conditions stated below.
7. Click **Close** to close the window.

MainBoss will not replace an old key with a new key unless the new key is “better” than the old one. This means that the new key must have a later expiry date or version number than the old key.

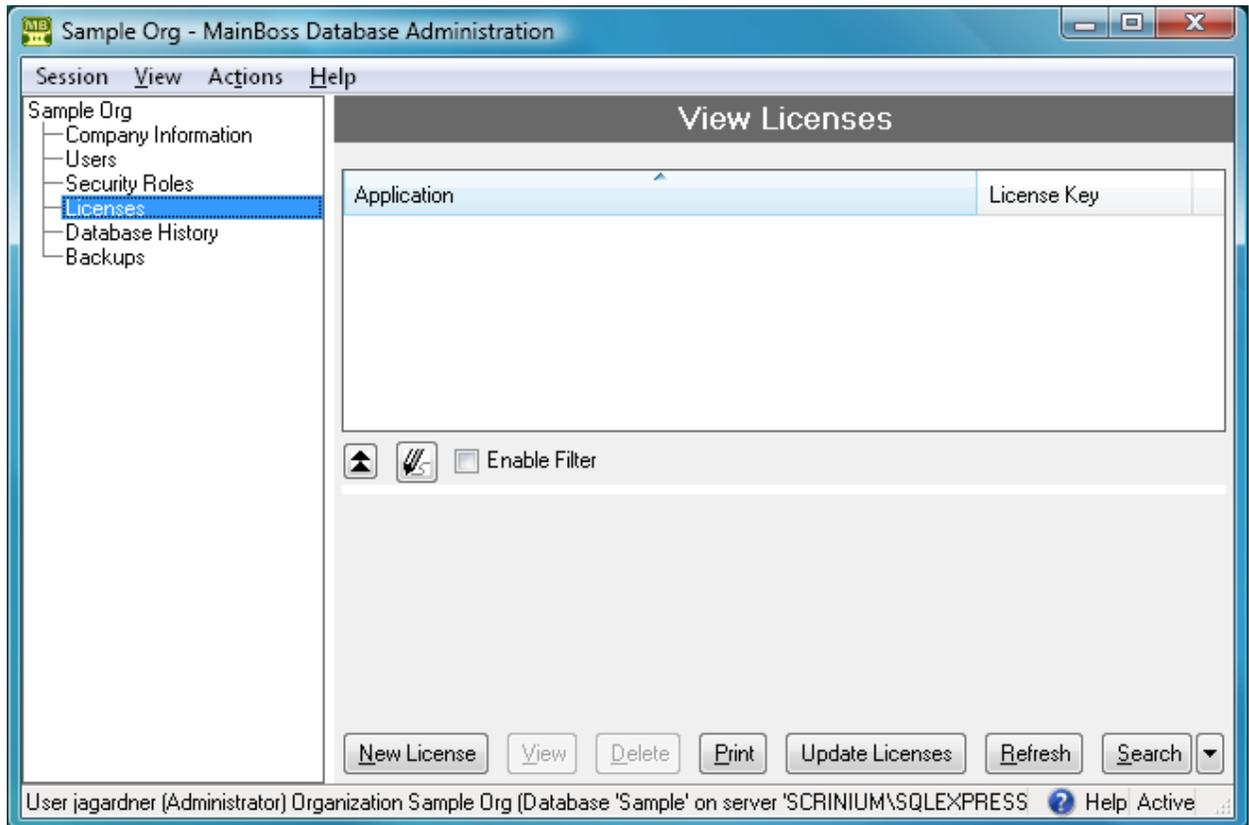
Also, all your license keys must have the same License ID as the **MainBoss** key. (If you do not have a **MainBoss** key, the other keys must have the same License ID as the **MainBoss Requests** key.)

Note: After changing keys, you must close and open the database in order for the change to take effect. This means that you must go to MainBoss's **Session** menu and select **Change Maintenance Organization**. In the resulting window, select the same organization and then click **Open Organization**. Until you do this, MainBoss will behave as if you're still using the old license keys.

If you do not receive your license keys in a format that allows copying to the clipboard, you must enter the keys by hand:

□ **To enter your license keys by hand:**

1. In the MainBoss control panel, go to **Administration | Licenses**:



2. Click [New](#). MainBoss opens a window where you can enter a license key:

3. In “**License Key**”, enter the **MainBoss** license key (or **MainBoss Requests** if you have not purchased a **MainBoss** license). Letters can be typed in either upper or lower case—it doesn’t matter which. You must type the hyphens “-” between groups of characters.
4. When you have typed the key correctly, MainBoss will fill in the rest of the window with information extracted from the key. If this doesn’t happen, check the key to make sure you have typed it correctly.
5. Click [Save & New](#) to save what you’ve just typed in. MainBoss will clear all the fields and let you type in a new key.
6. Repeat Steps 3-5 until you have typed in all the keys. Click [Close](#) or [Save & Close](#) to return to the previous window. The window will show all your new keys.

Users

In order for users to access a MainBoss maintenance organization, their login names must be recorded in the MainBoss database. When a maintenance organization is first created, the only user who can access the organization is the person who originally created the database.

Important: In order for someone to be able to use MainBoss from several different computers, that person must have the same login name and password on each of the computers. (This is automatically true if you use domains.)

Scopes: In the procedure described below, you record the login names of people authorized to use MainBoss. During this process, you’ll be given the opportunity to specify a *scope* for that person’s login name.

- If your site uses *trusted domains*, the scope should be the trusted domain to which the user belongs.

- If your site doesn't use trusted domains (or if you aren't sure whether you use them or not), **we strongly recommend leaving the “Scope Name” field blank.** A blank scope field means that the given login name is a valid account on the computer where SQL Server runs. SQL Server will then accept access from any other computer in your local network, provided that the login name and password on the other computer match the name and password on the Server computer.

For example, suppose you authorize `jsmith` to use MainBoss and leave “Scope Name” blank. Then the Server computer must accept `jsmith` as a login name. SQL Server will accept access from any other `jsmith` in your local network, provided the password for `jsmith` on non-Server computers is the same as the password for `jsmith` on the Server computer.

The names in MainBoss's **Users** list must be individual login names; they can't be groups. In MainBoss, login names are associated with records in order to create an audit trail. This is why MainBoss itself doesn't accept group authorizations—an audit should record exactly who made a particular change, which means tracking the individual login name, not just a group name.

Security Roles: When you create a new user record, it has no associated security roles. This means that new users have no permission to do anything in MainBoss, unless you specifically assign them roles. You must therefore assign each user at least one security role if you expect the person to use MainBoss in any way. For more on security roles, see [Security Roles on page 17](#).

Note: The person who creates a MainBoss database is automatically given a set of security roles which grant full access to all MainBoss operations.

SQL Server Authorization: In order for someone to use MainBoss, the person's login name must be registered in both the MainBoss database and with SQL Server. Only someone with SQL Server Administration privileges can register new users with SQL Server.

- The easiest scenario for adding new users to MainBoss is if someone with SQL Server Administration privileges does the work. In this case, MainBoss can automatically register each new user in the MainBoss database and with SQL Server.
- If the person who adds new users to MainBoss *doesn't* have SQL Server Administration privileges, then the process needs two separate steps:
 - Registering the new users with MainBoss, as described in [Registering New Users with MainBoss on page 15](#) (which can be done by anyone who's already registered with MainBoss and SQL Server)
 - Registering the new users with SQL Server, as described in [Authorizing Users in SQL Server on page 72](#) (which can only be done by someone with SQL Server Administration privileges)

In order to deal with these two scenarios, MainBoss has an option set in **Administration | Users**. Go to the **Defaults for User** section.

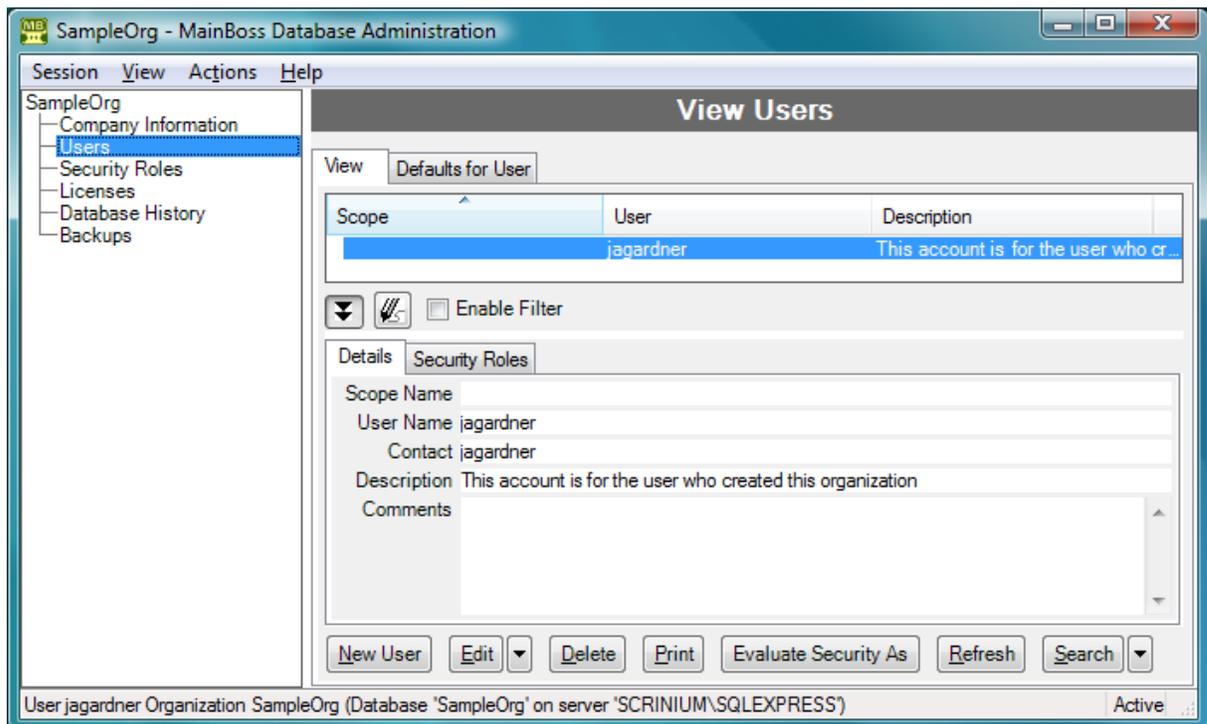
- If the option **MainBoss manages SQL Security** is checkmarked, anyone adding new users must have SQL Server Administration privileges
- If the option is blank, you must use the two-stage approach to adding new users (add the users in MainBoss first, then add them in SQL Server)

(As an alternative two-stage approach, you could create a Windows group named `mainboss` in the domain. A SQL Server Administrator could then set up SQL Server permissions so that anyone in the group could access the MainBoss database. Then, whenever someone new needs to be authorized to use MainBoss, a Windows administrator simply adds the new person to the group. Some IT departments may prefer the “group” approach over authorizing each individual within SQL Server.)

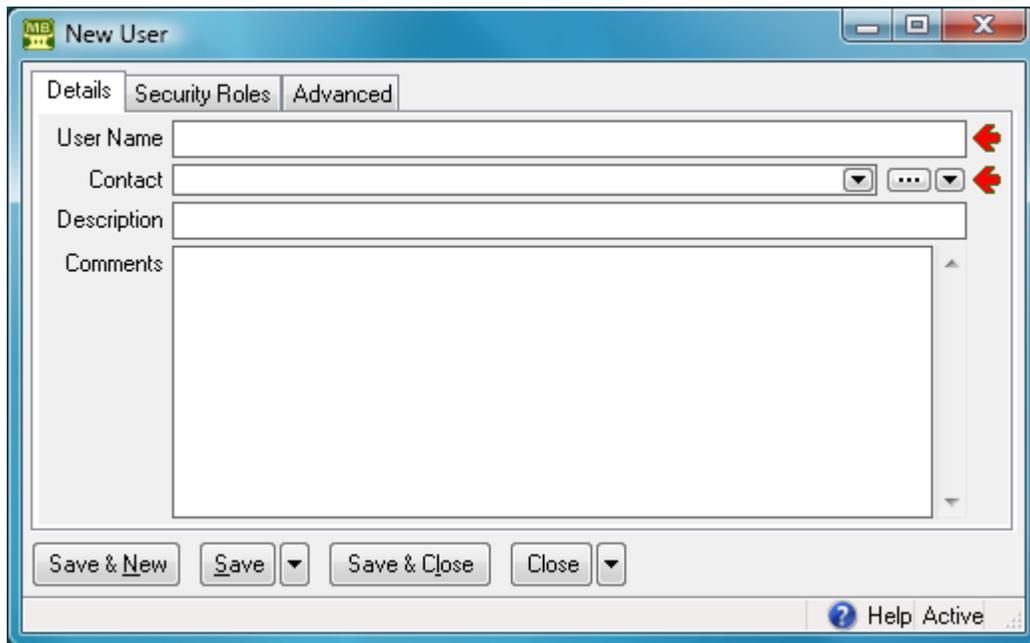
Registering New Users with MainBoss

To authorize someone to access a particular MainBoss database, follow these steps:

1. In the MainBoss control panel, go to **Administration | Users**:



2. Click **New**. This opens a window where you can specify other users who can use the database.



3. If your site uses trusted domains, go to the [Advanced](#) section and enter the user's domain name in "[Scope](#)". Otherwise, you can skip this step (and leave "[Scope](#)" blank).
4. In the [Details](#) section, type the person's login name into "[User Name](#)".
5. On the "[Contact](#)" line, click the second drop-down arrow. From the resulting menu, click [New Contact](#).
6. Fill in contact information for the user whose record you are creating. When you're done, click [Save & Close](#) to save the contact information and close the window.
7. Back in the user record, click [Save & New](#).
8. Repeat Steps 3-7 for each person who'll be using MainBoss. Click [Close](#) or [Save & Close](#) to return to the previous window. The window will show the users you have authorized.

Your MainBoss license restricts how many entries there may be in the [Users](#) table.

SQL Server Security: By default, the option [MainBoss manages SQL Security](#) is checkmarked in the [Defaults for User](#) section of [Administration | Users](#). If you add a new user when this option is in effect, MainBoss attempts to give the user appropriate SQL Server permissions on the MainBoss database. This will only work if you have SQL Server Administration privileges on the SQL Server that manages MainBoss.

If you *don't* have SQL Server Administration privileges, you must turn off [MainBoss manages SQL Security](#). Otherwise, you'll get an error when you try to add new users. If [MainBoss manages SQL Security](#) is turned off, new users must be separately authorized

within SQL Server using Microsoft's SQL Server Management Studio. For more information, see *Authorizing Users in SQL Server on page 72*.

In order to add new users within MainBoss, you must have the MainBoss Administration security role, or else you must have Windows Administrator privileges and start MainBoss with "Run as administrator".

Local Users vs. Domain Users: If your site uses domains, it's possible for the same login name to exist both inside and outside of a domain. For example, suppose you have a domain named `OurDomain` that contains a user named `jsmith`. It's possible for the SQL Server computer to have a local login name `jsmith` as well as the domain version (typically written `OurDomain\jsmith`).

If both versions of `jsmith` need to use MainBoss, they must both be in the MainBoss **Users** table. For the domain `jsmith`, set "**Scope**" to the domain name (`OurDomain`). For the non-domain `jsmith`, set "**Scope**" to the name of the computer. (This can be determined from the computer's **Control Panel** by going to **System**.) The non-domain `jsmith` will only be able to use SQL Server if the Server machine also has a local non-domain `jsmith` with the same password, and if the Server computer has been appropriately set up for network file-sharing. Also the non-domain `jsmith` must have a SQL Login recorded with SQL Server, which MainBoss may or may not create automatically (depending on various options). If you need to create a SQL Login by hand, see *Authorizing Users in SQL Server on page 72*.

If you delete a user from the **Users** table and later wish to restore the same user, just double-click the word `Active` in the bottom right corner of **Administration | Users**. This will show all the deleted users as well as the active ones. Click on the entry for the user you wish to restore, then click the drop-down button beside **View** and click **Restore**.

Security Roles

In order to use MainBoss, users need to be assigned one or more security roles. The available roles are listed in **Administration | Security Roles**. The comments provided in each role record indicate what permissions that role provides.

Security roles affect what a user sees: if a user doesn't have permission to see a particular type of information, that information will be blanked out or missing entirely from MainBoss windows. Security roles also affect what a user can do; for example, if a user has permission to view work orders (`WorkOrderView`) but not to close them, the **Close Work Order** button will be disabled for that user.

Important: When information is blank because you don't have appropriate permissions, move the cursor to the blank; MainBoss will tell you what security roles will give you permission to see that information. Similarly, if a button is disabled, move the cursor to the button; MainBoss will tell you what security roles will allow you to use that button. Note, however, that in some cases, information will disappear entirely (e.g. sections of records just won't be displayed); in this case, you may not know that something is missing.

To assign security roles to a user, you use the [Security Roles](#) section of a user record (**Administration** | **Users**). In order to decide what roles an individual user should be granted, you must consider what that user is expected to do in his/her job. For example, consider someone working on a help-desk and receiving problem reports from clients outside the maintenance department. What does that person need to do?

- He or she will need to create work requests describing problems; that requires `Request` permission.
- Help-desk personnel also need a small amount of information on work orders (so that they can tell a client, "Your work has been scheduled for Thursday"). This suggests the `WorkOrderSummary` security role.
- The `UnitSummary` role might also be useful. It gives help-desk personnel enough information about units to make sure they understand which unit the client is talking about.

Other roles may also be appropriate, depending on what help-desk personnel are expected to do, and on your organization's policies.

The *MainBoss Configuration Guide* offers suggestions on which security roles are appropriate for various duties within a maintenance organization.

Related Security Roles: Security roles tend to come in related groupings; for example, `WorkOrder`, `WorkOrderView`, `WorkOrderFulfillment` and `WorkOrderSummary` are all roles related to work orders.

In such a grouping, some roles automatically include others. For example:

- `WorkOrder` automatically includes all the other roles in the grouping.
- `WorkOrderView` automatically includes `WorkOrderSummary`.

For this reason, there's no point in giving someone both `WorkOrder` and `WorkOrderView` (for example), because `WorkOrder` automatically includes all the permissions of `WorkOrderView`.

In general, a `View` role automatically includes the related `Summary` role and a role with a simple name automatically includes roles of the same name with extra words (e.g. `PurchaseOrder` automatically includes `PurchaseOrderView`, `PurchaseOrderSummary`, and `PurchaseOrderReceive`).

Users with Windows Administration Privileges: If a user with Windows Administration privileges starts MainBoss using “**Run as administrator**”, MainBoss automatically gives that person the MainBoss Administration security role. This is intended to make it possible for a privileged Windows user to change security roles, in the event that there’s no one with the MainBoss Administration role. (This might happen, for example, if your current MainBoss Administrator leaves the company.)

As a side effect, you cannot “downgrade” the MainBoss security permissions of anyone with Windows Administration privileges. That person will always be able to get the MainBoss Administration security role by starting MainBoss with “**Run as Administrator**”, even if you do not explicitly give that person the role. (On Windows XP, “**Run as Administrator**” doesn’t exist and people with privileges get the Administration security role automatically.)

Testing Security Roles

It can be difficult to figure out the effects of various security roles, especially when a user has several different roles combined. To test what a particular user can and can’t do, you can use the [Evaluate Security As](#) button in **Administration | Users**. (You must have the Administration security role to use [Evaluate Security As](#).)

If you select a user in the **Users** table, then click [Evaluate Security As](#), your MainBoss session changes to have the same security permissions as the selected user. If certain types of data are invisible to that user, they’ll become invisible to you too; if certain buttons are disabled, they’ll be disabled for you too.

In this way, [Evaluate Security As](#) lets you see all the consequences of a user’s security roles. Once you’ve examined what the user can and can’t do, you can return to your own security roles by going to the **Session** menu and clicking **Reset to user YOURNAME security**.

Note: If you use [Evaluate Security As](#) to evaluate the security roles of someone who doesn’t have Administration or AdministrationView, the first thing that will happen is that you lose permission to see **Administration | Users**. This may look as if you’re being told that you don’t have permission to use [Evaluate Security As](#); however, it really means that the person you’re evaluating doesn’t have that permission.

[Evaluate Security As](#) gives you the same security roles as the selected user, but it does *not* change who you are. In particular, you keep your own set of assigned requests, work orders and purchase orders.

Roles for Administering MainBoss

If you are administering MainBoss, you should have the `Administration` security role. You are automatically granted this role (and others) if you're the one who creates the MainBoss database.

The `Administration` role gives you permission to assign security roles to any user, including yourself.

Installing MainBoss on Other Computers

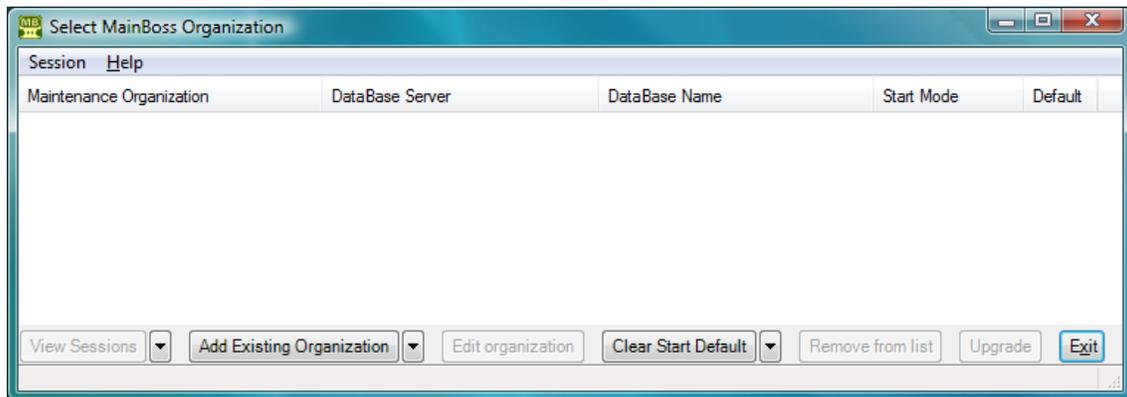
Once you have set up MainBoss on one computer, and are sure that it is working correctly with SQL Server, you can set up MainBoss on other computers (if you wish).

A MainBoss license dictates the number of people who may be authorized to use MainBoss. More specifically, it dictates the number of users who may be entered in the **Users** table (**Administration | Users**). Your license does *not* affect the number of computers where the software may be installed; therefore, you may install MainBoss on any number of computers within your organization.

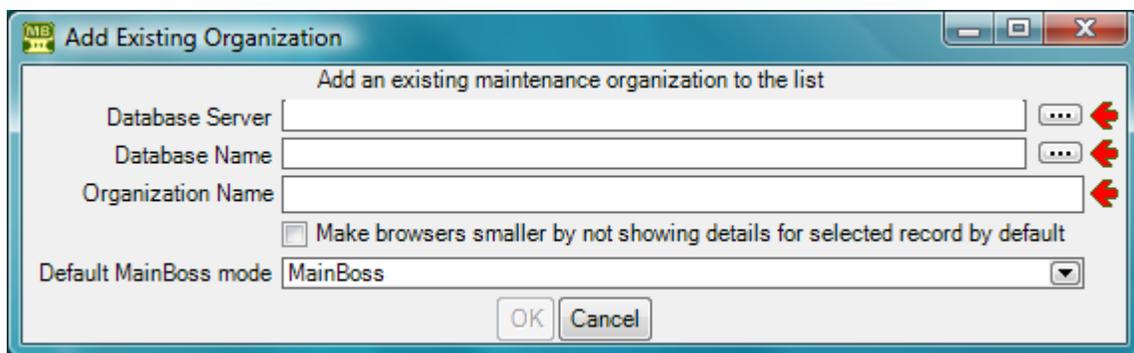
To install MainBoss manually on any computer, follow the steps given on the web page where you obtained the MainBoss software. Once you've done so, **each person who will use MainBoss on that computer** must set up his or her options for connecting with the MainBoss database. The alternative is to use ClickOnce deployment, as described in *ClickOnce Deployment on page 5*.

Important: MainBoss options are set up for each individual user. This means that each user must login and set up a connection to the MainBoss database. The process is easy, but the MainBoss Administrator must tell every user the “**Database Server**” and “**Database Name**” needed for the connection. Alternatively, you can have each user log in and then the administrator takes over to set up the database connection.

-
- **To set up MainBoss so that it can access an existing maintenance organization:**
 1. A MainBoss user should login to the computer under his/her usual login name.
 2. Start MainBoss on the new machine. It will display a window asking you to specify the maintenance organization:

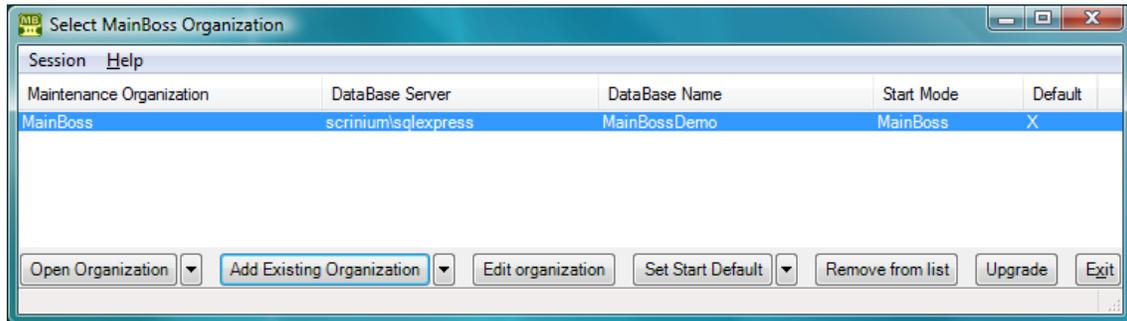


3. Click **Add Existing Organization**. This opens a window like this:



4. Set “**Database Server**” and “**Database Name**” to the same values specified when the database was created—see *Creating a Maintenance Organization on page 7*. The easiest way to set these fields is to click the “...” buttons associated with each field. These display lists of appropriate values. However, under some conditions (related to firewall settings), the “...” lists may not supply the values you want; in that case, you must type in the values by hand.
5. If you specify “**Database Name**” using the “...” button, MainBoss will fill in “**Organization Name**” with the company name specified in the database (from **Administration | Company Information**). If you wish, you can change “**Organization Name**” to your own private name for the organization; this will not affect any other users. (You might change the “**Organization Name**” if you have a number of organizations you must keep track of, and you want to make sure their names are distinctive.)

6. Click **OK**. MainBoss will add the database name to the list, as in



7. Click **Open Organization**.

Once you have set up this computer to access the maintenance organization, you don't have to do it again.

MainBoss Service

This section only applies if you have licensed the **MainBoss Service** module.

MainBoss Service handles communications between MainBoss and other applications. This includes sending and receiving all e-mail messages to and from requestors and assignees, as well as interacting with your web site if you have the **Web Access** and/or **Web Requests** module.

For the most up-to-date information on setting up MainBoss Service, as well as complete step-by-step instructions, see the mainboss.com web pages from which you downloaded your software. Material in this manual is only intended to provide background information that will help you make decisions about how you want to set up the service—when you are actually installing and configuring, work from the download web page.

Installing MainBoss Service

In order to use MainBoss Service, you must activate a Windows service. This service watches for incoming e-mail sent to the address associated with MainBoss Service. The service also sends out acknowledgement and notification messages when appropriate.

MainBoss Service can only be activated on a single computer; MainBoss won't let you install it on more than one computer. You need Windows Administrator privileges to install MainBoss Service.

MainBoss Service is designed to run continuously. Therefore, it should not be installed on a computer that is regularly turned off. (If the computer *is* turned off, information will not be

lost. However, incoming and outgoing messages won't be processed until the computer is turned back on.)

In order to configure MainBoss Service, you should install MainBoss itself on the computer where MainBoss Service will run. Once you have installed and configured MainBoss Service, you may choose to uninstall MainBoss on that machine. However, there are good reasons to keep MainBoss installed; for example, you will find it easier to access the MainBoss Service event log (diagnostic messages generated by MainBoss Service) if you can run MainBoss on the computer where MainBoss Service is actually running.

Accessing the MainBoss Service event log from a different computer is possible, but there are some preconditions. For more, see *The MainBoss Service Event Log* on page 31.

Important: We strongly recommend that you install MainBoss Service on the same computer where SQL Server is running (the instance of SQL Server that manages the MainBoss database). While it is possible to install MainBoss Service on a different computer, it will then be complicated to set up appropriate permissions to allow MainBoss Service to access the MainBoss database.

If you stop MainBoss Service, incoming messages will stop being processed. When you restart the service, it should begin processing the backlog of messages that built up while the service was off. The same principle applies if you shut down the computer where MainBoss Service is running.

To install MainBoss Service, you must run an executable program. Follow the instructions given on the web page where you obtained the software download. You will be asked to specify a login name for running the service. See below for suggestions on what name to use.

What Login Name Do You Specify for Running the Service: On Windows Server 2008, Windows Vista and Windows 7, we recommend that you run MainBoss Service using the built-in `Network Service` name. This is a standard name for running services like MainBoss Service, and will greatly simplify the process of setting up permissions. However, `Network Service` can only be used if MainBoss Service runs on the same computer as SQL Server.

Unfortunately, Windows XP and Windows Server 2003 don't have the concept of `Network Service`. Instead, you must specify a username and password; MainBoss Service will then run as if it was a program invoked by the specified user. The following considerations apply (but only for XP and Server 2003):

- Ideally, you should create a new login name for running MainBoss Service, and you should *only* use this name for running MainBoss Service. This makes it easier to track what MainBoss Service is doing and to separate MainBoss Service activities from everything else on the computer.
- Ideally, the login name associated with MainBoss Service should not have any special privileges; in particular, it should not be an administrator account. MainBoss Service

doesn't need privileges, and it's best not to give privileges to any program that doesn't need them. Since you must install MainBoss Service from an account with administrator privileges, this means that your login name will be *different* from the one you're logged into when you install MainBoss Service.

Note, however, that the login name for MainBoss Service must have **Log on as a service** permission (as discussed below).

- The login name should never have its password expire.
- When you enter the name during the installation of MainBoss Service:
 - If the login name is part of a domain, **you must specify the domain name as part of the username**, e.g. OURDOMAIN\jsmith.
 - If the login name is not part of a domain, you must specify the machine name, as in LOCALHOST\jsmith. (To get the name of the computer, right-click *Computer* or *My Computer* in the Windows Start menu, then click **Properties**. The resulting window includes the computer's name.)

MainBoss Service will use the "Regional Settings" of the user name under which it runs. This means, for example, that diagnostic messages will be issued in the language associated with that user name (if MainBoss supports that language).

Log On As A Service: The login name used for running MainBoss Service must have "service login" allowed by your system's security policies. On Windows 7 and Vista, *Network Service* automatically has this permission, and therefore you don't have to make any changes. On XP, you must give "service login" permission to the username you've specified to run MainBoss Service. You can do this by following these steps:

1. In the Windows Control Panel, click **Administrative Tools**.
2. If this computer controls domain security, you will see an entry for **Domain Security Policy**; click that. Otherwise, click **Local Security Policy**. Either way, Windows opens a window where you can set the policies.
3. In the left-hand section of the window, expand **Local Policies**, and click **User Rights Assignment**.
4. In the right-hand section of the window, double-click **Log on as a service**.
5. In the resulting window, click **Add User or Group**.
6. Enter the username you intend to use, then click **OK**.

Note: Domain security policies can be set up to prevent changes in local security policies. This means that you may not be permitted to change your local policies; if so, talk to the person who administers domain policies in order to resolve the situation.

Password changes: If you ever change the password associated with the service's login name, you must change the information associated with the service so that it uses the new password. To do so, the easiest approach is to use MainBoss to stop MainBoss Service, uninstall it, and then install it again with the same login name and the new password. You can also change the password in the properties associated with the service in the Computer Management window.

Configuring MainBoss Service

The first time you configure MainBoss Service, you create a configuration record by clicking [New MainBoss Service Configuration](#) in **Administration | MainBoss Service | Configuration**. Once you have created an initial configuration, you can edit the configuration by clicking [Edit](#) in the same window.

You can only configure MainBoss Service on the computer where the service runs. Therefore, the MainBoss software must be installed on that computer and you must use that computer for the configuration process.

In order to configure MainBoss Service, the service must be paused or stopped. This will be true the first time you configure MainBoss Service. If you want to change the configuration later on, you must click [Pause Service](#) or [Stop Service](#) in **Administration | MainBoss Service**. [Pause Service](#) requires the MainBoss Administration security role; [Stop Service](#) requires Windows Administration privileges.

Configuring MainBoss Service requires that you specify a mailbox where people can send problem reports. You must also specify how MainBoss Service can send and receive messages from that mailbox.

- Messages are sent using a technique called SMTP.
- Messages are received (read) using one of two techniques: POP3 or IMAP4. We recommend that you use POP3 unless your site has a reason for preferring IMAP4. (For MainBoss's purposes, POP3 is more efficient than IMAP4.)

There are several versions of both POP3 and IMAP4. We do not recommend plain POP3 or IMAP4; these techniques transmit passwords in unencrypted form, making them insecure. POP3S and IMAP4S are secure enhancements of POP3 and IMAP4 that use encryption. TLS (Transport Level Security) offers a different approach to POP3 and IMAP4, also using encryption to obtain secure communications.

Which version should you use? It depends on your e-mail software. Different e-mail packages accept different techniques. If you don't know what your software accepts, we recommend trial and error in this order: TLS within POP3; POP3S; TLS within IMAP4; IMAP4S; POP3; IMAP4. As noted previously, POP3 and IMAP4 are not recommended—only use them if your e-mail software is too old to accept any of the secure techniques.

For more information on SMTP, POP3 and IMAP, see the documentation for your e-mail software.

The window for configuring MainBoss Service contains the following:

Details section: Specifies basic information about MainBoss Service for this organization.

Code: Identifies the service configuration record. By default, this is
MainBossService.

Description: A more detailed description of the configuration record.

Machine Name: A read-only field telling the name of the computer on which the service is running (or will run).

ServiceName: The actual Windows name of the service.

Comments: Any comments you wish to record.

Incoming Mail section: Controls how MainBoss Service processes requests sent in by e-mail.

Allow processing of incoming request mail: If this box is checkmarked, MainBoss Service will operate normally. If the box is blanked out, MainBoss Service will not process incoming requests. In general, this box should be checkmarked.

Incoming mail server type: Choose one of the options listed.

Incoming mail server: The name of the computer that receives your incoming mail. For example, if you're running Microsoft Exchange, this is usually the name of your Exchange server. This machine must allow mail access through POP3 or IMAP4.

Incoming mail server port: The port used by the mail server. When you select an option under "**Incoming mail server type**", MainBoss automatically sets the port to the standard default:

- For POP3 and TLS within POP3: 110
- For POP3S: 995
- For IMAP4 and TLS within IMAP4: 143
- For IMAP4S: 993

Note: Getting the port numbers wrong is the most common source of errors when configuring MainBoss Service.

Username: The name of the e-mail account to which requests will be sent. For example, if users send mail to `workreqs@yourcompany.com`, the **Username** would be `workreqs`.

Password: The password (if any) for the specified **Username**.

Mailbox (IMAP4 only): The name of the mailbox, if you're using any version of IMAP4. The default is `inbox`.

Although the IMAP4 standard calls this the mailbox, most people would likely call this value a folder name. In general, the only time a value should be entered here is if incoming request e-mails somehow end up stored in a different folder from the default. (This can happen if you're using server-side rules to sort incoming mail into folders.)

Process E-mail Interval: Dictates how often MainBoss Service will check for new incoming messages. By default, this is 0:30 (every 30 minutes).

Automatically create new requestors: If this is checkmarked, MainBoss Service will automatically create new entries in the **Requestors** table (**Coding Definitions | Requests | Requestors**) whenever an e-mail message is received from someone who isn't currently on the list.

Remember that your **MainBoss Requests** license may place limits on the total number of requestors allowed in the **Requestors** table.

Outgoing Mail section: Controls how MainBoss Service sends out e-mail (acknowledgements to requestors and notifications to assignees).

Allow processing of outgoing notification mail: If this box is checkmarked, MainBoss Service will send out notifications as normal. If the box is blanked out, MainBoss Service will not send out notifications. In general, this box should be checkmarked.

Return E-mail address: The return e-mail address to be placed on acknowledgements and notifications (i.e. the address that will be used if the recipient wants to reply). This should be the e-mail address of a person in the maintenance department who can personally handle responses from clients.

Important: The "**Return E-mail address**" should *not* be the same as the mailbox to which users mail requests. If it is, you'll run into trouble if a requestor has an auto-reply set up, such as "Hi, I've gone on vacation and won't be answering my e-mail." What happens is this: if MainBoss Service sends an acknowledgement to the user, the auto-reply replies to the MainBoss Service mailbox; MainBoss Service thinks this is a new request, so sends an acknowledgement to the requestor; the requestor's auto-reply sends another reply to MainBoss Service; MainBoss Service sends another acknowledgement; and so on, until someone runs out of disk space. The way to avoid this is to set "**Return E-mail address**" to refer to a human being (who can be smart about dealing with auto-replies).

Return E-mail Display Name: The name to be associated with "**Return E-mail Address**".

Send E-mail notifications as HTML: If this is checkmarked, MainBoss Service sends notifications in HTML format. Otherwise, notifications are sent as plain text.

MainBoss Remote URL for E-mail notifications: If you have a **Web Access** license, MainBoss Service can add HTML links to notifications that will let users jump from the notification e-mail directly to a web page displaying an associated request or work order. In order to do this, you have to specify the URL of the web site that you use for MainBoss's **Web Access**. For example, you might set "**MainBoss Remote URL for E-mail notifications**" to

`http://ourcompany.com/MainBossRemote`

Notification Interval: Dictates how often MainBoss Service will check to see if notifications should be sent. By default, this is 0:10 (every 10 minutes).

Outgoing SMTP mail server: The name of the computer that will handle MainBoss Service's outgoing mail. Normally, this is the same as "**Incoming mail server**", but it doesn't have to be.

Outgoing SMTP port: The port used by the SMTP mail server. This is usually port 25.

Use SSL encryption for outgoing SMTP connection: If this box is checkmarked, MainBoss Service will use SSL encryption when sending out mail (to requestors).

Outgoing SMTP server authentication: The options in this area determine what kind of authentication (if any) MainBoss Service will use when sending out mail.

Anonymous: If this option is selected, MainBoss Service will not use authentication (mail is sent without going through any identification process).

Use the default network credential: If this option is selected, MainBoss Service uses whatever authentication is provided by the network as the default.

Using the specified SMTP domain, username and password: Choosing this option indicates that your SMTP server requires a domain, username, and password in order to send out mail. The fields below specify the required information:

Outgoing SMTP Domain: The domain that MainBoss Service should specify when sending out mail.

Outgoing SMTP Username: The username that MainBoss Service should specify when sending out mail.

Outgoing SMTP Password: The password for the given username.

Notification Preferences section: Controls how the format that MainBoss Service uses when sending out notifications.

Requestors subsection: Preferences for formatting e-mail acknowledgements sent to requestors.

Subject Prefix: A character string to be used at the beginning of the e-mail message's subject line.

Message Introduction: A character string to serve as the first line of the e-mail message itself.

Request Assignees subsection: Preferences for formatting e-mail notifications sent to people assigned to requests.

Subject Prefix: A character string to be used at the beginning of the e-mail message's subject line.

Message Introduction: A character string to serve as the first line of the e-mail message itself.

Work Order Assignees subsection: Preferences for formatting e-mail notifications sent to people assigned to work orders.

Subject Prefix: A character string to be used at the beginning of the e-mail message's subject line.

Message Introduction: A character string to serve as the first line of the e-mail message itself.

Purchase Order Assignees subsection: Preferences for formatting e-mail notifications sent to people assigned to purchase orders.

Subject Prefix: A character string to be used at the beginning of the e-mail message's subject line.

Message Introduction: A character string to serve as the first line of the e-mail message itself.

///Save & Close: Saves the current information and closes the editor window.

After you have created or edited your configuration information and saved the configuration record, you must click [Set Service Parameters](#) in **Administration | MainBoss Service | Configuration. [Set Service Parameters](#) is what actually changes the configuration, by copying information from the configuration record into the MainBoss Service software itself. If you do not click [Set Service Parameters](#), MainBoss Service will not be adjusted with the new configuration information. In order to use [Set Service Parameters](#), you must have Windows Administration privileges.**

Once you have [Set Service Parameters](#), you should go to **Administration | MainBoss Service** and use [Resume Service](#) or [Start Service](#) to start MainBoss Service running. [Resume Service](#) is used if you paused the service using [Pause Service](#); [Start Service](#) is used if you stopped the service with [Stop Service](#).

Allowing MainBoss Service to Access the MainBoss Database

MainBoss Service needs to access the MainBoss database. This means that MainBoss Service's login name must be granted SQL Server permissions on the database. To grant these

permissions, you must be logged in under a login name that has Windows Administrator privileges and SQL Server Administrator permissions on the instance of SQL Server that manages the MainBoss database.

If you are running MainBoss Service under a system account like `Network Service`, the account may already have appropriate SQL Server permissions. If so, you can skip this step. Otherwise, add a SQL Server login for the account under which you are running MainBoss Service, by following these steps:

1. Login to Windows under a login name that has SQL Server Administration privileges.
2. Start SQL Service Management Studio and connect with the instance of SQL Server that manages the MainBoss database.
3. In the left hand panel of Management Studio, expand **Security**.
4. Right-click on **Logins**, and click **New Login**.
5. In "**Login name**", enter the login name under which you will run MainBoss Service. (Specify the full login name in the format `DOMAIN\USERNAME`. If you aren't sure of the correct format, use the **Search** button to find the right name.)
6. In "**Default database**", select the name of the MainBoss database.
7. In the **Select a page** panel, click **Server Roles**.
8. In the list of server roles, make sure that **public** is checkmarked.
9. In the **Select a page** panel, click **User Mapping**.
10. In the list of databases under **Users mapped to this login**, click the name of the MainBoss database.
11. In the bottom panel of the window (**Database role membership for:**), checkmark **public** and **MainBoss**.
12. Click **OK**.

Starting and Stopping MainBoss Service

Administration | MainBoss Service contains buttons that will start or stop MainBoss Service. To start the service, click [Start Service](#).

- If you are logged in to the computer where MainBoss Service is installed, [Start Service](#) (and [Stop Service](#)) will work if you have Windows Administrator privileges. On Windows Vista and Windows 7, MainBoss will attempt to go into “elevated privileges” mode and you will be asked to confirm this.
- If you are logged in to a different computer, [Start Service](#) and [Stop Service](#) only work if the following are true:

- You have Windows Administrator privileges on the computer where MainBoss Service is installed.
- The computer where MainBoss Service is installed has file-sharing turned on. (For how to turn on file-sharing, see *File-Sharing on page 61.*)

Uninstalling MainBoss Service

You may wish to uninstall MainBoss Service (for example, to change the computer on which it's running). In order to do the uninstall, you must be logged in on the computer where the service is running, on an account with administration privileges.

To uninstall the service, follow the usual procedure for uninstalling software:

- Go to the Windows control panel.
- Click **Programs and Features** (Windows Vista or Windows 7) or else **Add or Remove Programs** (Windows XP).
- Select **MainBoss Service** in the list of installed software.
- Click **Uninstall** (Windows Vista or Windows 7) or else **Remove**

The MainBoss Service Event Log

The MainBoss Service event log lists any diagnostic messages that MainBoss Service has received. If MainBoss Service isn't behaving the way you expect, checking the event log may help you determine what's going on.

The easiest way to see the event log is to log in to the computer where MainBoss Service is running. Start MainBoss; **Administration | MainBoss Service** will list the log messages.

Depending on your Windows configuration, you may need Windows Administrator privileges to see the event log. If you need privileges to see the log but you don't have them, you'll see an error message saying that you don't have permissions to see the log.

Messages are only put into the event log when MainBoss Service has some kind of problem. Therefore if you are having difficulties with MainBoss Service, check the event log to see if the messages help determine what's going on. (As always, it may be useful to use Google or another search engine to search for explanations of the messages.)

Don't confuse the event log with **Administration | MainBoss Service | E-mail Requests**. The **E-mail Requests** table shows incoming e-mail messages that were turned into requests. These can be read from any computer.

Seeing the Event Log from a Different Computer: As noted above, the easiest way to see the event log is to be logged into the computer where MainBoss Service is running. However, you can see the event log from a different computer provided the following are true:

- ❑ You must have Windows Administrator privileges on the computer where MainBoss Service is running. (You do *not* need Windows Administrator privileges on the computer where you're logged in.)
- ❑ The computer where MainBoss Service is installed must have file sharing turned on. For instructions on how to turn on file-sharing for a computer, see [File-Sharing on page 61](#).
- ❑ The **Remote Registry** service must be running on the computer where MainBoss Service is installed. (On some systems, this service is turned on by default; in others, it's turned off.)

To turn on the **Remote Registry** service if it isn't already running, follow these steps:

1. Login to an account with Windows Administration privileges on the computer where MainBoss Service is installed.
2. Click on the Windows **Start** button.
3. Right-click **My Computer** (Windows XP and Server 2003) or **Computer** (Windows 7, Vista, and Server 2008).
4. In the resulting menu, click **Manage**.
5. In the left-hand panel of the resulting window, expand **Services and Applications**.
6. Click **Services**.
7. In the right-hand panel, find the entry for **Remote Registry**.
8. If the **Remote Registry** service has a status of "Started" and a startup type of "Automatic", it's already set up correctly. You can close the window.
9. Otherwise, right-click on the entry for **Remote Registry**. Click **Properties**.
10. In the resulting window, set **Startup type** to **Automatic**.
11. Click **OK**.
12. Right-click on **Remote Registry** again.
13. Click **Start**.

Note: Once you've done the above, you should check the firewall settings for **Remote Administration** to make sure that its use is restricted to your local network, not the whole Internet.

If all the conditions for displaying the event log are not met, **Administration | MainBoss Service** displays an error message.

If you are logged into the computer where MainBoss Service is installed, the event log is automatically updated whenever an event occurs. If you are logged into a different computer, the event log is only updated when you click the [Refresh](#) button.

You can clear the contents of the event log by going to **Administration | MainBoss Service** by clicking [Clear Events](#) (on the [Set Minimum Logging](#) drop-down button).

Transferring a Database to a New Computer

When you install MainBoss Service on a computer, MainBoss stores various configuration information in the database. Amongst other things, this information tells MainBoss that the service is installed.

Now suppose you want to move your MainBoss database to a different computer, or you move your SQL Server to a different computer. Ideally, you should do this by following these steps:

1. Have all users on all computers exit the MainBoss program.
2. On the original server computer, login to an account with Windows Administrator privileges.
3. If you are running MainBoss Service, uninstall it as described in *Uninstalling MainBoss Service on page 31*.
4. Start up MainBoss and backup the database using **Administration | Backups** (as described in *Backups within MainBoss on page 39*).
5. Exit MainBoss.
6. Copy the backup file to the new server computer.
7. Use [Create New Organization from Backup](#) to create a new MainBoss database from the backup file (as described in *Restoring a Backup Within MainBoss on page 41*).
8. Install MainBoss Service on the new server computer (as described in *Installing MainBoss Service on page 22*).

This is the recommended approach for transferring a database to a new server or when you transfer SQL Server to a different computer. In some cases, however, you may be doing the transfer because the old server computer is unusable (e.g. due to hardware failure). In this case, you don't have a chance to uninstall MainBoss Service first, and you'll be working from an old backup. The old backup database contains records stating that the service is still installed, even though the service hasn't been installed on the new computer. To correct this situation, follow these steps:

1. Make a copy of the most recent backup of your database from the old server computer.
2. Use [Create New Organization from Backup](#) to create a new MainBoss database from the backup file (as described in *Restoring a Backup Within MainBoss on page 41*).

3. Install MainBoss Service on the new computer and specify that it should work with the newly created database (as described in *Installing MainBoss Service on page 22*).

If the computer that was running the old MainBoss Service ever comes back into operation, you may need to delete the old service using `sc delete`. If you do not, the old service will start up every time Windows does. However, it will then check the MainBoss database and see that the database is no longer configured to use the old service. The old service will then issue an error message and terminate itself. Therefore, the old service won't interfere with MainBoss operations; however, it will add overhead to your system startup, so you should still get rid of it with `sc delete`.

MainBoss Service and MainBoss Upgrades

Before installing a new update of MainBoss, we strongly recommend that you use the old version of the software to stop MainBoss Service before you install the new software. Once it's stopped, you can install the new software (including the new version of MainBoss Service). Once MainBoss is working again, you can restart the service (as described in *Starting and Stopping MainBoss Service on page 30*).

Using Multiple Maintenance Organizations

Some maintenance departments may decide to license multiple maintenance organization databases. For example, a property management company that services multiple independent properties may choose to have a separate database for each property.

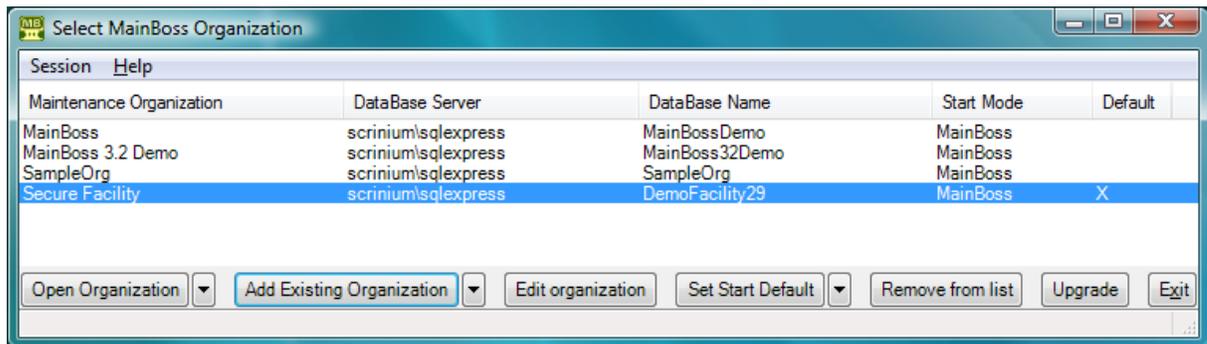
If you have multiple databases, each must have its own separate set of license keys. You may not use the same license keys for multiple databases.

1. You create each new database following the same procedures described in *Creating a Maintenance Organization on page 7*.
2. You then record the database's license keys as described in *Entering License Keys on page 9*.
3. You authorize appropriate users (as described in *Users on page 13*).
4. On every computer where someone will wish to access a particular database, you follow the steps in *Installing MainBoss on Other Computers on page 20* so that the databases are known on each appropriate computer.
5. If you are using MainBoss Service, each separate database must have its own e-mail address for receiving mailed-in requests. You must also install a separate MainBoss Service for each database where MainBoss Service will be used. For more information, see *Installing MainBoss Service on page 22*.

You will end up with a list of maintenance organizations you may access. One organization is designated as the default; whenever you start MainBoss on a particular computer, that computer will start with its default organization. To switch to another maintenance organization, go to MainBoss's **Session** menu and select **Change Maintenance Organization**. MainBoss will display a list of available organizations.

□ **To switch to another maintenance organization:**

1. Go to MainBoss's **Session** menu and select **Change Maintenance Organization**. MainBoss will display a list of available organizations:



2. Select the organization you want, then click **Open Organization**. MainBoss will open the organization and you can begin working with it.

If you wish to change the default, select the desired database in the above window and click **Set Start Default**. This designates the chosen database as the default. From this point on, MainBoss on this computer will start with the selected default. (Note that each user on each computer can have a different default.)

Start Modes

MainBoss can start in a number of different modes:

MainBoss: Full MainBoss mode with all available modules operational. Your license limits the maximum number of names that may be entered in the **Users** table.

MainBoss Requests: Requests-only mode. The control panel will only display entries relevant to dealing with requests. You can always open MainBoss in this mode, provided you have a **MainBoss Requests** license key and you have been granted permissions to access the database.

Administration: Only allows access to the **Administration** part of the control panel. You can always start MainBoss in this mode, even if you currently have no valid license keys. In fact, when you create a blank organization, you *must* start MainBoss in this

mode in order to enter your license keys. Once you've done so, you can quit and start MainBoss again in its normal mode.

Administration functions can only be used if you have the Administrator security role.

View Sessions: Only shows who else is using MainBoss.

You can specify a start mode in the **Select MainBoss Organization** window. You can set a default mode for any organization by using the **Set Start Mode** drop-down button or by choosing a mode from the **Open Organization** drop-down button.

As an example of the use of start-up modes, your help-desk personnel might set their starting mode so that they always access the database in requests-only mode unless they manually open it in some other mode.

If you sometimes want to open a database in full mode and sometimes in requests-only mode, you can give the same database multiple organization names. For example, suppose your database has the "**DataBaseName**" MyMainBoss. You could use **Add Existing Organization** to create two different lines in the organization list:

- One line might have the "**Organization Name**" MyMainBoss-Full, with a start mode of **MainBoss**.
- A second line might have the "**Organization Name**" MyMainBoss-Requests, with a start mode of **MainBoss Requests**.

If you click **Open Organization** on MyMainBoss-Full, MainBoss opens in full **MainBoss** mode. If you click **Open Organization** on MyMainBoss-Requests, MainBoss opens in requests-only mode.

You can also use command line options to specify start mode and maintenance organization you wish to access. This makes it easy to create shortcuts and desktop icons that each open a different organization or open the same organization in different modes. For more on command line options, see the next section.

Command Line Options

If you will frequently access different maintenance organization, you might want to create a set of desktop icons, each of which starts up MainBoss with a different organization. To create such icons, you need to use MainBoss command line options. These options are described in full detail in the online help, but this guide offers a quick overview.

You cannot specify command line options with ClickOnce deployment. If you think you'll need to use command line options on a particular computer, use manual installation on that computer.

When MainBoss starts, it usually opens your default database. To tell it to open a different database, use the command line:

```
mainboss /on:organizationname
```

For example,

```
mainboss /on:OurOrganization
```

opens the database that has the organization name `OurOrganization`.

Start Modes: The command line also lets you specify a particular *mode* in which you want MainBoss to operate. For example, you can start MainBoss in “requests only” mode—this lets the user view and enter requests, but nothing else. Help-desk personnel might run MainBoss in this mode so they can record problem reports but not use other MainBoss features.

To start in requests mode, use the command line

```
mainboss /mode:requests
```

You can also add options specifying an organization name, as shown previously.

Culture Information: The `/CultureInfo` option lets you specify Windows “culture” setting to be used when you execute MainBoss. A *culture* is a collection of information about language and other locale-based information, e.g. what monetary symbols are used in a particular place.

By default, MainBoss takes its culture information from your Windows Regional Settings; it then attempts to operate in the language given by those settings (e.g. MainBoss attempts to run in French if that’s what your settings dictate). However, if you specify a `/CultureInfo` argument on the command line, the argument overrides the Regional Settings. This is particularly useful if you’re creating a batch command file or shell script that you want to have work in a specific language, no matter what the user’s Regional Settings might be.

The argument of `/CultureInfo` is the official Windows “CultureInfo” string name for the desired culture. For example, if you want generic Spanish, you’d specify `/CultureInfo:es-ES`; for U.S. English, you’d use `/CultureInfo:en-US`. See your Windows documentation for recognized “CultureInfo” string identifiers.

Options on the MainBoss command line are not affected by `/CultureInfo`. For example, the option `/Mode:Requests` does *not* change if you switch to a language where “requests” is translated to a different word.

<p>Note: If you change the culture information with <code>/CultureInfo</code>, MainBoss makes the change <i>after</i> the command line arguments have been parsed. This means that if your command line has syntax errors, you may see error messages in the user’s original preferred language, not in the language specified by <code>/CultureInfo</code>.</p>

Compact Browsers: The `+CompactBrowsers` option invokes MainBoss in a mode that initially hides the details panel for records selected in table viewers. The `-CompactBrowsers` option tells MainBoss not to hide such panels.

Using Command Line Options: The easiest way to use command line options is to create a desktop icon that specifies the options. You can do this by following these steps:

1. Right-click an open area of the Windows desktop. In the resulting menu, click **New**, then **Shortcut**.
2. Windows asks you to specify the file to execute. Click the **Browse** button and use it to locate the MainBoss executable file (named `mainboss.exe` in the folder where you installed the MainBoss software—typically `\Program Files\Thinkage\MainBoss\3.3`).
3. Click **Next**.
4. Enter a descriptive name for the shortcut, then click **Finish**. This creates a new desktop icon with the name you specified.
5. Right-click on the new desktop icon. In the resulting menu, click **Properties**. Windows will open a Properties window for the icon.
6. The “**Target**” field contains the name of the MainBoss executable file in double quotes. After the closing double quote on the file name, add a space and whatever options you wish to specify.
7. Click **OK**.

The icon that you just created will start up MainBoss with the command line options you specified. You can have multiple MainBoss desktop icons, each with a different command line. (Each such icon has to be given a unique name.)

Backups

We strongly recommend that you backup your database on a regular basis. Most commercial backup software packages can tell SQL Server to create a backup of a database, after which the backup package makes the backup. In this way, backing up your MainBoss database is automatically incorporated into your normal backup procedures.

If you use commercial backup software, check that it can, in fact, deal with SQL Server databases. With some backup products, dealing with SQL Server is an extra that you have to pay for on top of standard backup operations.

If you do not have commercial software that deals with SQL Server, you have a number of options:

- You can do backups manually through SQL Server Management Studio. For more information, see *Backups with SQL Server* on page 54.

- You can use the MBUtility command as described in *Backing Up Your Database with MBUtility on page 51*.
- You can back up your database inside MainBoss by using **Administration | Backups**. For details, see the next section.

Ideally, however, you should use automated backup facilities as discussed above, either through commercial software or through SQL Server's built-in facilities. Because these facilities operate automatically, you won't have to remember to do backups manually.

We strongly recommend that you save copies of your backup files in off-site locations. For example, you might copy your backup files to a CD or DVD, then take the disk home with you; alternatively, you could copy your backup files to a computer at a company branch office or to a location in the Internet "cloud". If your only backups are in the same building as the computers that hold your original data, a fire or flood in that building could wipe out all your records.

Backups within MainBoss

You can perform backups within MainBoss using **Administration | Backups**. The general procedure is:

1. Create one or more *backup names*. A backup name is the name of a file into which MainBoss should write backup data. For example, you might create seven backup names: one for each day of the week.
2. When you want to perform a backup, select a name from the list of available backup names. Then click **Backup**. This submits a request to the SQL Server asking the server to create a backup. (In order to use this function, you must have SQL Server Administrator privileges.) When the backup occurs, it will overwrite any current contents of the specified backup file.
3. The next time you want to do a backup, select a different name from the list and click **Backup** again. MainBoss sorts the backup names so that the oldest backup file is at the top of the list. Therefore, if you have seven backup names, and you always select the top name whenever you make a backup, your backup will always overwrite the oldest file. This makes it easy to reuse the same set of files by cycling through them.
4. When you initiate a backup operation, MainBoss makes an appropriate note in the database history (**Administration | Database History**). If the backup fails for some reason, MainBoss makes note of the failure in the database history; however, if the backup succeeds, MainBoss doesn't make a history note. In other words, if there's no note about the backup failing, you can assume that it succeeded.

A number of important considerations apply to the backup name:

- Backup operations are run by SQL Server itself on the computer where SQL Server is running. Because SQL Server does the backup, backup names must refer to files that are accessible to the login name under which SQL Server runs. Furthermore, backup names are interpreted relative to the computer where SQL Server is running.

For example, suppose SQL Server is running on Computer X, but you're working on Computer Y. When you specify the backup name,

```
C:\MyBackups\Monday.bak
```

you may think that this refers to a file on Computer Y's C: drive. However, the backup is done by SQL Server on Computer X; therefore, SQL Server will try to save to Computer X's C: drive, not Computer Y's. If the directory C:\MyBackups doesn't exist on Computer X (or if SQL Server's login name doesn't have permissions to write to that folder), you'll get an error message and the backup won't work.

- If you specify a backup name that does not begin with "\\\" and does not begin with a drive letter (e.g. "C:\\"), SQL Server automatically assumes the name refers to a file under SQL Server's working folder. The location of this working folder depends on information specified when SQL Server was installed.
- SQL Server backup files typically have names ending in the extension ".bak", as in MyBackup.bak. Therefore, if you specify a simple name for a backup name—a name that doesn't have any slashes, backslashes or dots—MainBoss automatically adds ".bak" on the end of the name. Therefore, if you specify a simple name like "abc", MainBoss automatically turns this into "abc.bak".
- For safety's sake, backup names should refer to a disk drive that is *different* from the one that contains the actual MainBoss database. Otherwise, if the disk drive malfunctions, you could lose both your original database and your backups. It's even better if the backup name refers to a completely different computer, as in
\\NotTheSameComputer\MyBackups\Backup1.bak.

It's also a good idea to make copies of backup files and to keep those copies somewhere off your premises. That way, if you have a fire or some other problem that affects your entire site, you'll have backups someplace else safe.

(By default, SQL Server puts backup files on the same disk as the corresponding database. Therefore, you should make sure *not* to use the default location.)

When you specify a backup name, the "**Defaults**" line in **Administration | Backups** specifies the computer, the directory, and the file name extension. **We strongly recommend that you examine the "Defaults" line whenever you create a backup name and before you click Backup.** This will avoid failed backups or accidentally creating a backup file somewhere you don't expect.

The information in “**Defaults**” is generated by MainBoss at the time the window is displayed. It’s dependent on your SQL Server configuration. Therefore, suppose you specify a backup name of “abc”. “**Defaults**” shows where the backup file would be written if you clicked **Backup** right now. However, if your SQL Server configuration changes, future backups with the “abc” backup name might be written to a different folder.

The window for viewing backup names includes the following:

Name list: As noted above, the default is to put the oldest backup file at the top of the list.

Information area: The area below the list shows information about the selected backup name/file.

Last backup: The last date/time that backup information was stored in the selected file.

Name: The name you specified for the file.

Defaults: Information telling where the backup information will be written if you click **Backup** right now.

Comments: Any comments you’ve associated with this backup name.

New Backup Name: Opens a window where you can specify a new backup name.

Backup: Begins a backup on your database. See the notes at the start of this section for further information on the backup process.

Note: If you perform backups and restores entirely through SQL Server, MainBoss won’t store information about such operations. You won’t see corresponding entries in the **Backups** list or in the database history.

When MainBoss initiates a backup in this way, it makes an appropriate entry in the database history (**Administration | Database History**). If the backup fails, MainBoss makes a second entry in the database history reporting the failure. If the backup succeeds, MainBoss doesn’t record this—the default is to assume that the backup was successful.

Restoring a Backup Within MainBoss

SQL Server offers various methods for restoring a database from a backup file. For further information, see the SQL Server documentation.

However, you can also restore a database from within MainBoss itself, using facilities in the Maintenance Organization window. (This is the window that lets you choose a database to open. One way to open this window is to go to MainBoss’s **Session** menu and click **Change Maintenance Organization**.)

MainBoss offers two operations for restoring databases from backup:

- **Restore Organization** overwrites an existing database. First you select the database to be overwritten (by clicking on the entry for that database in your Maintenance Organization list), then you click on **Restore Organization** to specify the backup file you want to use.

Typically, you would use **Restore Organization** if you made some sort of large-scale error that you wanted to undo (e.g. mistakenly generating and committing a large number of planned maintenance work orders). **Restore Organization** is not intended for situations where your database is no longer usable because it's been deleted or corrupted.

Restore Organization is particularly useful when you're just getting started with MainBoss. For example, you can backup your database and then experiment with various ways of setting up your work (especially planned maintenance tasks). If you decide to take a different approach, you can restore from your backup and try again.

Restore Organization also ensures that the permissions on the database file are the ones that MainBoss needs and expects. This can be helpful if the permissions somehow get changed.

- **Create New Organization from a Backup** creates a new database using data from a backup file.

Typically, you would use **Create New Organization from a Backup** if your original database has been deleted or corrupted. You could also use this operation if you wanted to create a test database using data obtained from your production database.

To execute either **Restore Organization** or **Create New Organization from a Backup**, click the drop-down button associated with **Add Existing Organization** and choose the operation from the resulting menu.

In both cases, MainBoss performs the operation by submitting requests to SQL Server. You must therefore have SQL Server Administrator privileges to perform either operation.

Restore operations are run by SQL Server itself on the computer where SQL Server is running. Because SQL Server does the work, the backup file that will be used must be accessible to the login name under which SQL Server runs. Furthermore, the name of the backup file should be relative to the computer where SQL Server is running. Unless the file name explicitly begins with `\\computer` or a drive name (e.g. `C:\`), the file name will be assumed to be relative to SQL Server's home directory. (This is true even if the file name begins with a `\`.)

For example, suppose SQL Server is running on Computer X and you submit a restore request while working on Computer Y. MainBoss will ask you to specify the name of the backup file containing the database you want to restore. Suppose you give the name

`C:\MyBackups\Monday.bak`

You may think this refers to a file on Computer Y's `C:` drive. However, the restore operation is performed by SQL Server on Computer X; therefore, SQL Server will try to find the file on

Computer X's C: drive, not Computer Y. If the directory C:\MyBackups doesn't exist on Computer X (or if SQL Server's login name doesn't have permissions to read that folder), you'll get an error message and the restore operation won't work.

For this reason, we recommend that you only submit restore requests while logged in to the computer where SQL Server is running. You should also be aware of what permissions SQL Server has and what files will actually be accessible to SQL Server's login name.

Both [Restore Organization](#) and [Create New Organization from a Backup](#) ask you to specify the following:

Database Server: The network location of the SQL Server through which you will access the database. If you click the accompanying "..." button, MainBoss displays a list of database servers that are known to your Windows system. There may be additional servers that you can use but that Windows doesn't currently know about.

Database Name: The name of the database you want to overwrite or create. With [Restore Organization](#), this must be the name of a valid MainBoss database, and the "..." button will show all known MainBoss databases on the specified "**Database Server**". With [Create New Organization from a Backup](#), you can specify any name (existing or not), and the "..." button shows all databases, not just MainBoss ones.

Organization Name: A name that you personally will use for this database. This should not be the same as the organization name for any other database.

[Restore Organization](#) also asks you to specify:

Backup File Name: Fill in the field with one of the names in your list of backup names (as given in **Administration | Backups**). If you choose a name from this list, MainBoss tries to restore from the associated backup file.

MainBoss's list of backup files only contains files made inside MainBoss using Administration Backups . The list doesn't backups made directly with SQL Server Management Studio.
--

[Create New Organization from a Backup](#) asks you to specify:

Restore Data: Fill in the field with the name of a SQL Server backup file containing a backup of a MainBoss database.

This field has an associated "..." button. If you are logged in to the same computer where SQL Server is running, clicking "..." opens a standard "file open" dialog to let you find the backup file you want.

If you are logged in to any other computer, the "..." button does nothing and you must type in the backup file's name by hand. The name should start with \\computer or a drive name (e.g. c:\), or else it should be relative to the SQL Server's default folder on the computer where SQL Server is running. (See above for more details on specifying the file name.)

Once you have specified the required data, click **OK**. This submits an appropriate request to SQL Server, which performs the restoration.

The MBUtility Command

The MBUtility command offers a command-line interface to selected MainBoss operations. This allows administrators and IT personnel to create shell scripts (e.g. `.bat` or `.cmd` command files) which perform common administrative functions.

MBUtility is installed as an `.exe` file in the same folder as other MainBoss software. To execute MBUtility, you can `cd` to this folder or you can create a shortcut to the program. You can also add the MainBoss software folder to your `PATH` environment variable.

MBUtility is only available if you have installed the MainBoss package manually. The software will not be available on your computer if you use ClickOnce deployment.

In general, the format of the command is

```
mbutility verb option option option ...
```

The verb must always come immediately after `mbutility`, but the options may appear in any order. Options may have any of the following forms:

`/keyword:value`

Specifies a value. For example, `/Output:filename` specifies an output file.

`+Option`

Turns on an option. For example, `+Probe` may be used with the `AddOrganization` verb; it tells MBUtility to check that the corresponding database is actually accessible from the current computer.

`-Option`

Turns off an option. For example, `-Probe` may be used with the `AddOrganization` verb; it tells MBUtility not to check the database's accessibility, but just to add it to the list of known organizations.

Abbreviations on the MBUtility Command Line: Most keywords on the MBUtility command line may be abbreviated. In the sections that follow, letters that *must* be included are shown in upper case; any or all other letters may be omitted. For example, the following are all valid abbreviations for the option `/DataBaseName`

```
/databasename  
/databasen  
/dbname  
/dbn
```

Although the documentation shows some letters in upper case and some in lower, you can type letters in any case you want. For example, `/DBN` is exactly the same as `/dbn` or `/Dbn` on the MainBoss command line.

Getting Help for MBUtility

The command

```
mbutility Help
```

displays a summary of MBUtility's syntax and options. As noted in the previous section, Help may be abbreviated by omitting any or all lower case letters, as in

```
mbutility h
```

Listing MainBoss Organizations

The ListOrganizations verb of MBUtility lists MainBoss maintenance organizations known to the current user (i.e. the organizations that would be listed in the [Select Maintenance Organization](#) window). The command has the format

```
mbutility ListOrganizations option ...
```

where the possible options are:

+Probe

Determines whether you can actually connect with each organization listed. The default behavior is -Probe, which means that MBUtility doesn't test connections in this way.

+RealNames

Displays the real registry name for each database, as well as the databases' usual display names. The default behavior is -RealNames, which means MBUtility only shows the usual display names.

Built-In Data Schemas

A *data schema* consists of XML code describing the format of data in a database. Schemas are used when importing data into a database or exporting data from the database. MBUtility has a number of built-in schemas that can be used for this purpose. To get a list of these built-in schemas, execute the command

```
mbutility ListImportSchemas
```

The result is a list of keywords that may be used on an MBUtility command line, as described in later sections of this guide.

Generating Schema Definitions: You can obtain the actual XML code for a built-in schema using MBUtility's GenerateImportSchema verb. The command line has the format:

```
mbutility GenerateImportSchema option option ...
```

where the options are:

`/SchemaIdentification:schema`

Specifies the schema whose definition you wish to obtain. This should be one of MBUtility's built-in schemas. Names are case-sensitive. If the schema name contains blank characters, the name should be enclosed in quotes, as in

```
/si:"Storeroom Assignment"
```

`/Output:filename`

A file where MBUtility should write the XML definition of the schema. This file will be written in Unicode characters, which means it should only be edited with software that can deal with Unicode (e.g. Wordpad).

`+EXCEL`

Specifies that the XML code in the schema should be in a format acceptable to Microsoft Excel.

For example, the following creates a schema for unit records, in a format acceptable to Excel:

```
mutility gis /si:Unit /out:unitdef.xml +excel
```

Exporting Data from Your Database

The `Export` verb of MBUtility exports selected data from your database to an output file. For example, you might regularly wish to export data to another application for some reason; by making a command file that uses MBUtility, you could automate the export process, thereby simplifying the task (and also avoiding errors).

The command line for exporting is

```
mutility Export option option ...
```

where the options are:

`/SchemaIdentification:schema`

Specifies a data schema for exporting the data. This should be one of MBUtility's built-in schemas (as discussed in *Built-In Data Schemas on page 45*). If the schema name contains blank characters, the name should be enclosed in quotes, as in

```
/si:"Storeroom Assignment"
```

`/+EmbeddedSchema`

Tells MBUtility to embed the specified data schema in the output file. This is useful if you're exporting the data to software that accepts embedded schemas. However, Microsoft Excel doesn't seem to accept such schemas, so don't use `+es` for going to Excel.

`/-EmbeddedSchema`

Tells MBUtility not to embed a data schema in the output file. This is the default.

`/Output:filename`

Specifies a file where the output should be written. This file will be written in Unicode characters, which means it should only be edited with software that can deal with Unicode (e.g. Wordpad).

`/OrganizationName:name`

The name of the maintenance organization (associated with your MainBoss database). This name is case-insensitive; for example, `MainBoss` is the same as `mainboss`.

`/DataBaseServer:servername`

The name of the server that holds the MainBoss database.

`/DataBaseName:name`

The name of the MainBoss database.

If you specify `/OrganizationName`, you don't have to specify either `/DataBaseServer` or `/DataBaseName`. If you don't specify `/OrganizationName`, you must specify both `/DataBaseServer` and `/DataBaseName`.

For example,

```
mbutility ex /si:Unit /out:myunits /on:MyMainBoss +es
```

exports data about units to a file named `myunits`. The output file will include an embedded data schema for unit records.

An Example of Exporting to Excel 2007

The previous sections of this manual gave basic details of exporting MainBoss data. This section provides a concrete example, showing how to export unit data to Microsoft Excel 2007.

The first step is to create a file containing the data schema for unit data. You do this with the `GenerateImportSchema` verb:

```
mbutility gis /si:unit /out:unitschema.xml +excel
```

This writes the schema into a file called `unitschema.xml`.

The next step is to export the data:

```
mbutility ex /si:unit /out:data.xml /on:mymb
```

This exports data from a database with the organization name `mymb`, and writes the data into a file named `data.xml`.

The next step is to modify the data file's XML code so that it refers to the schema file. Start the Windows `wordpad` command and read in the data file. The second line will look like this:

```
<dsUnit xmlns="http://thinkage.ca/MainBoss/dsUnit.xsd">
```

Using Wordpad, edit the line so that it looks like this:

```
<dsUnit xmlns="http://thinkage.ca/MainBoss/dsUnit.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://thinkage.ca/MainBoss/dsUnit.xsd unitschema.xml">
```

Note that this line ends with the name of the file containing the schema (followed by the characters ">"). Once you've made these changes, save the file.

The data file is now ready to be used by Excel. If you have Microsoft Office 2007, here's what you do:

1. Start Excel.
2. Click the "Office" button (in the upper left hand corner of the Excel window).
3. In the resulting window, click "Excel Options" (at the bottom of the window).
4. In the resulting window, click "Popular" in the left part of the window, then checkmark "Show Developer Tab in the Ribbon" (if it isn't already checkmarked).
5. Click OK to close the options window.
6. In the main Excel window, click "Developer" in the ribbon.
7. In the XML section of the ribbon, click "Import".
8. In the resulting window, specify the name of the data file (in our example `data.xml`).

Excel gives you the option of reading the data file into the current spreadsheet or into a new one.

Importing Data into Your Database

The `Import` verb of `MBUtility` imports data into your database from an input file. For example, if you are migrating to `MainBoss` from some other maintenance management software package, you might be able to import some subset of the data from that other package.

Important: Importing is a complicated procedure, and should only be done by people with strong IT expertise. We strongly recommend that you backup your database before you attempt an import operation. If an error occurs during an import operation, restore the database from backup, correct the error in the import data, then try again.

The command line for importing is

```
mbutility import option option ...
```

where the options are:

`/SchemaIdentification:schema`

Specifies a data schema for exporting the data. This should be one of MBUtility's built-in schemas (as discussed in *Built-In Data Schemas on page 45*). Names are case-sensitive. If the schema name contains blank characters, the name should be enclosed in quotes, as in

```
/si:"Storeroom Assignment"
```

`/Input:filename`

Specifies a file containing the data to input. This file should use Unicode characters.

`/ErrorOutput:file`

Specifies a file where MainBoss should write any error messages that arise during the import process.

`/OrganizationName:name`

The name of the maintenance organization (associated with your MainBoss database). This name is case-insensitive; for example, MainBoss is the same as mainboss.

`/DataBaseServer:servername`

The name of the server that holds the MainBoss database.

`/DataBaseName:name`

The name of the MainBoss database.

If you specify `/OrganizationName`, you don't have to specify either `/DataBaseServer` or `/DataBaseName`. If you don't specify `/OrganizationName`, you must specify both of `/DataBaseServer` and `/DataBaseName`.

For example,

```
mbutility im /si:Unit /in:myfile /eo:errs /on:MainBoss
```

imports unit data from a file named `myfile`.

Important: This version of MainBoss will not let you import data that conflicts with existing records in the database. For example, if you are importing unit data, each new unit's identifier code must be different from any units that are already in the database. This means that you can't export MainBoss data, edit it with some other piece of software, then import it again to overwrite MainBoss's existing data.

If you wish to create a database for testing, we recommend using backup and restore (using [Create New Organization from Backup](#)) rather than exporting and importing data. For more information, see [Backups within MainBoss on page 39](#) and [Restoring a Backup Within MainBoss on page 41](#).

Tip: Sometimes it's difficult to figure out what format to use when you are preparing data for import. When in doubt, start up MainBoss and create a record of the type you intend to import; for example, if you intend to import Unit records, create a Unit record inside MainBoss. Then export the record as previously described in the exporting section. The format of the exported record will be the same that's expected for imported records.

Adding Organizations

The `AddOrganization` verb of `MBUtility` lets you add an organization to the current user's organization list. The database for this organization must already exist and the user must have appropriate permissions on the database (which means that the user's name must be specified in the database's **Users** table).

For example, if you are logged in under the name `jsmith`, you can use `AddOrganization` to put a new organization in `jsmith`'s list of known organizations, provided that `jsmith` appears in the database's **Users** table.

The format of the command is

```
mbutility AddOrganization option option ...
```

where the options are:

+Replace

This option is relevant if the user's organization list already contains an organization with the same name. `+Replace` says the old organization should be replaced with the new organization. If you do not specify `+Replace`, `MBUtility` will not replace old organization's with new ones; if there is a name conflict, you will be receive an error message.

+Probe

If you specify this option, `MBUtility` will attempt to verify that the user can actually access the database. If you do not specify `+Probe`, the database will be added to the user's organization list, but `MBUtility` doesn't check to see if the user can actually connect to the database.

/Mode:startmode

Specifies the default start-up mode when the user connects to the database. The `startmode` value must be one of the following strings:

```
MainBoss Requests  
MainBoss  
View Sessions  
Administration
```

For explanations of these startup modes, see [Start Modes on page 35](#) of this guide.

/OrganizationName:name

The name that should be used in the user's organization list. This name is case-insensitive.

/DataBaseServer:servername

The name of the server where the database resides.

/DataBaseName:name

The actual name of the database that you want to add.

You must specify all three of /OrganizationName, /DataBaseServer and /DataBaseName.

Backing Up Your Database with MBUtility

The Backup verb of MBUtility lets you back up a MainBoss maintenance organization database. The format of the command is

```
mutility Backup option option ...
```

where the options are:

/BackupFile:filename

The name to be used for the backup file. This file should not already exist. Traditionally, SQL Server backup files end in “.bak”, so

```
/bu:"c:\SomeFolder\SomeFile.bak"
```

tells MBUtility to save your database’s data in a file with the given name.

/OrganizationName:name

The name of the maintenance organization (associated with your MainBoss database). This name is case-insensitive; for example, MainBoss is the same as mainboss.

/DataBaseServer:servername

The name of the server that holds the MainBoss database.

/DataBaseName:name

The name of the MainBoss database.

The MBUtility Backup verb is subject to all the conditions that affect the behavior of **Administration | Backups** within MainBoss itself. For more, see *Backups within MainBoss on page 39* of this guide.

Backups done with MBUtility are *not* added to the list in **Administration | Backups**.

Adding an Administrator to a Database

In some rare cases, a MainBoss database may not contain any users who have administration privileges. This may happen, for example, if only one user has administration privileges and that user accidentally deletes his/her name from the **Users** table. It may also happen if an administrator leaves your organization without authorizing anyone to take over administration duties.

In this case, the BreakIn verb of MBUtility gives you a way to plant your own login name in the **Users** table of an existing database, and to give yourself MainBoss Administration privileges. To use this function, you need SQL Server Administrator privileges.

For information on user records, see the reference manual or the online help.

The format of the `BreakIn` command is:

```
mbutility BreakIn option option ...
```

where the options are:

```
/OrganizationName:name
```

The name of the maintenance organization (associated with your MainBoss database).

This name is case-insensitive; for example, MainBoss is the same as mainboss.

```
/DataBaseServer:servername
```

The name of the server that holds the MainBoss database.

```
/DataBaseName:name
```

The name of the MainBoss database.

If you specify `/OrganizationName`, you don't have to specify either `/DataBaseServer` or `/DataBaseName`. If you don't specify `/OrganizationName`, you must specify both of `/DataBaseServer` and `/DataBaseName`.

```
/ContactCode:name
```

Specifies a **Contacts** table entry to be associated with the created **User** record. For example,

```
/cc:"Joe Smith"
```

indicates that the **User** record should be associated with the **Contacts** record with the name Joe Smith. If your login name is already in the **Users** table, you should not specify this command line argument; otherwise, the argument is mandatory.

When the user record is created, it will be in your name (i.e. the login name of whoever executes the `MBUtility BreakIn`). This user record may or may not have a scope name; in particular, `MBUtility` may set the scope name to the name of the computer where you executed `MBUtility`. This means that you will only be able to login from that computer. This is no problem if you are only breaking into the database so that you can set up someone else as a new database administrator. However, if you intend to keep this user record in the long-term, you may wish to edit the record to set the scope name to something more useful.

Appendix A: Setting Up SQL Server

Note: All web addresses given in this appendix are subject to change without notice. If Microsoft does change a web address, go to microsoft.com and search for the appropriate page.

MainBoss Advanced needs to use one of the versions of SQL Server specified in *Microsoft SQL Server on page 2*. If you already have this software installed at your site, MainBoss can use your existing installation. If you do not already have the software, you can purchase SQL Server from Microsoft or download the free version of SQL Server called SQL Express.

Note: Before you look into obtaining any version of SQL Server, check to see if your company already has one installed. Many organizations may already have SQL Server in connection with some other software package.

There are several important options that should be specified when you install SQL Server. Therefore, make sure to follow the installation instructions given later in this appendix.

Server Hardware Requirements: The machine where SQL Server is running should meet the hardware requirements specified by Microsoft for the version of SQL Server you will be using. If you will be running MainBoss Advanced on the same computer, the machine should also meet the hardware requirements for MainBoss Advanced (stated in the main body of this guide).

The speed of the computer where SQL Server runs has a major effect on the overall speed of MainBoss. The effect is far greater than the speed of the computers where people actually run MainBoss.

Authentication within SQL Server: SQL Server offers two types of user authorization: SQL Authentication or Integrated Authentication. MainBoss requires Integrated Authentication. Mixed mode (accepting both authentication types) will work with MainBoss, but mixed mode is offered only for backward compatibility and Microsoft has deprecated it.

Instances

You can have multiple independent copies of SQL Server running simultaneously on the same computer. Each of these is called an *instance* of SQL Server. Each instance maintains its own separate set of database files.

If you already have SQL Server running at your site, it presumably manages a set of databases. Your IT department may prefer to keep your MainBoss database(s) separate from databases for other software packages. You can do that by creating a new instance of the SQL Server. This can be set up so that it only deals with MainBoss databases.

Different instances of SQL Server are distinguished by having different *instance names*. This is just an identifying name. One instance can have its name blank, in which case it's called the *default instance*. If someone creates a SQL Server database on a computer without specifying an instance name, the database is created and managed by the default instance.

By default, the installation procedures for full versions of SQL Server set up an instance with its name blank. However, for SQL Express, the default installation procedure specifies the instance name `SQLEXPRESS`.

SQL Server Installation

The default installation procedures for full versions of SQL Server are designed to let other computers connect with the Server computer. Therefore, their default options will generally work well with MainBoss.

However, the default installation procedure for SQL Express assumes that it will only be used on a single computer, without users on other computers trying to connect with SQL Server. If you intend to have users on other machines connect with SQL Express, you must change a number of default options during the installation. You must also set several configuration options *after* SQL Express is installed, as discussed later in this section. For more information, see *SQL Express Considerations on page 56*.

Overall, we believe customers will find it easier to use one of the full versions of SQL Server than the free SQL Express—full versions are simpler to install and to maintain (e.g. backing up the database). However, SQL Express is available at no charge and can be used successfully with MainBoss, especially by small maintenance departments.

SQL Server on Windows 7, Vista or Server 2008: If you will be installing SQL Server on Windows 7, Vista or Server 2008, we recommend that you read Microsoft's background material provided at

<http://msdn2.microsoft.com/en-us/library/ms143719.aspx>

In particular, make sure you comply with the specified hardware and software requirements.

Default Backup Folder: SQL Server 2008 and R2 let you specify the default folder to be used to hold backup files. (SQL Server 2005 does not provide this ability.) We recommend that you set the default folder to be some device *other* than the disk drive that holds the actual MainBoss database. If your backups go to the same disk that holds your original database, a hardware error on that disk may kill both your database and the backups.

Backups with SQL Server

If you have the full SQL Server, the easiest way to implement backups is to use the automated facilities called *maintenance plans*. To set up a maintenance plan, follow these steps:

1. Start SQL Server Management Studio and connect to the SQL Server instance that manages the MainBoss database.
2. In the left-hand panel, expand **Management**.
3. Click **Maintenance Plans**.
4. In the right-hand panel, right-click. In the resulting menu, click **Maintenance Plan Wizard**.
5. The Maintenance Plan Wizard will walk you through the process of setting up automatic backup procedures.

We do not recommend using the default save folder for the backup file, unless you set the default folder as discussed in the preceding section of this guide. SQL Server's usual default backup folder makes backup files difficult to find and work with, especially on Vista. Instead, we recommend that you save backup files in some folder that you'll remember and find easily. Also, backup files should be copied to some medium that can be removed from the premises; it's important to keep a recent backup off-site in case of fire.

Some commercial backup software packages can work with SQL Server so that SQL Server backups are included when the rest of your computer is backed up. For more information, see the documentation for your backup software.

A formal backup using SQL Server Management Studio is better than just saving the raw disk file(s) containing the database, since a raw save may leave a little bit of data unusable. However, a raw save every day is better than a formal save once a week—losing a week's worth of work is worse than losing a transaction or two.

Note: From time to time, you should check the SQL Server logs to make sure that backups really are taking place successfully. Thinkage has encountered situations where the backup software reports no problems, but where the SQL Server logs show that the database backup failed.

If you do backups directly through SQL Server Management Studio, information about the backup will *not* appear in MainBoss's internal database history (**Administration | Database History**). Furthermore, the backup will not appear in MainBoss's list of known backups (**Administration | Backups**).

Using SQL Server to Restore a Database from Backup

To restore a database from a backup file, follow these steps:

1. Start SQL Server Management Studio and connect to the SQL Server instance that manages the MainBoss database.
2. In the left-hand panel, expand **Databases**.

3. Right-click on the entry for the database you want to restore, then click **Tasks**, then click **Restore**, then click **Database**.
4. SQL Server opens a window displaying your existing backup files. In the list of available backups, click the one you want to restore.
5. Click **OK**.

The restoration process will overwrite any existing contents of the database. Therefore, you should only restore a database if the current contents are no longer usable.

SQL Express Considerations

SQL Express is a free version of SQL Server. It is freely available from Microsoft. For up-to-date information on downloading SQL Express from Microsoft, go to

<http://www.mainboss.com/info/microsoft.shtml>

SQL Express will provide acceptable performance for small sites. Larger sites should buy one of the larger versions of SQL Server.

We should note that SQL Express lacks some features of paid-for versions of SQL Server. For example, SQL Express does not have automatic maintenance plans, Microsoft's facilities that simplifies automatic backups and integrity checks. However, `expressmaint` is a free software package that provides some of the functionality that's missing in SQL Express. For more information, see

<http://www.sqldbatips.com/showarticle.asp?ID=27>

The <code>expressmaint</code> package is not a Thinkage or Microsoft product. Neither MainBoss Support nor Microsoft will provide any support for this package.

The rest of this appendix describes considerations for installing and working with SQL Express.

Installing SQL Express

The following description assumes that you do not have any instance of SQL Server installed on your computer. To determine whether you do have such an installation, go to the Windows Control Panel and check "Add/Remove Programs" (Windows XP and Windows Server 2003) or "Programs and Features" (Windows Vista, Server 2008 or Windows 7).

Microsoft recommends that SQL Express be installed with a limited permission set and/or as a limited user. For information on this process, see

<http://msdn2.microsoft.com/en-us/library/ms143504.aspx>

If you ever intend to have multiple users, we offer the following suggestions as options to choose during installation. Your site might decide to make different choices, but our suggestions should help typical users find their way through the many possibilities.

Unless otherwise stated below, we recommend that you accept the default options in each phase of the installation.

- In the **Instance Configuration** phase of the installation, specify a suitable name for this instance of the server. The default is `SQLEXPRESS`; however, if you are only going to use this instance of the server for MainBoss, you might specify the name `MAINBOSS` to make it clear what the instance is being used for.
- In the **Database Engine Configuration** phase, in the **Data Directories** section, you have the ability to specify a backup directory: the default location for backup files. Ideally, this should be a directory on a different computer than the one holding the original database files—you don't want your originals and your backups to be on the same computer, because if something happens to that computer, you lose everything.

Also in the **Database Engine Configuration** phase, in the **Account Provisioning** section, you can specify who will have administration permissions on this instance of SQL Server. By default, the list will only contain your own name (i.e. the name of the person installing SQL Express). If someone else will be in charge of adding new users to MainBoss, that person will also need SQL Server administration permissions and should be added to the list.

- In the **Server Configuration** phase, set the SQL Server Browser's startup type to `Automatic`.

You should also set the account name(s) to be associated with the database engine and the browser. We suggest that Network Service is the best choice (`NT AUTHORITY\NETWORK SERVICE`). However, the Network Service account is local to this specific computer and typically won't be able to access other computers. This means that SQL Server won't be able to write database backups to other computers. If the current computer has multiple disks, this is acceptable, since you can write backups to a different disk than the one that holds your original database. However, if the current computer has only one disk, this is a problem—writing backups to the same disk that holds your original database gives you almost no protection, since disk problems will likely affect both your original and your backups. In this case, specify an account name with permissions that can write to another disk on another computer.

If you specify an account name other than Network Service to run the database engine, you must ensure that this account is authorized to run services. For information on how to authorize an account for **Log on as a service** permission, see the **Log On As A Service** subsection of *Installing MainBoss Service on page 22*.

The options above constitute a standard configuration for use with MainBoss Advanced. They match Microsoft's recommendations for SQL Server. If you make different configuration choices, you may find you have to make changes in future; also, if you run into trouble, MainBoss Technical Support may recommend that you reset your SQL Server options as listed above.

SQL Express Installation Notes: After installing SQL Express, you must enable TCP/IP connections. This process is described in this guide, in the section *SQL Server Configuration on page 66*.

If you intend to connect with SQL Express from other computers, you must also adjust the Server computer's firewall to allow remote users to connect with the SQL Server and the SQL Server Browser. This process is explained in *Adjusting the Firewall on page 68*.

Finally, you may have to adjust your local security settings to allow access to shared files. This process is explained in *Local Security Settings on page 71*.

Backups with SQL Express

Maintenance plans aren't available with SQL Express. For information on automatic backups with SQL Server Express, see

<http://www.sqldbatips.com/showarticle.asp?ID=27>

Otherwise, just use the backup facilities within MainBoss.

Important: By default, SQL Server configures itself so that backup files are written to the same folder as the databases themselves. **This offers no protection against hardware errors**—if you get a disk crash on the disk that holds the databases, you'll lose the backup files too. Therefore, you should configure SQL Server so that backup files are written to a completely different device, preferably on a completely different computer.

Ideally, you should make copies of your backup files and keep those copies off your premises. That way you don't lose data if there's a fire or some other disaster that affects your entire site.

SQL Server Maintenance

From time to time, you should clean-up your SQL Server database. Clean-up operations can include reorganizing the database index, rebuilding the index from scratch, and various other actions.

If you have a full SQL Server (as opposed to SQL Server Express), you can arrange clean-up operations through SQL Server Management Studio. To do so, follow these steps:

1. Login to an account with Windows Administrator privileges.

2. Start SQL Server Management Studio. (On Windows 7 and Vista, you should use **Run as Administrator**.)
3. In the left-hand panel, expand the entry for **Management**.
4. Right-click the entry for **Maintenance Plans**, and click **Maintenance Plan Wizard**.

The wizard will then walk you through the process of creating a maintenance plan that performs various operations automatically. During the process, you can choose what operations will be performed. As a minimum, we recommend the following:

- Check Database Integrity
- Reorganize Index
- Rebuild Index
- Clean Up History
- Maintenance Cleanup Task

(You can also include a backup operation, although you should already be backing up your database with a different maintenance plan—you don't need to clean your database as often as you need to back it up.)

Once you've used the wizard to create the maintenance plan, you can execute the operations by right-clicking the entry for the maintenance plan, then clicking **Execute**.

If you ever have a system crash or power failure on the server computer, you should make a point of cleaning up your database as soon as possible afterward.

If you have SQL Express, the associated Management Studio does not allow you to make maintenance plans. However, you can perform similar clean-up maintenance operations using the `expressmaint` software discussed in *SQL Express Considerations* on page 56. For more information on cleaning up the database, see the `expressmaint` documentation.

Appendix B: Troubleshooting

This appendix offers some help for determining whether SQL Server and other software are set up properly for use with MainBoss. The appendix also describes tests for checking whether a particular user can access the SQL Server databases. Finally, the appendix provides some tips on how to approach non-standard MainBoss configurations if your IT department insists on deviating from MainBoss's recommended set-up.

General Advice

There are many things that might go wrong when trying to use SQL Server, and Microsoft's diagnostic facilities may not be helpful. If an error condition occurs with SQL Server, MainBoss can only display the diagnostic message that SQL Server or Windows provides, and this might not tell you much.

If you get a diagnostic message that doesn't tell you enough, we recommend that you use Google to search `microsoft.com` for references to the *Details* section of message. (If the Details section is blank, use the main part of the message.) For example, if the Details section of the message is "Some text", you would type the following into Google's search field:

```
site:microsoft.com "Some text"
```

The `site:microsoft.com` tells Google that you only want responses from Microsoft's web site. Putting quotes around "Some text" means that you search for that exact string.

Note that if the error text contains specific references to names of computers, users, etc., you must remove them before you do the search and only put quote marks around each separate section. Also, if the message is very long, you can just extract important sections. For example, if you get the message

```
Login failed for user 'JSMITH'. The user is not associated  
with a trusted SQL Server connection.  
Unable to create the base database session
```

you could write up the Google search as

```
site:microsoft.com "Login failed for user" "trusted SQL Server connection"
```

Note: This appendix uses "the Server machine" to refer to the computer where SQL Server is running and where the MainBoss database is stored. We assume that the MainBoss database already exists, created in accordance with the instructions in the main body of this guide. "The Remote machine" is a different computer from which you want to access the MainBoss database; this computer should be on your local area network (LAN).

Several of the sections in this appendix describe tests you can try if something isn't working. Different tests are certainly possible, but the ones we describe provide a productive route for

checking potential sources of difficulty. All of these tests use standard Microsoft software. If the tests fail somewhere along the way, you can hope that the software will provide an error message that explains what went wrong. You can then fix the problem and try again. Once the test works with Microsoft software, you can try again with MainBoss itself.

The tests described in this section should be carried out in the order given. The purpose of each test is to detect problems in your set-up of Windows, your network, or SQL Server and to determine where the problem lies. It's important to eliminate the possibility of such problems before contacting MainBoss Support—don't mistake a problem in Windows for a problem in MainBoss.

If you have problems with Windows, your network, or SQL Server, contact Microsoft or your software service provider.

File-Sharing

Before other computers can connect with the Server machine, the Server's firewall must be set up to allow file-sharing.

If you have a commercial firewall product (e.g. one that comes as part of an antivirus package), consult the software's documentation for how to allow file-sharing. If you're using the standard Windows firewall, follow these steps:

1. On Windows 7, Vista or Server 2008:
 - In the Control Panel, click **Windows Firewall**.
 - In the resulting window, click **Change settings**.
2. On Windows XP or Server 2003:
 - In the Control Panel, click **Windows Firewall**.
3. A window opens where you can make firewall adjustments. Go to the **Exceptions** section of this window.
4. In the list, go to `File and Printer Sharing`. If the accompanying checkbox isn't already marked, checkmark it.
5. Click **OK** to exit.

This step is required for all the other troubleshooting discussed later in this appendix.

Note also that MainBoss users need read permission on whatever folder holds the MainBoss software that they're supposed to use. If you install the software on individual computers, make sure that on each computer, every person running MainBoss on that computer has read permission on the MainBoss software folder. If you install the software at a shared network location, make sure that every person using that software to run MainBoss has read permission on the shared folder.

Testing for the Server's Machine Presence

To check connections between the Server and Remote computers, the most basic test is a *ping*:

1. On the Remote computer, open a Command Prompt window by clicking the standard Windows **Start** button, clicking **All Programs**, expanding **Accessories** and clicking **Command Prompt**.
2. Type `ping`, followed by a space, followed by the name of the Server computer. For example, if the Server is called `OurServer`, you'd type

```
ping OurServer
```

Wait for results. If the connection can't be made, you'll get an error message or a time-out message (i.e. the `ping` command waited a significant length of time but never got an answer). If the connection can be made, you'll get a message saying that the Server computer replied and providing other statistics.

If `ping` fails, check the documentation on your network software to see what's gone wrong.

There are two types of pings: `ping -4` and `ping -6` (which test for IP4 and IP6, respectively). SQL Server generally uses IP4, so you usually want to use `ping -4`.

Testing That a User Can Connect with the Server Machine

This test determines if a particular user on a particular Remote machine can connect with the Server machine, and that the user has appropriate permissions to access the machine.

The user's login name and password must be the same on the Remote machine as on the Server machine. This will automatically be true if you're using domains. If you aren't using domains, have the user attempt to login to the Server machine using his/her login name and password. If this doesn't work, the login name and/or password must be changed so that they're the same on all relevant systems.

Note: If you aren't using domains, users should be warned that if they change their passwords on one computer, they should change the password on all other computers too. This is especially important on the Server machine.

It's important to note that SQL Server has its own security permissions that are separate from Windows permissions. For example, a disk may have general read/write permissions, allowing any user to read or write any file on the disk; still, SQL Server may only permit access to a limited set of users based on login name and password. If you can't connect to SQL Server, here's a way to make sure that a particular user on a Remote machine has login and password set up correctly.

Before you do this, you have to make sure that you don't have any existing connections to the Server computer. To do that, follow these steps:

1. On the Remote computer (where you'll be doing this test), open a Command Prompt window by clicking the standard Windows **Start** button, clicking **All Programs**, expanding **Accessories** and clicking **Command Prompt**.
2. Type `net use` (this displays any existing connections).
3. If there are no connections listed to the Server computer, you don't have to do anything; just close the Command Prompt window.
4. Otherwise, you have to delete all existing connections to the Server computer.
 - First, write down the information shown about connections to the Server computer. You'll need this information later in order to re-establish the connections. (You can save the output of `net use` in a file by using a command line of the form `net use >file`).
 - If a connection has a letter drive shown in the Local column (e.g. Z:), type a line of the form

```
net use Z: /delete
```

where you replace Z: with the letter shown.
 - If a connection doesn't have anything in the Local column, it will have a name in the Remote column of the form `\\machinename\folder`. Type

```
net use \\machinename\folder /delete
```

where you replace `\\machinename\folder` with the actual names shown.
 - Repeat the above for every connection to the Server computer. You do *not* have to delete connections to any other computer.
 - When finished, it's useful to leave the Command Prompt window open, since you can use it again later.

Note: The connections that you delete may be needed in order for other software to work. If this is so, you must re-establish the connections after you've done the test described in this section. We'll discuss re-connections below.

Once you've got rid of the connections, you can do the following test:

1. On the Server computer, use Windows Explorer to share a test folder with the rest of the network:
 - In Windows Explorer, create a new folder anywhere on the Server computer's disk drive(s).
 - In Explorer's **Tools** menu, click **Folder Options**.

- In the **View** section of the resulting window, go down to the bottom of the list of settings and turn off **Use Sharing Wizard** (on Windows 7 or Vista) or **Use simple file sharing** (on XP).
 - Click **OK**.
 - Right-click on the folder, then click **Share**.
 - In the **Sharing** section of the resulting window, click **Advanced Sharing**.
 - In the resulting window, checkmark **Share this folder**.
 - Click **Permissions**.
 - The resulting window shows who can access the new folder. Remove all existing permissions (if any) by clicking each name in the list, then clicking **Remove**.
 - Once you've removed all existing permissions, click **Add**.
 - Under **Enter the object names to select**, enter the login name of the person on the remote computer whose connectivity you're testing. (This should also be a login name on the Server computer.)
 - Click **OK**.
 - When you return to the previous window, checkmark **Full Control** under the **Allow** column.
 - Keep clicking **OK** until all windows close.
2. On the Remote computer, have the user log in using his/her login name and password.
 3. On the Remote computer, use Windows Explorer to connect to the shared folder.
 4. On the Remote computer, attempt to create a text file in the shared folder. Add text to the file (e.g. using Notepad) and save the file.
 5. On the Remote computer, attempt to delete the file you just created.

If you can do all this and you are never asked to enter a login name and password during the process, the user's network permissions are set up correctly. If you can't do one of these steps or if you have to type in a login name and password before one of the steps works, you don't have the right permissions. See *Local Security Settings on page 71* for suggestions of how to deal with the problem.

Once you've verified that the Remote user can pass these tests, the person who created the original (shared) folder on the Server machine can delete the folder.

Again, we emphasize that setting up a domain will avoid a lot of headaches. Microsoft recommends the use of domains with SQL Server.

If you had to remove any connections before testing the file-sharing, you can reconnect them as follows:

1. On the Remote computer, open a Command Prompt window (or return to the one you already had open).

2. If the original connection had a letter drive (e.g. Z:), type the following:

```
net use Z: \\machinename\folder
```

where you replace Z: with the letter drive it had previously and replace \\machinename\folder with the previous value. You may be asked to enter a login name and password.

3. If the original connection had no letter drive, type

```
net use \\machinename\folder
```

where you replace \\machinename\folder with the previous value. Again, you may be asked to enter a login name and password.

4. Repeat the above for every previous connection to the Server computer.

Comparing the DNS Name and Active Directory Name

It is possible for the DNS name of a system to get out of synch with the Active Directory name. (We have observed that this happens relatively often on Windows 7 and Vista, though not on XP.) If the names get out of synch, all kinds of anomalous problems may occur. Therefore, it's important to make sure these names refer to the same thing. To do this, follow these steps (on both the server computer and the remote computer where you're having trouble):

1. Open a Command Prompt window.

2. Type the following:

```
ipconfig
```

The system will display a list of information, including the IP address of the computer.

3. Type the following:

```
nslookup
```

The system will display some information, then type > to prompt for more input.

4. Type the name of the current computer (then press <Enter>). The computer will type the IP address of the computer.

5. Type `exit` to quit the `nslookup` program.

Both `ipconfig` and `nslookup` should display the same IP address for the computer. If not, the names are out of synch and you'll have to reset one or the other. For information on resetting these names, see your Windows documentation.

SQL Server Configuration

As noted in *SQL Server Installation on page 54*, the default installation procedures for SQL Server set things up so that SQL Server allows access to users on other computers via TCP/IP. However, they may have been disabled after installation. (Also some older versions of SQL Server have TCP/IP disabled by default.) Therefore, you may need to enable TCP/IP connections. To do so, follow these steps:

1. In the Windows **Start** menu, locate the entry for your version of SQL Server. Under this entry, locate **Configuration Tools** and then **SQL Server Configuration Manager**. This opens a window where you can configure your SQL Server.

If you can't find an entry for **SQL Server Configuration Manager**, you'll have to add the software. See "Maintenance Installs" below.

2. In the left-hand side of the window, expand the entry for SQL Server Network Configuration.
3. In the resulting expansion, click **Protocols for MAINBOSS**. (This will have a different name if you chose a different instance name.)
4. If MainBoss will be used on a network, with or without a domain, right-click on **TCP/IP** in the right-hand side of the window and click **Enable** (if this isn't already enabled). You do not have to do this if you'll only be using MainBoss on a single computer.

A message will appear saying that your changes will only take effect once you stop and restart the service. The steps below do exactly that.

The list of protocols also offers the possibility of enabling SQL Server access through named pipes. However, Microsoft recommends that you don't use named pipes across a network. See below for more on named pipes.

5. In the left-hand side of the window, click the entry for SQL Server Services. You should see an entry for **SQL Server (MAINBOSS)**. (If you used a different instance name than **MAINBOSS**, that name will be displayed instead.) Right-click on this entry, then click **STOP**. (This will actually stop both instances displayed in the right-hand side of the window.)
6. Right-click on **SQL Server (MAINBOSS)** and click **START**.
7. Right-click on **SQL Server Browser** and click **Properties**. This opens a window where you can set the browser's properties.
8. In the **Service** section of the properties window, click **Start Mode**.
9. Drop down the associated arrow (at the end of the line) and click **Automatic**.
10. Click the window's **Apply** button.

11. In the **Log On** section of the same properties window, click **Start** to start the browser again.

12. Click **OK** to close the window.

Named Pipes: As noted above, you have the option of allowing SQL Server to use named pipes in addition to TCP/IP. We strongly recommend that you disable named pipes. There are several reasons.

- Each named pipe counts against the maximum number of sessions that Windows allows, while TCP/IP connections do not. Therefore, using named pipes decreases the number of people who can use the Windows system for other purposes.
- The default permission structure associated with named pipes essentially means that Windows Administrators can access SQL Server but nobody else can. It's possible to change the structure, but this is seldom done.
- If you *do* enable named pipes (e.g. because some other software using SQL Server requires them), you'll have difficulties debugging any TCP/IP problems that might arise. The reason is that the .NET framework (which underlies MainBoss) attempts to contact SQL Server first through shared memory; this won't work if SQL Server is running on a different computer. Next, .NET tries TCP/IP, which is the preferred connection method...but if this fails for any reason, .NET immediately goes on to try named pipes. You will *not* receive any error message explaining what happened to TCP/IP. If named pipes work, they'll count as a Windows session (as discussed above), and if they don't work, you'll get an error message related to named pipes, rather than one telling you the problem with TCP/IP. In other words, named pipes simply interfere with your ability to get TCP/IP working properly.

As this discussion shows, we see no good reason for using named pipes and a number of reasons not to. Avoid them if possible.

Maintenance Installs: When your SQL Server was installed, it's possible that SQL Server Configuration Manager was omitted—its installation is optional. If you're missing the configuration manager, you'll have to do a *maintenance install* to add the software.

To do this, start the SQL Server or SQL Express installation again. Tell the installation procedure that you want to change the installation, then follow the suggestions given in *Installing SQL Express on page 56*.

Starting the SQL Server Browser: The SQL Server browser makes it possible for other computers to detect SQL Server on the server system. If the browser is not running, instances of SQL Server on this computer will not appear in the drop-down list for “**Database Server**” when you are specifying a maintenance organization. (See, for example, *Creating a Maintenance Organization on page 7*.)

By default, the browser is installed when you install the rest of SQL Server. For full versions of SQL Server, the browser is also set up to start automatically. However, for SQL Express, the browser is *not* set up to start automatically. To set it up that way, follow these steps:

1. In the Windows **Start** menu, locate the entry for the version of SQL Server you are using. Under this entry, locate **Configuration Tools** and then **SQL Server Configuration Manager**. This opens a window where you can configure your SQL Server.
2. In the left-hand panel, click the entry for SQL Server Services.
3. In the right-hand panel, examine the entry for **SQL Server Browser**. If the state is *Running*, the browser is already configured to be active. You can quit and skip the remaining steps below.
4. If the state is *Stopped*, you must set up the browser for automatic start. Right-click the entry for **SQL Server Browser**, then click **Properties**.
5. In the resulting window, go to the **Service** section.
6. Click the entry for **Start Mode**. Click the value associated with this entry; this opens a drop-down list. In the list, click *Automatic*.
7. Click **OK**.
8. When you return to the previous window, right-click the entry for **SQL Server Browser**. In the resulting menu, click **Start**.
9. Exit the Configuration Manager.

Adjusting the Firewall

In order for other computers to access SQL Server on the Server machine, you must configure the Server machine's firewall to allow such access. (If SQL Server is already in use at your site, the Server machine is probably configured appropriately all ready.)

The following considerations apply:

- If you're running an anti-virus program, it has probably installed its own firewall. Check the program's documentation for how to grant access to SQL Server.
- If you're using the Windows XP or Windows Server 2003 firewall, check the MainBoss web site for a program that will create a rule to allow access through the firewall. You can determine the pathname as follows:
 1. Start the SQL Server Configuration Manager on the computer where SQL Server is running.
 2. In the left-hand panel, click the entry for SQL Server Services.
 3. In the right-hand panel, right-click the entry for **SQL Server (MAINBOSS)** or whatever entry there is for SQL Server itself.
 4. In the resulting menu, click **Properties**.
 5. In the properties window, go to the **Service** section.

6. Double-click on the **Binary Path** entry. Windows will display the name of the SQL Server executable file; grant access through the firewall to this file, as described in the next section.
7. Repeat steps 3-6 for **SQL Server Browser** in the right-hand panel.

Granting Access to a Program through the Firewall

If you have commercial firewall software (typically part of an antivirus package), follow the software's instructions to let SQL Server and the SQL Server browser through the firewall (as discussed in the previous section). If you use the built-in Microsoft firewall, follow these steps.

1. On Windows 7, Windows Vista or Server 2008:
 - In the Control Panel, click **Windows Firewall**.
 - In the resulting window, click **Change settings**.
2. On Windows XP or Server 2003:
 - In the Control Panel, click **Windows Firewall**.
3. A window opens where you can make firewall adjustments. Go to the **Exceptions** section of this window.
4. Check in the list to see if `sqlbrowser.exe` and `sqlservr.exe` are already there and checkmarked. If so:
 - Double-click on `sqlbrowser.exe`. A window will open to show you the full pathname of the file. Check that the pathname refers to the SQL Server you will be using. (This is necessary in case you have multiple versions of SQL Server on your computer, or if the entry for `sqlbrowser.exe` refers to the software for some previous version of SQL Server.) If so, click **OK** to exit.
 - Repeat the above procedure for `sqlservr.exe`.
5. If `sqlbrowser.exe` and `sqlservr.exe` are both in the list, both checkmarked, and both refer to the correct programs, you're finished—click **OK** to exit.
6. If the correct files are in the list but not checkmarked, checkmark them then click **OK** to exit.
7. If one or both file names are missing, click **Add Program**.
8. In the resulting window, click **Browse**.
9. In the resulting window, find the name of the SQL Server executable file (see the previous section of this guide for how to find this name). Click the file name, then click **Open**.
10. You'll return to the previous window. Click **OK**. The file is added to the list.

11. Repeat steps 7-10 for the SQL Server browser. Click **OK** when you're done.

Scopes: Each program in the Windows Firewall list has an associated *scope* (unrelated to scopes in MainBoss). The scope may be any of the following:

- Any computer**, in which case the firewall lets the program be used by any computer anywhere (including those on the Internet).
- My network**, in which case the firewall only lets the program be used by computers in your local area network.
- Custom list**, in which case the firewall only lets the program be used by a specified list of computers (e.g. ones identified by IP number).

Most sites will wish to restrict MainBoss access to users on your local area network (**My Network**), not to users anywhere on the Internet. If you open up access to all Internet users, you must be sure that you've protected yourself with appropriate security measures.

Your usage requirements may change with time. For example, you may originally restrict MainBoss access to **My network**. Later on, you might decide that you want to be able to connect from outside sites (e.g. when working at home or at a remote job site), in which case you'll have to change your configuration.

To see the scope associated with a program (and possibly to change it), follow these steps:

1. Follow steps 1-3 listed earlier in this section.
2. In the **Exceptions** section of the firewall settings window, click the entry for `sqlservr.exe`.
3. Click **Properties**.
4. In the resulting window, click **Change Scope**.
5. In the resulting window, check the scope. If it isn't what you want, change the setting.
6. Click **OK** twice to return to the firewall settings window.
7. Repeat steps 2-6 for `sqlbrowser.exe`.

Firewall Off and On

Some versions of Windows incorrectly report that the firewall is off when it's actually on. Specifically, suppose you go to **Windows Firewall** in the Windows control panel. Your computer will respond with a window that tells you whether the firewall is off or on, *as set by the last time you used this window*.

However, it is possible to turn the firewall off/on using other windows. In particular, you can turn it off or on using the Services window (obtained by selecting **Manage on Computer** or

My Computer). If you turn the firewall off or on using the Services window, the other window (accessed through the control panel) doesn't change.

As a result, the firewall may be on, even though the control panel says it's off. Even more confusing, it is sometimes possible for administrators to access the database just fine, but others cannot. We've seen this happen because the firewall was letting named pipes access the MainBoss database; people allowed to use the named pipes could get access while others could not.

If you find yourself in this position, go to the Services window and make sure that the Windows Firewall service is actually in the condition you think it is (stopped or started). You may need to start or stop the service in order to put it into the state you actually want.

Local Security Settings

If you are not using domains and you intend to use MainBoss on multiple machines, you may have to change the security settings on the computer where SQL Server is running. **This is unnecessary if you're using domains.**

In many cases, the security settings will already be correct by default. However, some versions of Windows XP (and possibly Vista) do not have the correct settings. Also, if you upgrade your version of Windows, the upgrade process retains your old settings, even if they're different from the usual defaults of your new operating system.

To set up the correct settings, follow these steps on the computer where SQL Server is running:

1. In the Windows Start menu, click **Control Panel**.
2. In the resulting menu, click **Administrative Tools**.
3. In the administrative tools menu, click **Local Security Policy**. This opens a window where you can change the security settings.
4. In the left-hand panel of the window, expand **Security Settings**, then expand **Local Policies**, then click **Security Options**. MainBoss opens a list of security options you can set.
5. Double-click on the entry for **Network access: Sharing and security model for local accounts**. This opens a window where you can set the option.
6. In the drop-down list, choose the entry for **Classic - local users authenticate as themselves**.
7. Keep clicking **OK** until you've closed all the windows.

The alternative to **Classic** is that anyone logging into the computer will end up as a user called Guest (provided that Guest is enabled which is not true on many systems). Such a user

would not be able to use MainBoss unless you authorized `Guest` as a MainBoss user...but then *anyone* could use MainBoss since `Guest` usually requires no password.

Authorizing Users in SQL Server

If you have checkmarked the option **MainBoss manages SQL Security** in the **Defaults for User** section of **Administration | Users**, then MainBoss automatically gives new users appropriate permissions to access the MainBoss database through SQL Server. If you have turned off this option, you must authorize users manually. You might also have to authorize a user manually if someone else (or another program) has de-authorized the user for some reason.

In order to follow the steps described in this section, you must have SQL Server Administrator permissions on the SQL Server that manages MainBoss.

The following steps describe how to check whether a user has appropriate permissions for accessing the MainBoss database through SQL Server. The steps also describe what to do if permissions for a user have somehow been removed:

1. On the computer where SQL Server is running, start SQL Server Management Studio.
2. When Management Studio asks to specify the “**Server Name**”, give the name of the instance of SQL Server that holds the MainBoss database. (This is the same server name you specified when you created the database.)
3. Click **Connect**. Management Studio will open a window showing the configuration of the given instance of SQL Server.
4. In the left-hand panel, expand the entry for **Security**.
5. Under **Security**, click **Logins**. Management Studio will display a list of authorized users. This list may contain user groups as well as the login names of individual users.
6. If the user you want to authorize isn't currently in the list:
 - Right-click **Logins**.
 - In the resulting menu, click **New Login...** Management Studio will open a window where you can authorize a new user.
 - In “**Login name**”, enter the login name of the person you want to authorize. This must be a valid login name on the computer where SQL Server is running.
 - Click **OK**.
7. Once the user's name is on the list of logins, you must check that the user has correct permissions for accessing the MainBoss database. Right-click the name of the user in the right-hand panel, then click **Properties**. MainBoss opens a window providing information about the user.

8. In the left-hand panel of the “Login Properties” window, click **User Mapping**.
9. In the right-hand panel, checkmark the entry for the MainBoss database (if it isn’t already checkmarked). Management Studio will highlight the line and put the user’s login name in the “User” column.
10. The entry in the “Default schema” column should be “dbo”. If it isn’t:
 - Click the drop-down button (...) at the end of this line. Management Studio opens a window where you can specify a default schema.
 - Under “Enter the object names to select”, type “dbo”.
 - Click **OK**. The original line should now give the name of the MainBoss database, the user’s name, and “dbo”.
11. Under “Users mapped to this login”, make sure the name of the MainBoss database is highlighted.
12. Under “Database role membership for:”, checkmark **MainBoss** (if it isn’t already).
13. In the left-hand panel, click **Status**.
14. Click **Grant** and click **Enabled** (if they aren’t already).
15. Click **OK**.
16. Repeat Steps 6-15 for every user you want to authorize.

Remember that the name you specify must be a valid login name for the current computer. When logging in from other computers, users must have the same name and password as on the computer where SQL Server is running. (This will always be true if you use domains, since the whole point of domains is to let users have the same name and password on multiple machines.)

Spelling: If a particular user can’t access the MainBoss database, always check that the user’s name is spelled correctly in the various places it should appear, e.g. MainBoss’s **Users** table and SQL Server’s **Logins** list.

Groups: SQL Server lets you grant permissions to user groups as well as individuals. Therefore, you might choose to use the above procedure to grant permissions to a “MainBoss User” group. Once you do that, you can add new users to the group and they automatically receive SQL Server permissions on the MainBoss database. However, the **Users** table inside MainBoss *only* allows individual login names, not groups.

Note that you might be tempted to set up SQL Server permissions so that *anyone* can access the MainBoss database. However, MainBoss itself will only work for people explicitly authorized in the MainBoss **Users** table. If you grant SQL Server permissions to all users, you end up with the undesirable situation where some people may be prevented from using MainBoss itself, but could still change the database by hand (e.g. with Microsoft Access) if

they wanted to. If someone can access the database, it's best to make sure that they do it by using MainBoss, not some other piece of software.

Deleting Users: When you add a user to **Administration | Users**, MainBoss grants that user permission to connect with SQL Server (if you've turned on the **MainBoss manages SQL Security** option). However, when you delete a user from the **Users** table, MainBoss does *not* delete the user's permission to connect with SQL Server—the user may need “Connect SQL” permission in order to use SQL Server with another software package.

If you wish to completely remove a user's access to SQL Server, remove the user's name from SQL Server's **Logins** list, using SQL Server Management Studio.

Testing Whether a User Has Access to SQL Server and the MainBoss Database

In order to access the MainBoss database from a Remote machine, a user must have appropriate permissions with SQL Server. The following procedure can be used to determine if a user has these permissions. (In order for this to work, the user who performs the test must have administrator privileges, i.e. be part of the `Administrators` group.)

1. Login to the Remote machine in question under the login name you want to test.
2. Click the usual Windows Start button, then click **Control Panel**.
3. In the resulting menu, click **Administrative Tools**.
4. In the Administrative Tools menu, click **Data Sources (ODBC)**. (On Windows 7, Vista and Server 2008, you may be asked for permission to continue. Click **Continue**.)
5. In the resulting window (ODBC Data Source Administrator), go to the **System DSN** section.
6. Click **Add**.
7. In the list, click **SQL Server** (typically near the bottom of the list), then click **Finish**.
8. Windows opens a box where you can create a new data source for SQL Server. For **Name**, specify anything (e.g. `TEST`). In **Server**, pick the SQL Server where MainBoss resides.
9. Click **Next**, then click **Next** again.
10. Checkmark **Change the default database to:**. In the resulting drop-down list, pick the name of the MainBoss database on the SQL Server system.
11. Click **Next**, then click **Finish**.
12. Click **Test Data Source**.

You should end up with a window saying that the test completed successfully.

Once you get the message that the test completed successfully, you can click **OK** twice. This gets you back to the ODBC System Administrator window. At this point, you can **Remove** the

data source that you just added. This doesn't do anything to the MainBoss database, it just removes the entry from the list. Click **OK** to finish up.

Remember, if you get an error during this process, use Google to look up the error message: you may get useful tips about what went wrong.

Testing Database Access with Microsoft Excel

You can test your access to the MainBoss database by using Microsoft Excel. Any user can perform this test, but the Excel software must be installed on your system.

If you have Microsoft Office 2007 or 2010:

1. Login to the Remote machine in question under the login name you want to test.
2. Start Microsoft Excel.
3. In the menu bar, click **Data**.
4. In the ribbon, click **From Other Sources**, then click **From SQL Server**.
5. Excel opens a window for you to specify a SQL Server connection. Under **Server Name**, enter the name of the SQL Server that holds the MainBoss database. Click **Next**.
6. Select the name of the MainBoss database from the drop-down list.
7. The wizard displays a list of tables in the MainBoss database. Since this is just a test, you can select any table; **License** is a good choice since it always contains a few lines of data, but not too much. Select this table.
8. Click **Next**, then click **Finish**.
9. Excel displays a window asking how you want to view the data. Just click **OK**.

If all goes well, Excel will insert your license keys and other data into the current spreadsheet. If this process works, the user has all the correct permissions to access the MainBoss database. If not, error messages from Excel may help you determine what went wrong. You may also find the following article useful:

<http://www.microsoft.com/technet/prodtechnol/sql/bestpractice/CISQL2005ASCS.msp>

If you have Microsoft Office 2003, the process is similar to the one above. To begin, go to Excel's **Data** menu, click **Import External Data**, and then **Import Data**. In the resulting menu, click **New Source**. From that point onward, the process is essentially the same as above, starting at Step 4.

Testing Database Access with SQL Server Management Studio Express

If you don't have Microsoft Word on a particular system, you can test database access with SQL Server Management Studio Express, available free for download from Microsoft:

<https://www.microsoft.com/downloads/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en>

Follow these steps:

1. Have a privileged user install SQL Server Management Studio Express on the Remote computer where you wish to test access.
2. Under your own login name, start Management Studio Express.
3. When the software asks you to specify a server name, enter the name of the Server computer, followed by a backslash, followed by the SQL Server instance name where MainBoss is running, e.g. MYSERVER\MAINBOSS.
4. Click **Connect**.
5. In the left-hand panel, expand the entry for **Databases**.
6. Expand the entry for the MainBoss database.
7. Expand the entry for **Tables**.
8. Expand the entry for **dbo._DAccessCode**.
9. Expand the entry for **Columns**.

If you can see entries for **Code** and other data fields, SQL Server is allowing you to look at the database. (You don't need to see the actual database values.)

Testing POP3/IMAP4 Permissions for MainBoss Service

The **MainBoss Service** module needs to obtain mail messages from its mailbox using either the POP3 or IMAP4 protocols (techniques for accessing a mailbox). Some sites configure their systems to prevent POP3 and/or IMAP4 from being used. Therefore, it's useful to test whether these protocols are usable on the computer where you've installed MainBoss Service (see *Installing MainBoss Service on page 22*).

If you intend to use POP3 or POP3 with SSL, and if you have the Telnet client installed on your system, it's easy to test whether POP3 is enabled. (If you do not have the Telnet client installed, you can install it by opening the **Programs and Features** entry of the Windows control panel. Click **Turn Windows features on or off**, and checkmark **Telnet Client** in the resulting window.)

With Telnet client installed, you can test whether POP3 is enabled by opening a command prompt window and entering

```
telnet SYSTEMNAME 110
```

where SYSTEMNAME is the name of the computer that handles your e-mail (e.g. mailhandler.ourcompany.com). If the answer begins with the characters +OK, then POP3

or POP3 with SSL is enabled. Similarly, if you intend to use IMAP4 or IMAP4 with SSL, enter the command

```
telnet SYSTEMNAME 143
```

If the answer begins with the character * OK, then IMAP4 or IMAP4 with SSL is enabled.

Unfortunately, this approach won't work if you intend to use POP3S or IMAP4S. In that case, the easiest way to check is to try to create a POP3S or IMAP4S mailbox. (This approach will also work to test normal POP3 and IMAP4, with or without SSL.)

Different mail software products have different ways of creating mailboxes. If you have Microsoft Outlook or Outlook Express, you can do the following:

1. In Outlook's **Tools** menu, click **E-Mail Accounts**.
2. In the resulting wizard, click **Add a new e-mail account**.
3. Click **Next**.
4. In the resulting window, click **Add**.
5. Click either **POP3** or **IMAP** (whichever you're using for MainBoss Service).
6. Click **Next**.
7. If you have configured MainBoss Service to use POP3S or IMAPS (which is recommended), checkmark **Log on using Secure Password Authentication (SPA)**.
8. Continue to fill in information as the wizard requires. Make sure that you use the same port numbers that you specified when configuring MainBoss Service.
9. When you've finished creating the account, send mail to it and see if the mail arrives.

As noted, some sites have set up their e-mail systems to prevent POP3 and/or IMAP4, since these protocols can create security holes if used in the wrong context. This has led some sites to ban the protocols entirely, even though they are safe when used in the right context. If your site has banned the protocols, the information in

<http://www.mainboss.com/english/products/pop3.shtml>

may help convince your IT department that the protocols can be allowed for MainBoss.

On Windows 7 and Vista, if you don't have Outlook, you can use the built-in Windows Mail software. The process for adding a new account isn't exactly like the procedure above, but it's similar.

Odd Processing by Outlook/Exchange: Several MainBoss customers have encountered an odd behavior in Outlook and/or Exchange where HTML messages are mistaken for plain text. As a result, Outlook/Exchange tells MainBoss that a message is plain text, when it's really HTML; the result is that MainBoss displays mail messages as raw (hard-to-read) HTML, rather than processing them correctly. For help in fixing this behavior, see our online FAQ article at:

Testing Access to the MainBoss Service Event Log

In order to see the MainBoss Service event log, various conditions have to be met (as explained in *The MainBoss Service Event Log on page 31*). You can test these conditions as follows:

1. Click on the Windows **Start** button.
2. Right-click **My Computer** (Windows XP and Server 2003) or **Computer** (Windows 7, Vista and Server 2008).
3. In the resulting menu, click **Manage**.
4. In the left-hand panel of the resulting window, right-click **Computer Management (Local)**.
5. In the resulting menu, click **Connect to another computer**.
6. In the resulting window, fill in “**Another computer**” with the name of the computer where MainBoss Service is installed.
7. Click **OK**.

If this works (i.e. if you don't get an error message and you can see useful information in the next screen), then you have appropriate permissions to see the MainBoss Service event log. The MainBoss Service computer and the computer where you are logged in are both configured to allow the event log to be seen.

Testing that You Can Start and Stop MainBoss Service

As discussed in *Installing MainBoss Service on page 22*, you can start and stop MainBoss Service from a computer other than the one where MainBoss Service is installed, provided you have appropriate permissions and the MainBoss Service computer is appropriately configured. As a quick test for checking whether these conditions are met, follow these steps:

1. Open a Command Prompt window by clicking the standard Windows **Start** button, clicking **All Programs**, expanding **Accessories** and clicking **Command Prompt**.
2. Type `sc`, followed by “ `\\`”, followed by the name of the computer where MainBoss Service is running. After this type a space followed by `query`. For example, if the MainBoss Service computer is called `MBServ`, you would type

```
sc \\MBServ query
```

If this works correctly, you'll get a list of all the services running on the MainBoss Service computer. This means you can start and stop services on that computer. Otherwise, you'll get

an error message, indicating that conditions for starting and stopping services haven't been met.

General Troubleshooting

In addition to all the specific troubleshooting points listed in the appendix, there are a number that always apply to Windows programs.

- Check for viruses. Viruses can cause almost any kind of strange behavior.
- Check your disks for hardware problems. The most thorough way of doing this is using the CHKDSK command. In a command prompt window, type

```
chkdsk /r /f
```

Then reboot your computer. The boot process will do a lengthy but thorough check to find disk errors and recover from them.

- Check your event logs. You do this starting with the **Control Panel**. Go to **Administrative Tools**, then select **Event Viewer**. Check especially for errors and warnings—these may indicate problems with your computer (e.g. hardware errors or viruses).

If you expand **Window Logs** in the left-hand panel and then click **System**, the center panel will list recent events for your computer. Any marked with red error signs are particularly serious and may indicate critical problems with your hardware or software. Remember, use Google to look up any error messages.

Appendix C: MainBossRemote

This appendix offers instructions on setting up a web site for use with the MainBoss Advanced **Web Requests** and **Web Access** modules. These modules provide the ability to deal with work orders and requests through the Internet. The web-based facilities of MainBoss Advanced are supported by software called **MainBossRemote**.

Before setting up MainBossRemote, first make sure that MainBoss Advanced is working properly through direct network access (as described in the main body of this guide).

MainBossRemote System Requirements

MainBossRemote is an ASP.NET web application which must run on a Windows system. This means that the web site used by MainBossRemote must be hosted on a Windows system and must use the IIS web server.

We recommend that you use IIS 7 or IIS 7.5 running on either Windows Server 2008 (with Service Pack 2 or later) or R2.

IIS 6 on Windows Server 2003: This version of MainBoss requires .NET 4. Microsoft has stated that .NET 4 web applications will run under IIS 6 on Windows Server 2003. However, getting such applications up and running is so technically difficult that Thinkage will not attempt to give guidance on the process. Thinkage will provide support for any problems that you might run into with MainBoss *after* you get it running successfully with IIS 6—we will support Thinkage software—but we cannot support the initial installation or configuration process, due to all the complications with Microsoft software.

Thinkage does not support the installation of MainBossRemote on the workstation versions of Windows XP, Windows Vista or Windows 7.

Whatever version of IIS and Windows you use, you should use Windows Update to keep the software up to date.

Minimum Server Configuration

It is beyond the scope of this guide to discuss complete configuration of a Windows web server. However, the following list gives a recommended minimum of what is required in the web server. (This list is for Windows Server 2008 R2. The list is similar for Windows Server 2003 and Windows Server 2008, but there may be slight differences.)

- Required server roles (specified by using the **Add Roles** wizard during initial Windows configuration or through the functions of Manage Computer):

- Web Server (IIS)
- Application Server
- For the role services of Application Server, select **Web Server (IIS) Support** (and all the required services).
- For the role services of Web Server (IIS), select all the defaults dictated by the previous settings. This includes the following:

Common HTTP Features:

- Static Content
- Default Document
- Directory Browsing
- HTTP Errors
- HTTP Redirection

Application Development

- ASP .NET
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters

Health and Diagnostics

- HTTP Logging
- Logging Tools
- Request Monitor
- Tracing

Security

- Basic Authentication
- Windows Authentication
- Digest Authentication
- Client Certificate Mapping Authentication
- IIS Client Certificate Mapping Authentication
- URL Authorization
- Request Filtering
- IP and Domain Restrictions

Performance

- Static Content Compression
- Dynamic Content compression

Management Tools

- IIS Management Console
- IIS Management Scripts and Tools
- Management Service

Note that with IIS 7.5 running on Windows Server 2008 R2, some of the above are *not* selected by default. In particular, “HTTP Errors” and “HTTP Redirection” are not selected by default. Therefore, you must activate them manually.

License Keys

Before you begin setting up MainBossRemote, record your **Web Requests** and/or **Web Access** license keys in the MainBoss database. To do this, follow the instructions in *Entering License Keys* on page 9.

You cannot use **Web Requests** or **Web Access** without appropriate license keys. To obtain such keys, contact your MainBoss dealer or e-mail info@mainboss.com.

Initial Set-Up

Create a folder which will hold all the files required to support the web site. By default, IIS runs from a folder named C:\inetpub; therefore, you might run MainBossRemote from a subfolder called

C:\inetpub\wwwroot\MainBossRemote

Very Important: Set-up will be much easier if you set up the IIS server on the same computer where you run the SQL Server for MainBoss's database. Having the two on different computers adds many complications to the configuration process.

You obtain the MainBoss Remote software by downloading it from our mainboss.com web site. Follow the instructions on the web page to download the necessary files and to copy them to an appropriate folder.

In setting up IIS, follow Microsoft's documentation. Considerable differences exist between the various Windows systems that might be used. For a discussion of IIS configuration, see <http://msdn.microsoft.com/en-us/library/ms178477.aspx>

The above web page contains links that explain how to start the IIS manager on supported versions of Windows.

Note: The rest of this appendix applies to set-up and configuration using IIS 7 or 7.5 on Windows Server 2008 (SP2 or R2).

Security Considerations

Before proceeding to configure your MainBossRemote web site, you must make some decisions about security. This section discusses various factors that you should consider.

Depending on your ways of working, especially with cell phones and similar devices, you may find you have to sacrifice some level of security in order to get anything done. You may decide this means you won't use cell phones with MainBossRemote; alternatively, you may decide to live with reduced security or other complications. Thinkage takes no responsibility for any problems you may encounter if you opt for reduced security.

Web Requests: In order to use the **Web Requests** module, users must type in their e-mail address and send it to the MainBossRemote web page. This process must have anonymous authentication: anyone who can access the web page is allowed to type in an e-mail address and submit it. (Processing only continues if the e-mail address is authorized to submit requests.)

If you do not have the **Web Requests** module, you do not have to allow anonymous authentication to this particular facility.

Web Access: In order to use the **Web Access** module, your MainBossRemote web site must be able to authenticate people as Windows users on the system where the web site runs. This means that people must enter their Windows login names and passwords.

The safest way to do this is to use ASP.NET's integrated Windows Authentication. When users attempt to use the **Web Access** module, they will be asked to send the login names and passwords, which will be securely encrypted when transmitted to the MainBossRemote site.

Unfortunately, integrated authentication does not work with some cell phone and PDA services. Whether or not the device itself can handle encryption, the service provider may use proxy servers that do not support integrated authentication. (This may mean that the device works fine when connected to your own Wi-Fi network but not when connecting through the device's usual service provider.) The symptom of this is that you aren't asked for your login name and password; you simply get a "permissions denied" message.

If the cell phones or PDAs that you intend to use can't handle integrated authentication, you must consider your options.

- One choice would be not to support access through these devices—users would only access MainBossRemote through networked computers or through handheld devices that *do* allow integrated authentication.
- The other choice would be to use "classical" authentication. If you go this route, you have two further options:
 - Using SSL (Secure Socket Layer) or TLS (Transport Layer Security). Users will access the MainBossRemote web site with `https` rather than `http`, as in `https://www.ourorg.com/MainBossRemote`

If the device supports this facility, login names and passwords will be encrypted when transmitted.

In order to take this approach, IT personnel will be required to set up SSL/TLS

access, which includes the use of a security certificate. See below for more details.

- No encryption. In this case, login names and passwords will be sent in plain text through wireless connections. This leaves you seriously exposed to wireless eavesdroppers, and is therefore not recommended.

Security Certificates: A security certificate may be obtained from a trusted Certification Authority (CA) or may be self-generated. A CA security certificate may cost a lot of money; however, large organizations often have a CA certificate already, in which case the same certificate may be used for MainBossRemote.

You can create your own self-generated security certificate using the IIS 7 manager. (See *Initial Set-Up on page 82* of this guide for a reference on how to start the IIS manager.) Once you've started the manager, click the entry for the server in the left-hand panel, then click **Server Certificates** in the **IIS** section of the middle panel. In the resulting window, click **Create Self-Signed Certificate** (in the right-hand panel) to create a self-signed certificate.

If you use a self-signed certificate, devices using `https` to connect to your MainBossRemote web site must be told to trust this certificate. Note that most browsers display strong warning messages when a user first tries to connect with a web site that has a self-signed certificate; therefore, users must be reassured that connecting with your site really is secure.

If you are using SSL/TLS, make sure that your firewall allows such communications through. Typically, SSL/TLS use port 443, so the firewall should allow connections to this port (if you wish to open your web site to outside connections).

Application Pools

Roughly speaking, an application pool consists of one or more web applications that share processing time together as a single process. You must decide whether to put MainBossRemote into an existing application pool or to create a new pool that only contains MainBossRemote. The following considerations apply:

- Each application pool takes up a considerable amount of memory. Therefore, you can reduce memory requirements if you put MainBossRemote into an existing pool.
- Since all applications in a pool must share the processing time allocated to that pool, MainBossRemote will have to share time with everything else in the pool. In particular, if you put MainBossRemote into a pool that contains a high-traffic process, the performance of MainBossRemote will suffer—the high-traffic process will monopolize allotted processing time.

Perhaps the ideal is to put MainBossRemote into an existing pool whose other members only have a modest amount of traffic.

.NET VERSION: When you create an application pool, you specify which .NET version it uses. All applications within the pool must use the same .NET version. Thus, you must put MainBossRemote into a pool that uses .NET 4 (specifically .NET Framework v4.0.30319). Your site may have other ASP.NET applications which use different versions of .NET (e.g. .NET framework v2.0.50727); you cannot put MainBossRemote into such a pool. Furthermore, you should not change the .NET version of any existing pools, since any applications within those pools will stop working.

Application Pool Identity: Each application pool must have an *identity*. This corresponds to a login name that will be used to run all the applications in the application pool. The login name must have sufficient permissions to run all the applications in the pool. In particular, the identity login name for the pool that contains MainBossRemote must have all the permissions required by MainBoss.

Due to a problem in SQL Server, the pool containing MainBossRemote must run under the **NetworkService** identity. (For more information about this problem, see <http://support.microsoft.com/default.aspx/kb/2002980>.) The **NetworkService** identity corresponds to the login name **NT AUTHORITY\NETWORK SERVICE**, which is a name automatically built into Windows. If you do not have any existing application pools that run under this identity, you must create a new pool that does. Otherwise, you can add MainBossRemote to any existing pool that has the **NetworkService** identity.

Important: Whatever application pool you use for the web site, we recommend that it should run in the *Integrated* managed pipeline mode. This ensures appropriate authentication security. However, as discussed in *Security Considerations on page 82*, some cell phone and PDA services do not support integrated authentication, so you may have to choose a different authentication scheme.

To work with application pools, you use the IIS manager. Start the manager on the computer where you will run the web server. (See *Initial Set-Up on page 82* of this guide for a reference on how to start the IIS manager.)

If you decide to create a new application pool for MainBossRemote, you must create the pool:

1. In the left-hand panel of the IIS manager, expand the entry labeled with the name of the computer.
2. Right-click on **Application Pools**. In the resulting menu, click **Add Application Pool**.
3. In the resulting window, enter a name for the pool (e.g. MainBoss). The .NET Framework version should be the highest available and the managed pipeline mode should be *Integrated* (or *Classical* if you make that security choice). When you click **OK**, the pool will be created, using default settings.
4. The new pool is automatically given a default identity. Typically, this is either **NetworkService** or **ApplicationPoolIdentity**. If the default identity is not

NetworkService, you must change the pool's identity to **NetworkService** by following these steps:

- Right-click on the name of the pool in the list of application pools.
- In the resulting menu, click **Advanced Settings**.
- In the resulting window, click the entry for **Identity** (under **Process Model**).
- Click the "...” button on the right-hand side of the field.
- In the resulting window, click **Built-in Account**, drop the arrow, and select **NetworkService** from the list.
- Keep clicking **OK** until you get back to the IIS manager.

Giving Folder Permissions to Network Service or the Application Pool Identity

Whether you choose to run under **NetworkService** or an application pool identity, you must make sure that the identity's login name has permission to read/write the folder that contains MainBossRemote files. For example, suppose you installed the files in

C:\inetpub\wwwroot\MainBossRemote

Then you must give the identity permissions on this folder. To do this, follow these steps:

1. Use Windows Explorer to locate the folder that contains the MainBossRemote files.
2. Right-click on the folder name; in the resulting menu, click **Properties**.
3. In the **Security** tab of the resulting window, click the **Edit** button.
4. In the resulting window, click **Add**.
5. In the resulting window, under "Enter the object names to select", enter `Network Service` (with a space between the words) or else the application pool identity.
6. Click **Check Names** to have Windows verify the specified name.
7. Click **OK** to return to the previous window.
8. With `NETWORK SERVICE` selected, click "Full control" in the list of permissions.
9. Keep clicking **OK** until you return to Windows Explorer.

Giving SQL Server Permissions to Network Service or the Application Pool Identity

In order for the appropriate identity to access the MainBoss database, it must be given appropriate permissions within SQL Server. To do so, follow these steps:

1. Start SQL Server Management Studio (or Management Studio Express). Specify the instance of SQL Server that holds the MainBoss database.

2. In the left hand column of Management Studio, expand the entry for **Security**.
3. Right-click on **Logins**, then click **New Login**.
4. In the resulting window, click **General** in the left hand column.
5. In the right hand part of the window, click **Search**.
6. In the resulting window, under “Enter the object names to select”, enter `Network Service` (with a space between the words) or else the application pool identity.
7. Click **Check Names** to have Windows verify the specified name.
8. Click **OK** to return to the previous window. You should see an appropriate identity filled into the “Login name” field.
9. In the left hand column of the window, click **User Mapping**.
10. In the right hand part of the window, checkmark the checkbox associated with the **MainBoss** database.
11. Under “Database role membership”, checkmark the checkbox associated with **MainBoss**. (The “public” checkbox should be checkmarked automatically.)
12. Click **OK** to return to Management Studio, then exit Management Studio.

Web Sites vs. Applications

The next decision to make is whether you want to implement **MainBossRemote** using a separate web site or an application within an existing web site.

- A separate web site has its own unique IP address and/or port number on the server computer.
- An application uses the same IP address and port number as an existing web site on the server computer. (Loosely speaking, an application is a type of *virtual directory*.)

If you already have a web site on the server computer, we recommend that you implement **MainBossRemote** as an application under that web site. The only reason to give **MainBossRemote** its own separate web site is if the server computer doesn't have any existing web sites, or if there is an incompatibility between the needs of **MainBossRemote** and the configuration of the existing sites.

Adding and Configuring an Application

This section describes what to do if you decide to implement **MainBossRemote** as an application under an existing web site.

As noted in a previous section, you should have copied the MainBossRemote files to a subfolder under the folder used by the IIS web service. If you have not done so, do so now.

Start the IIS manager. In the left-hand panel of the IIS manager, expand the entry for the server computer, then click on **Sites**. Expand the entry for sites until you see the name of the web site under which you will put MainBossRemote.

In order to add MainBossRemote to this web site as an application, **you must stop the web site** (i.e. shut down the web site temporarily). To stop the web site, click on its entry in the left-hand panel of the IIS manager, then click **Stop** in the far right-hand panel.

Once you've stopped the web site, right-click on the web site's entry in the left-hand panel. In the resulting menu, click **Add Application**. This opens a window where you can specify information on MainBossRemote.

- In "**Alias**", specify a name for the application. This is simply a name that will be displayed in the IIS manager to refer to this application; it can be any name that isn't already in use.
- Click the **Select** button associated with the "**Application pool**" field and specify the name of the application pool you have chosen for MainBossRemote—either an existing pool or one you created expressly for MainBossRemote.
- In "**Physical Path**", specify the folder that contains the MainBossRemote files (e.g. `C:\inetpub\wwwroot\MainBossRemote`).
- Click **OK** to close the window.

Once you have configured the web site, you can restart the web site. In the left-hand panel, click the entry for the web site that contains the MainBossRemote application. Then, in the far right-hand panel, click **Start**.

Adding and Configuring a Web Site

This section describes what to do if you decide to implement MainBossRemote as a separate web site.

As noted in a previous section, you should have copied the MainBossRemote files to a subfolder under the folder used by the IIS web service. If you have not done so, do so now.

Start the IIS manager. In the left-hand panel of the IIS manager, expand the entry for the server computer, then click on **Sites**. In the far right-hand panel, click **Add Web Site**. This opens a window where you can specify information on MainBossRemote.

- Click the **Select** button associated with the "**Application pool**" field and specify the name of the application pool you have chosen for MainBossRemote—either an existing pool or one you created expressly for MainBossRemote.

- In “**Physical Path**”, specify the folder that contains the MainBossRemote files (e.g. C:\inetpub\wwwroot\MainBossRemote).
- In “**Host Name**”, enter the name through which users will access your MainBossRemote site.
- In “**Site Name**”, enter MainBossRemote (or some other suitable name). This name will be used in the URL for accessing the MainBossRemote services. Specifically, users will access MainBossRemote using the URL

<http://HOSTNAME/SITENAME>

Therefore if “**Host Name**” is ourcomputer.ourdomain.com and “**Site Name**” is MainBossRemote, users will access the software with the URL

<http://ourcomputer.ourdomain.com/MainBossRemote>

- In “**Binding**”, specify the appropriate information (e.g. the port number the web site should use). The default port number is 80, and we strongly recommend that you use this default—anything else will make the URL more complicated, since the port number will have to be specified explicitly. (Also, some cell phone services do not support connections to non-standard port numbers.)

Note that if you’re using SSL or TLS security (as discussed in *Security Considerations on page 82*), you specify https as the binding type and then specify an SSL certificate using the drop-down list.

- Click **OK** to close the window.

Once you have configured the web site, you can start it. In the left-hand panel, click the entry for the web site. Then, in the far right-hand panel, click **Start**.

Authentication Settings

Whether MainBossRemote is a separate web site or an application within another web site, you must set its authentication settings (i.e. how the software determines who is or isn’t an authorized user).

In the left-hand panel of the IIS manager, expand **Sites** and click on the name of the MainBossRemote web site or application.

In the middle panel of the IIS manager, the IIS section has an entry for *IIS Authentication*. Double-click this entry to open a window where you can specify authentication settings. We recommend the following:

- Enable Anonymous Authentication
- Disable ASP.NET Impersonation (this is the default)
- The Forms Authentication setting can be either enabled or disabled; it doesn’t matter to MainBoss

- Enable Windows Authentication

Application Settings

Whether MainBossRemote is a separate web site or an application within another web site, you must set its application settings. These specify which database the software should access.

In the left-hand panel of the IIS manager, click on the name of the MainBossRemote site. In the middle panel of the IIS manager, the ASP.NET section has an entry for *Application Settings*. Double-click this entry to open a window where you can specify the settings.

You will see there are settings for `dbserver` and `dbname`. Initially, these have stand-in names that should be replaced with the real names used by your site.

Click on the entry for `dbserver`. In the far right-hand panel, click **Edit**. In the resulting window, set “**Value**” to the name of the SQL Server that maintains the MainBoss database. This name will have one of the following two forms:

COMPUTER\INSTANCE

The name of the computer where the SQL Server resides and the name of the particular SQL Server instance that maintains the MainBoss database.

COMPUTER

Just the name of the computer where the SQL Server resides. This indicates that the MainBoss database is maintained by an unnamed instance of SQL Server.

Click **OK** once you have entered the appropriate “**Value**”.

Now click on the entry for `dbname`. In the far right-hand panel of IIS manager, click **Edit**. In the resulting window, set “**Value**” to the name of the MainBoss database as maintained by the server specified with the `dbserver` setting. (Note that this is the database name, not the organization name that might be specified by a particular user.) Click **OK** once you have entered the appropriate “**Value**”.

When you’re done, the application settings window should look something like this:



Application Settings

Use this feature to store name and value pairs that managed code applications can use at runtime.

Group by: No Grouping		
Name	Value	Entry Type
dbname	OurMainBossDatabase	Local
dbserver	OURCOMPUTER\SQLSERVER	Local

Important: After setting this information, you may have to stop and start the application pool in order for the settings to take effect. In IIS manager, right-click on the entry for the application pool, then click **Stop**. Wait a moment, then right-click and click on **Start**.

Software Initialization

The first time someone connects with the MainBossRemote web site, the software must compile itself and perform various set-up processes. This can take a long time and use a lot of computer memory. Therefore, you should make the first connection at a time when the increased processor and memory load will not affect important work on the computer.

Once the software has set itself up, it doesn't have to go through the process again unless something significant changes in your configuration, e.g. you install a new version of the web server, SQL Server, or MainBoss.

Accessing SQL Server on a Different Computer

As noted previously, configuring MainBossRemote is easier if the web server is on the same computer as the SQL Server that manages MainBoss. If the two are on different computers, more configuration is required.

1. Create a domain account that will be used to login to the SQL Server. For the sake of illustration, we will call this account `IIS_MAINBOSS`. Also Give the account a suitable password. (Be sure to remember this password—you may need it in future.)
2. Give `IIS_MAINBOSS` Domain User permissions.
3. On the SQL Server computer, start SQL Server Management Studio.
4. Using Management Studio, configure the SQL server's logins to allow `IIS_MAINBOSS` to login. (Note that you do *not* need to add `IIS_MAINBOSS` to MainBoss's own list of authorized users, given in **Administration | Users**.)
5. Using Management Studio, add `IIS_MAINBOSS` to the list of accepted users of the MainBoss database.
6. Using Management Studio, give `IIS_MAINBOSS` the `MainBoss` security role.
7. Start the IIS manager. In the left-hand panel, expand **Sites** and click on the MainBossRemote web site. In the middle panel, IIS section, double-click *Authentication*.

In the resulting window, click *ASP.NET Impersonation*, then click **Edit** (in the far right-hand panel).

In the resulting window, click **Specific user**. Enter the `IIS_MAINBOSS` login name in the accompanying field, using the format `DOMAIN\IIS_MAINBOSS`, where `DOMAIN` is the

name of the domain where IIS_MAINBOSS is defined. You will be asked to enter the login name's password.

Note: The password for this login name will be stored in plain text (not encrypted or hidden) in the web.config file. For information on how to fix this, see <http://support.microsoft.com/default.aspx?scid=kb;EN-US;329290>.

8. On 64-bit versions of Windows, give DOMAIN\IIS_MAINBOSS read/write file system privileges to the directory

%SystemRoot%\Microsoft.NET\Framework64\versionNumber\Temporary ASP.NET Files

On 32-bit versions of Windows, do this for

%SystemRoot%\Microsoft.NET\Framework\versionNumber\Temporary ASP.NET Files

Note that %SystemRoot% is typically C:\Windows. If you're in doubt, open a command prompt window and enter the command

```
echo %SystemRoot%
```

This will display the pathname associated with %SystemRoot%.

Integrating MainBoss Remote with MainBoss Service

If you are using the MainBoss Service module, you should adjust its configuration so that the service knows about MainBoss Remote. To do this, follow these steps:

1. Login under a user name with Windows Administrator and MainBoss Administration permissions.
2. Start MainBoss.
3. Go to **Administration | MainBoss Service**.
4. If MainBoss Service is running, drop the arrow on **Start Service** and click **Stop Service**.
5. Go to **Administration | MainBoss Service | Configuration**.
6. Click the single record in the table viewer, then click **Edit**.
7. In the resulting window, go to the **Outgoing Mail** section.
8. Set the field "**MainBoss Remote URL for E-mail notifications**" to the URL for your MainBoss Remote web site, e.g. <http://ourcompany.com/MainBossRemote>.
9. Click **Save and Close**.
10. Go to **Administration | MainBoss Service**.
11. Click **Start Service**.

If you do not do the above, messages sent out by MainBoss Service may contain URLs that do not work.

MainBossRemote Troubleshooting

This section lists a number of error messages you might see when trying to use MainBossRemote, plus ways to correct the problems.

```
There was a problem validating access to the database XXX on server
YYY. The database-principal 'dbo' does not exist or user is not a
member. Failed SQL command is: declare @result int; exec @result =
sp_getapplock 'MainBossSession', 'shared', 'session', 0, 'dbo';
select @result
```

This indicates you did not give permissions to the login name for the identity of the application pool where MainBossRemote runs. Follow the instructions in *Application Pools on page 84*.

```
An error occurred while processing your request. Database server
'ServerMainBossDatabaseIsOn' was not found or was not accessible.
```

This indicates that you did not change the default dbserver application setting. See *Application Settings on page 90* of this guide.

```
Could not load file or assembly 'System.Web.Mvc' or one of its
dependencies. Access is denied.
```

This indicates that you did not give DOMAIN\IIS_MAINBOSS read/write file system privileges to the directory containing temporary ASP.NET files. See the previous section of this guide for more information.

Note: Whenever you encounter diagnostic messages, you can usually find useful information by typing them into Google and searching for information.

The Windows Firewall: In our experience, many of the difficulties that arise when configuring MainBossRemote are due to firewall problems. If the Windows firewall is not adjusted to allow various information to pass through, MainBossRemote will not work. Firewall problems are especially difficult to diagnose because they generate no error messages or log entries; you just don't see anything happening.

Cookie Usage

Cookies used by MainBossRemote are stored as subkeys under the cookie key MainBossRemote. The following subkeys are defined:

```
requestorEmail
```

The email address that a user last entered, provided that the address was recognized as a valid requestor in MainBoss.

INDEX

- .NET framework, 2
- abbreviations, 44
- active directory, 65
- add organizations, 50
- administration, 35
 - backups, 39, 55
 - database history, 39, 55
 - licenses, 10, 12
 - MainBoss Service, 92
 - configuration, 25, 92
 - security roles, 17
 - users, 4, 15, 16, 19
- administration backups, 43
- administrator privileges, 4
- application pools, 84
- applications, 87
- ASP.NET, 80

- backups, 38, 51, 54
 - database, 41
 - restoring, 41
- breakin, 51
- browser
 - SQL Server, 67

- ClickOnce deployment, 5
- command files, 44
- command line interface, 44
- command line options, 36
- CompactBrowsers, 38
- control panel, 70
- CultureInfo, 37
- currency, 8

- database, 2
 - backup, 41
- database history, 55

- database name, 43
- database server, 43
- desktop icon, 38
- DNS name, 65
- domain, 2
- domains, 17

- evaluate security as, 19
- Excel, 47
- exporting data, 46
- expressmaint, 56, 59

- file-sharing, 61
- firewall, 61, 68, 69, 70

- hardware requirements
 - MainBoss, 2
 - SQL Server, 53

- identity, 85
- IIS, 80
- IIS 6, 80
- IIS 7, 80
- IMAP4, 76
- importing data, 48
- installation
 - MainBoss software, 7
 - manual, 5
- instance, 72
- instances, 53
- international support, 37
- Internet security, 82

- language support, 37
- license keys, 9
 - MainBossRemote, 82
- Linux, 2
- local users, 17

- MainBoss manages SQL Security, 72
- MainBoss Remote, 28
- MainBoss Service, 22, 78, 92
 - configuring, 25
 - edit, 25
 - event log, 31, 78
 - installing, 22
- MainBossRemote, 80
 - application settings, 90
 - authentication settings, 89
 - URL, 89
- maintenance
 - SQL Server, 58
- maintenance organizations
 - creating, 7
 - multiple, 34
- maintenance plans, 54
- mbutility, 44
 - adding organizations, 50
 - AddOrganization, 50
 - Backup, 51
 - breakin, 51
 - built-in schemas, 45
 - Excel, 47
 - export, 46
 - GenerateImportSchema, 45
 - Help, 45
 - import, 48
 - ListImportSchemas, 45
 - ListOrganizations, 45
 - MainBoss organizations, 45
- Microsoft Excel, 75
- Microsoft Report Viewer, 3
- modes
 - administration, 35
 - MainBoss Requests, 35
 - start, 35
 - view sessions, 36
- named pipes, 67
- NetworkService, 85
- organization name, 43
- ping, 62
- POP3, 76
- privileges, 4
- read permission, 7
- remote registry, 32
- report viewer, 2
- Report Viewer, 3
- requests
 - mode, 35
- reset to user security, 19
- restoring, 55
- restoring from backup, 41
- roles, 14
- Samba, 2
- schemas, 45
- scopes, 13
- script, 44
- security, 82
- security roles, 14, 17
 - testing, 19
- security settings, 13
- shell script, 44
- SQL, 2
- SQL Express, 3, 56
- SQL Security, 72
- SQL Server, 54, 60
 - browser, 67
 - instances, 53
 - maintenance, 58
- start modes, 35
- system requirements
 - MainBossRemote, 80
- troubleshooting, 60
- trusted domains, 13
- upgrading MainBoss, 34
- users, 15

deleting, 17
view sessions, 36
virtual directory, 87

Web Access module, 80
Web Requests module, 80
web sites, 87