AMX®

Quick Start Guide

RMS

Resource Management Suite 3.1

Software

AMX Limited Warranty and Disclaimer

AMX Corporation warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase from AMX Corporation, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components that are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX Lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX Lighting products are under warranty. AMX Corporation does guarantee the
  control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality cannot be guaranteed due to the random combinations of dimmers, lamps and ballasts or transformers.
- Unless otherwise specified, OEM and custom products are warranted for a period of one (1) year.
- AMX Software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.

This warranty extends only to products purchased directly from AMX Corporation or an Authorized AMX Dealer.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX Corporation is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX Corporation is not liable for any claim made by a third party or by an AMX Dealer for a third party.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of
liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX Corporation or an authorized representative of AMX Corporation has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full
determination of rights.

EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX CORPORATION MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX CORPORATION EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY.

Software License and Warranty Agreement

LICENSE GRANT.
AMX grants to Licensee the non-exclusive right to use the AMX Software in the manner described in this License. The AMX Software is licensed, not sold. The AMX Software consists of generally available programming and development software, product documentation, sample applications, tools and utilities, and miscellaneous technical information. Please refer to the README.TXT file on the compact disc or download for further information regarding the components of the AMX Software. The AMX Software is subject to restrictions on distribution described in this License Agreement. YOU MAY NOT LICENSE, RENT, OR LEASE THE AMX SOFTWARE. You may not reverse engineer, decompile, or disassemble the AMX Software.

INTELLECTUAL PROPERTY.
The AMX Software is owned by AMX and is protected by United States copyright laws, patent laws, international treaty provisions, and/or state of Texas trade secret laws. Licensee may make copies of the AMX Software solely for backup or archival purposes. Licensee may not copy the written materials accompanying the AMX Software.

TERMINATION. AMX RESERVES THE RIGHT, IN ITS SOLE DISCRETION, TO TERMINATE THIS LICENSE FOR ANY REASON AND UPON WRITTEN NOTICE TO LICENSEE.
In the event that AMX terminates this License, the Licensee shall return or destroy all originals and copies of the AMX Software to AMX and certify in writing that all originals and copies have been returned or destroyed.

PRE-RELEASE CODE.
Portions of the AMX Software may, from time to time, as identified in the AMX Software, include PRE-RELEASE CODE and such code may not be at the level of performance, compatibility and functionality of the final code. The PRE-RELEASE CODE may not operate correctly and may be substantially modified prior to final release or certain features may not be generally released. AMX is not obligated to make or support any PRE-RELEASE CODE. ALL PRE-RELEASE CODE IS PROVIDED "AS IS" WITH NO WARRANTIES.

LIMITED WARRANTY.
AMX warrants that the AMX Software will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt. AMX DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE AMX SOFTWARE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. Any supplements or updates to the AMX SOFTWARE, including without limitation, any (if any) service packs or hot fixes provided to you after the expiration of the ninety (90) day Limited Warranty period are not covered by any warranty or condition, express, implied or statutory.

LICENSEE REMEDIES.
AMX's entire liability and your exclusive remedy shall be repair or replacement of the AMX Software that does not meet AMX's Limited Warranty and which is returned to AMX. This Limited Warranty is void if failure of the AMX Software has resulted from accident, abuse, or misapplication. Any replacement AMX Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, these remedies may not available.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL AMX BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS AMX SOFTWARE, EVEN IF AMX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

U.S. GOVERNMENT RESTRICTED RIGHTS. The AMX Software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.

This Agreement replaces and supercedes all previous AMX Software License Agreements and is governed by the laws of the State of Texas, and all disputes will be resolved in the courts in Collin County, Texas, USA. Should you have any questions concerning this Agreement, or if you desire to contact AMX for any reason, please write: **AMX Corporation, 3000 Research Drive, Richardson, TX 75082.**

Table of Contents

Installation

The Resource Management Suite® provides enterprise grade scalable solutions for administrators and managers of networked audio visual systems which include features not available through any other control system provider. A powerful web console interface allows users to monitor, schedule, and view reports on their systems and devices.

RMS 3.1 supports key markets: Corporate, Education, Houses of Worship, Museums, Broadcasting, Government, and Residential. These applications contain a unique appearance and terminology designed for each specific market.

The RMS Quick Start Guide will assist you in identifying what information you need to make installing or upgrading this software as seamless as possible.

Upgrading to RMS 3.1 from 3.0

- RMS 3.0 licenses work with RMS 3.1
- The Database Wizard automatically detects an existing RMS 3.0 database and performs the necessary updates for RMS 3.1

Upgrading to RMS 3.1 from RMS 2.2 or earlier

There are changes in the approach to licensing and supported databases.

- Contact AMX Global Customer Service to obtain new RMS 3.1 licenses for both Asset and Scheduling functionality. To obtain an RMS License, please contact AMX at **800-222-0193**, by email at **service@amx.com,** or contact your AMX dealer. Existing licenses will migrate in the following manner:

  1 MeetingManager license becomes 1 Asset license and 1 Scheduling license.

  1 AssetManager license becomes 1 Asset license.
- The Database Wizard automatically migrates the database from a previous RMS database into one of the RMS 3.1 supported database platforms; however, you will need to have one of the RMS 3.1 supported database platforms installed prior to starting the RMS 3.1 installation process.

Knowing these points, you can now proceed to the regular installation process. Use the *Resource Management Suite 3.1 Installation Checklist* section on page 3 to aid your installation.

Resource Management Suite 3.1 Installation Checklist

Hardware System Requirements

Hardware System Requirements		
Does your server hardware meet the minimum requirements for RMS?		**Yes/No**
Processor	Intel Pentium IV 2.0 GHz (x86)	
Memory	512 MB	
Display	1024x768 resolution	
Hard Disk	500 MB available space for RMS application files and database	

Yes to all	Please continue to the next step.
No to any	You must obtain a server that meets these minimum requirements to install RMS.

Server Operating System

Server Operating System	
Do you have a compatible server operating system installed?	**Yes/No**
Windows 2000 Server	
Windows 2003 Server	

Yes	Please continue to the next step.
No	You must obtain a compatible server operating system to install RMS.

Does your server operating system have the latest service packs installed?	**Yes/No**
Windows 2000 Server - Service Pack 4 (current as of 10/02/2006)	
Windows 2003 Server - Service Pack 1 (current as of 10/02/2006)	

Yes	Please continue to the next step.
No	You must obtain and install the latest operating system service packs to install RMS.

Server Operating System (Cont.)	
Does your server operating system have Internet Information Services installed?	**Yes/No**
Windows 2000 Server - Internet Information Services (IIS) 5.0	
Windows 2003 Server - Internet Information Services (IIS) 6.0	

Yes	Please continue to the next step.
No	You must install IIS on your server for RMS to serve web pages. While this component is optional for the Windows Server operating system, it is required by the RMS application. The installer will not continue if this component is not detected.

Do you have an administrative logon account to the server where RMS will be installed?	
Yes	Please continue to the next step.
No	You must obtain such an account, and logon to the server with a user account that has administrative access to the server. RMS is a system level application and requires administrative access to install and configure the RMS services and security settings.

Additional Software Dependencies

Additional Software Dependencies	
Does your server have the Microsoft .NET Framework 2.0 installed?	
Yes	Please continue to the next step.
No	You must obtain and install the Microsoft .NET Framework 2.0 before installing RMS. The installer will not continue if this component is not detected.

Does your server have Adobe Acrobat Reader installed?	
Yes	Please continue to the next step.
No	You must obtain and install Adobe Acrobat Reader to be able to display the RMS help files.

Database Platform

Database Platform	
Do you have a compatible database platform where the RMS database can be installed?	**Yes/No**
Microsoft SQL Server 2000	
Microsoft SQL Server 2005 - Standard Edition	
Microsoft SQL Server 2005 - Enterprise Edition	
Microsoft SQL Server 2005 - Express Edition	

Yes	Please continue to the next step.
No	You must obtain access to or install a compatible database platform for the RMS database. Microsoft SQL Server 2005 Express Edition is a no cost solution for small to medium sized RMS installations. If upgrading from RMS 2.x using an Access database, you can download and install SQL Server 2005 Express Edition for use with RMS 3.0. The RMS 3.0 installation will migrate your existing data from the existing RMS 2.x database to the new RMS 3.0 database. Microsoft SQL Server 2005 Express Edition can be downloaded using this link: `http://msdn.microsoft.com/vstudio/express/sql/download/`
Note: If installing Microsoft SQL Server 2005 Express Edition, please review *Appendix F: Installation Procedure for SQL Server 2005 Express Edition* section on page 347 of the *RMS Administrator's Guide*. Here you will find the specific information your will need for installation and configuration for Microsoft SQL Server 2005 Express Edition.	

Database Access

<table>
<tr><th colspan="4">Database Access</th></tr>
<tr><td><b>Database Server</b></td><td colspan="3"></td></tr>
<tr><td rowspan="3"><b>Using Windows Authentication?</b></td><td colspan="3"><i>Yes</i></td></tr>
<tr><td rowspan="2"><i>No</i></td><td><b>Username:</b></td><td></td></tr>
<tr><td><b>Password:</b></td><td></td></tr>
<tr><td><b>Database Name (Catalog)</b></td><td colspan="3"><b>(Default = RMS)</b></td></tr>
</table>

Database Server	This is the server name or path to the database server. If using Microsoft SQL 2005 Express Edition, this field would also contain the database instance name and be formatted like "server_name\instance_name"
Windows Authentication	If you are using Windows Authentication to access the database server, then no username or password is needed.
Username	If you are not using Windows Authentication, then a username is needed to logon to the database server.
Password	If you are not using Windows Authentication, then a password is needed to logon to the database server.
Database Name	This is the database name to create and use for the RMS system. By default this is named 'RMS'. Database name is also known as "Catalog".

Scheduling System

Scheduling System
RMS supports both an internal scheduling system and interfaces to the following external scheduling systems:
Microsoft Exchange 2000/2003/2007 Server
Microsoft Outlook 2000/2003/2007 (stand-alone mode)
Novell GroupWise 6.0/6.5
Lotus Notes R5/R6

Please complete the following information:		
Scheduling System	*Internal Scheduling*	
	External Scheduling	Microsoft Exchange
		Microsoft Outlook
		Novell GroupWise
		Lotus Notes
Note: If interfacing with an External Scheduling System, please review the corresponding section for your scheduling system under the *Scheduling System Plug-ins* section on page 267 of the *RMS Administrator's Guide*. Here you will find the specific information your will need for installation and configuration with the external scheduling system.		

Internet Information Services - Virtual Directory

Internet Information Services - Virtual Directory	
RMS provides a web user interface for the administration and management of the application. The RMS installation will create a new virtual directory in the Windows Internet Information Services web services. During the installation you can specify the virtual directory name used to access RMS. This virtual directory name is used as part of the path in the URL to access the RMS web application. `http://server_name/virtual_directory`	
Please complete the following information:	
Virtual Directory Name	**(Default = RMS)**

RMS Licensing

RMS Licensing	
RMS can operate with limited functionality in STANDARD edition. However, if you want the full capabilities of RMS you must purchase the PREMIUM edition from AMX. Upon purchasing PREMIUM edition, you will receive a server serial number. This serial number will be needed during the installation to license the RMS server.	
Please complete the following information:	
Server Serial Number	

Once the Premium edition of the RMS server is licensed, you must also enter client licenses for the number of rooms you wish to use with RMS for either Asset management, Scheduling, or both.	
Please complete the following information:	
Client Certificate ID	**Authentication Key**

RMS TCP/IP Communications

RMS TCP/IP Communications	
RMS uses TCP/IP communications between the RMS server and the remote NetLinx systems.	
Please complete the following information:	
TCP/IP Server Port Number	**(Default = 3839. This is an IANA registered port number for RMS)**
Does your server have a firewall that will block TCP/IP communication for this port?	
Yes	You will need to create a PINHOLE or exception for TCP/IP communications on the specified TCP/IP port for RMS communications.
No	Please continue to the next step.

Does your network router restrict or block traffic on this TCP/IP port?	
Yes	You will need to create a PINHOLE or exception for TCP/IP communications on the specified TCP/IP port for RMS communications.
No	Please continue to the next step.

RMS Security Settings

<table>
<tr><th colspan="6">RMS Security Settings</th></tr>
<tr><td colspan="6">RMS provides a flexible user account management system.</td></tr>
<tr><td colspan="6">Please complete the following information:</td></tr>
<tr><td rowspan="4"><b>Enable User Account Management</b></td><td colspan="5"><i>No</i></td></tr>
<tr><td rowspan="3"><i>Yes</i></td><td><b>Allow Anonymous Access:</b></td><td><i>Yes</i></td><td colspan="2"><i>No</i></td></tr>
<tr><td><b>Default Admin Username:</b></td><td colspan="3">(Default = Admin)</td></tr>
<tr><td><b>Default Admin Password:</b></td><td colspan="3"></td></tr>
</table>

Enable User Account Management If you would like any user that can access the RMS web pages to have full access to all RMS features and functions, then disable user account management.

If you would like restricted user logon RMS web pages where you can manage individual user's access permissions, then enable user account management.

Allow Anonymous Access If User Account Management is enabled, then you will also have the option to allow or disallow anonymous access to the RMS web pages. If anonymous access is allowed, users will be able to view the scheduling pages in RMS without having to logon with a user account.

Default Admin Username If User Account Management is enabled, then you must provide a username for the default administrator account.

Default Admin Password If User Account Management is enabled, then you must provide a password for the default administrator account.

Note: RMS also supports Windows Authentication for authenticating users in the RMS web pages. RMS will automatically detect if your website is configured for Windows Authentication. User account management should be enabled and anonymous access should be disallowed when using Windows Authentication. To learn more, or to configure your system for Windows Authentication, please review the *Windows Authentication* section on page 21 of the *RMS Administrator's Guide*.

SMTP Email Server

SMTP Email Server					
RMS supports Simple Mail Transport Protocol (SMTP) email for all outbound email notifications. In order to receive email notifications, the following SMTP information will be needed.					
Please complete the following information:					
Allow SMTP Messaging	*No*				
	Yes	**SMTP Server Address**			
		SMTP Server Port	**(Default = 25)**		
		SMTP Server Requires Authentication	*No*		
			Yes	**Username:**	
				Password	
		SMTP Email Address			
		Friendly Email Name			
		Reply-To Email Address			

SNPP Paging Provider

SNPP Paging Provider			
RMS support Simple Network Paging Protocol (SNPP) outbound electronic alpha/text paging notifications. In order to receive SNPP text pages the following SNPP information will be needed.			
Please complete the following information:			
Enable SNPP Paging	*No*		
	Yes	**SNPP Provider**	Select from the pre-defined list in the RMS Configuration Wizard or add your own SNPP provider information

SNMP Management Server

SNMP Management Server			
RMS supports the Simple Network Management Protocol for extending RMS information to your SNMP management console.			
Please complete the following information:			
Enable SNMP Services	*No*		
	Yes	**SNMP Agent Port**	**(Default = 161)**
		SNMP Community	
		SNMP Trap Community	
		SNMP Trap Recipients	

RMS Logging Options

RMS Logging Options				
RMS supports the logging of information to an internal log in the database and to the Windows Event log.				
Please complete the following information:				
Enable Logging to the Internal Database Log	*No*			
	Yes	**Maximum Number of Log Entries To Retain**	**(Default = 1000)**	
		Delete Log Entries After (Days)	**(Default = 90)**	
Enable Logging To the Windows Event Log	*No*			
	Yes	**Log Informational Messages**	*Yes*	*No*
		Log Warning Messages	*Yes*	*No*
		Log Error Messages	*Yes*	*No*

Maximum Log Entries

If Internal Logging is enabled, you can specify the maximum number of log records to retain for log reporting purposes. The RMS services will automatically purge the oldest log records to maintain a manageable database size.

Delete Log Entries After

If Internal Logging is enabled, you can specify the number of days to retain historical data for log reporting purposes. The RMS services will automatically purge data records that are older than the specified number of days in order to maintain a manageable database size.

SYSLOG Messaging

SYSLOG Messaging			
RMS supports broadcasting SYSLOG messages across the network to a SYSLOG listening server.			
Please complete the following information:			
Enable SYSLOG Messaging	*No*		
	Yes	**SYSLOG Server Address**	
		SYSLOG Server Port	**(Default = 514)**
		SYSLOG Facility ID	Select from listing in RMS Configuration Wizard

RMS Reporting Options

RMS Reporting Options			
RMS can provide historical and statistical reports based on system-collected data using the following configuration settings.			
Please complete the following information:			
Enable Reporting	*No*		
	Yes	**Delete Report Entries After (Days)**	**(Default = 90)**

Delete Report Entries After If Reporting is enabled, you can specify the number of days to retain historical data for reporting purposes. The RMS services will automatically purge data records that are older than the specified number of days in order to maintain a manageable database size.

Configuration Wizard

Welcome

The RMS application suite Configuration Wizard is used to guide you through the initial setup and configuration of your RMS application suite server. After installing an RMS application you must complete the Configuration Wizard to register and enable your server. Additionally, you may return to the Configuration Wizard at any time to modify system settings or diagnose system related problems.

Click **Next** to begin the RMS application suite Configuration Wizard.

Appointment Management/Scheduling System

The RMS application suite server software can manage appointments using an Internal or External scheduler such as Microsoft Exchange, Lotus Notes, or Novell GroupWise. Depending on your configuration, additional configuration steps need to be taken. This step helps the configuration wizard guide you through the appropriate options for your configuration.

Appointment Management/Scheduling System	
Internal Appointment Management/Schedule System	Select this option if you want to use the Appointment Management features of the RMS application suite, but do not want to connect to an external scheduling system.
External Appointment Management/Schedule System	Select this option if you want to use the Appointment Management features of the RMS application suite with an external scheduling system.

If you wish to use an existing scheduling system, please choose the *External Appointment Management/Scheduling System* option.

Otherwise, select *Internal Appointment Management/Scheduling System*.

Click **Next** to continue.

Database

The AMX RMS application suite uses a single central database for all data storage. This database can be configured in the RMS application suite Configuration Wizard.

Connection

The next step is to verify the RMS application suite database connection.

Configuration

NOTE *The Configuration screen may be skipped in the Configuration Wizard if a successful database connection is detected. You can navigate to the Configuration screen at any time by double-clicking the "Configuration" item in the navigation tree under the "Database" heading.*

The Configuration screen allows you to manually configure the database connection settings. The RMS application suite supports the following database types:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005 Standard Edition
- Microsoft SQL Server 2005 Enterprise Edition
- Microsoft SQL Server 2005 Express Edition

You need to specify the database server name/address and the database/catalog name.

Upon completion of the database configuration settings, click **Next** to proceed.

Updates

NOTE *The Updates screen may be skipped in the Configuration Wizard if a successful database connection is detected and no updates are required. You can navigate to the Updates screen at any time by double-clicking the "Updates" item in the navigation tree under the "Database" heading.*

The database update screen indicates if the existing database needs to be updated. If the database versions are mismatched, the *Update Database* button is available; click the **Update Database** button to start the database update process.

After the updates are complete, click **Next** to proceed.

Product Selection

AMX strategically focuses on meeting the needs of high-growth vertical markets. In the commercial space, this includes: Broadcasting, Education, Entertainment, Government, Healthcare, Hotels, Houses of Worship, Network Operations Centers, Presentation Facilities, and Retail. For the residential market, AMX delivers solutions for Whole Homes, Home Theater, Multi-Dwelling Units, and Private Transportation.

The RMS application suite now supports several vertical markets. Selecting one of the following determines what branch of RMS is installed as your server.

- **MeetingManager** - Presentation Facilities
- **ClassroomManager** - Education
- **ExhibitManager** - Retail and Museums
- **VenueManager** - Entertainment, Hotels, Healthcare, and Broadcasting
- **WorshipManager** - Houses of Worship
- **HomeManager** - Whole Homes, Home Theater, Multi-Dwelling Units, and Private Transportation
- **IntelligentManager** - Government

Web Services

The RMS application suite requires the use of the Microsoft Internet Information Services to host the RMS application suite web pages (ASP).

Microsoft IIS Server

This step in the Configuration Wizard ensures that the IIS web server is running.

If the IIS web server is not running, click **Start IIS Web Server**.

Click **Next** to continue.

Virtual Directory

The RMS application suite user interfaces are web pages designed to run in Windows IIS Server. This configuration step guides you through the proper setup of the IIS Virtual Directory.

Web Virtual Directory Configuration (IIS)	
Virtual Directory Alias Name	Enter the name of the virtual directory you would like to use for the RMS application suite web pages. The configuration wizard will make the appropriate changes to your IIS configuration when you click Create Virtual Web Directory. These include creating a virtual directory, creating an ASP application for this directory, and setting the "Enable Parent Paths" option to true.

1. Enter the name of the virtual directory used for the RMS application suite web pages, in the *Virtual Directory Alias Name* field.
2. Click **Create Virtual Web Directory**, the configuration wizard will make the appropriate changes to your IIS configuration.
3. Click **Next** to proceed.

Services

The RMS application suite server software is comprised of a collection of Windows NT Services. NT Services allow the program to load automatically on computer boot up and to run unattended without a user being logged onto the computer. NT Services must be registered with the Windows operating system. The RMS application suite services are compatible with Microsoft Windows 2000 and newer operating systems. You must register all services before proceeding to the next step.

Service Registration	
AMX RMS Server	This service is the primary RMS application suite service. This service loads automatically upon Windows boot up.
AMX RMS Communications Manager	This service handles all outbound communication for the RMS application suite system notifications and the following communication methods: • SMTP Email Messages • SYSLOG Messages • Windows Event Log Messages • SNPP Paging Messages • SNMP Trap Messages This service loads automatically upon Windows boot up.

Service Registration (Cont.)	
AMX RMS NetLinx Manager	This service is responsible for hosting, facilitating, and maintaining all connections and communications with the NetLinx systems. This service loads automatically upon Windows boot up.
AMX RMS Scheduling Manager	This service connects to external scheduling systems (Microsoft Exchange, Novell GroupWise, Lotus Notes, etc.) and acquires appointments for a given calendar folder for each room configured in the RMS application suite system. Upon clicking the "Register Services" button, you are prompted to choose between the system account and a local user account if you are connecting to an external scheduling system. If you are planning on integrating the room scheduling and appointment features of the AMX RMS application suite with an external messaging system you must configure this service to log on as a user or resource account that has Domain permissions to the target messaging system mailbox/calendar or local MAPI profile. This service loads automatically upon Windows boot up.

Click **Next** to continue.

Register

Initially, the RMS application suite services are not be registered. Click the **Register Services** button to start the registration process.

If the *External Appointment Management/Scheduling System* option was selected in the *Appointment Management/Scheduling System* step, the service registration prompts you to select a user account which the scheduling service will utilize for appointment access functions. This is important for some scheduling systems where specific user accounts require domain user security privileges. For example, to access a Microsoft Exchange account, the scheduling service must log on with a user account that has access to all of the desired Exchange mailboxes. If your third-party scheduling system does not require domain user permissions, you can use the *Local System account* option. Please review the documentation covering the particular RMS application suite Scheduling Plug-in that you intend to use.

After making your selection, click **Register Service** to continue.

After completing the registration process, the Configuration Wizard indicates all RMS application suite services were registered successfully.

Click **Next** to continue.

Start

After the RMS application suite services have been registered, you must start them.

Click the **Start Services** button.

As the Configuration Wizard is starting each service, a dialog indicates the startup status. Click **Cancel** to cease starting services and return to the Configuration Wizard.

Upon the successful start of the RMS application suite services, the Configuration Wizard visually indicates all services as *Running*.

Click **Next** to proceed.

NOTE

The AMX RMS Server Service is the primary service. All other services depend on this service; therefore it must always be started first and stopped last. The Windows Services manager and the RMS application suite Service Manager Utility will not allow you to stop this service until all other services have been stopped. When starting one of the other services first, the Windows Services manager and the RMS application suite Service Manager Utility will start the RMS Server service first.

Licensing

The RMS application suite requires a Server serial number, and the appropriate client licenses to provide either Asset management or Scheduling functions as desired.

Server Licenses

To obtain RMS application suite licensing, contact AMX at:

- Contact AMX Global Customer Service at 800-222-0193
- by email at service@amx.com or
- contact your AMX dealer.

Click **Next** to continue.

If you do not have a RMS application suite license key and you opted to operate in Standard mode, the Configuration Wizard indicates the key was not detected and the *Software Serial Number* reads: **Standard Edition**.

If your RMS server is behind a firewall or is otherwise unable to connect to AMX and finalize the authorization process, you can call AMX and receive a manual authorization key.

Click **Next** to continue.

Client Licenses

RMS application suite requires additional Client Licenses. Additional Client Licenses can be entered now, or at any time in the RMS application suite Configuration Wizard.

To obtain RMS application suite Client Licensing, contact AMX at:

- Contact AMX Global Customer Service at 800-222-0193
- by email at service@amx.com or
- contact your AMX dealer.

If you have a licensed RMS Premium edition with a software serial number, the Configuration Wizard displays the Software Serial Number and allows you to add or remove Client Licenses.

- To remove a client license, click on it and select **Remove**.
- Click **Add** to enter additional client licenses.

1. Enter the *Client License Certificate ID* and the *Authorization Key* in the appropriate fields.
2. Click **OK** to complete the client license entry.

If you do not wish to enter additional client licenses, click **Next** to continue.

If you do not have a RMS application suite license key installed and you opted to operate in Standard mode, the Configuration Wizard indicates the key was not detected and the *Software Serial Number* reads: **Standard Edition**.

Click **Next** to continue.

OS Permissions

Certain NTFS and registry access permissions may be required by the AMX RMS Scheduling Manager service to access resources on the RMS application suite server.

Service User

The configuration wizard automatically creates the appropriate NTFS and registry access permissions for the service user account. Below is a list of files and directories that require special permissions:

Web NTFS Permissions	
RMS application suite Registry Access	The RMS Scheduling Manager service user account must have read and write registry access permissions to the registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\AMX Corp.\RMS`

If the *External Appointment Management/Scheduling System* option was not selected on the *Appointment Management/Scheduling System* step, or the scheduling service was registered with a the Local System user account, then no permissions need to be configured.

Click **Next** to continue.

If the *External Appointment Management/Scheduling System* option was selected on the *Appointment Management/Scheduling System* step, and the scheduling service was registered with a user account other than the Local System account, then the Configuration Wizard ensures the scheduling server user account has all of the appropriate NTFS directory permissions and registry access permissions required to allow the scheduling service to interact with the system.

1. Click **Set Permissions** to begin.
2. Once the Configuration Wizard has completed setting all of the appropriate system permissions, it will indicate *Permissions Are Set*.
3. Click **Next** to continue.

Web User

NOTE

This screen may be skipped if your servers' file system is formatted as a FAT or FAT32 file system. These file systems do not support security options so this step is not required.

Certain NTFS permissions are required for the users of the web pages to access resources on the RMS application suite server. The configuration wizard automatically creates the appropriate NTFS permissions for the web users.

Below is a list of files and directories that require special permissions:

Web NTFS Permissions	
RMS application suite Dynamic Images Directory	The web users must have read and write access to the dynamic images directory.
RMS Temporary files directory	The web users must have read and write access to the temporary files directory.

1. To set the appropriate permissions, click **Set Permissions**.
2. Once the Configuration Wizard has completed setting all of the appropriate system permissions, it will indicate *Permissions Are Set*.
3. Click **Next** to continue.

System Settings

In the system settings section of the Configuration Wizard, the Configuration Wizard configures application specific setting and options.

NetLinx

The first step in the system settings section is the NetLinx Server Settings. All NetLinx systems must connect to the RMS application suite server over a TCP/IP connection. In this configuration step you can modify the IP Server Port the NetLinx systems uses to establish a connection and facilitate communication. The RMS application suite uses IP port 3839 by default.

NetLinx Server Settings	
TCP/IP Server Port	This field configures the IP port on which the RMS application suite server accepts connections from NetLinx masters. The default port is 3839, which is a IANA register port for RMS application suite communications. If you are upgrading from a version 1.0 of MeetingManager, you may wish to use port 9090. The MeetingManager 2.0 server is fully backwards compatible with the MeetingManager 1.0 NetLinx clients; however they will not take advantage of the new features and optimizations of 2.0. If this value is changed from one of the defaults, this new value must be configured in each NetLinx system using the 'SERVER-' command.
Ping Delay Time	The ping delay time is used to ensure that NetLinx clients are connected to the RMS application suite server. On this configured time interval, the RMS application suite server broadcasts request messages to the NetLinx clients. If the NetLinx clients do not respond within a specified amount of time, the MeetingManager server assumes the connection has been lost and the NetLinx system is offline. The default ping time is 30 seconds.
Ping Timeout Time	The ping timeout time setting is used as the maximum amount of time the MeetingManager server allows between NetLinx client ping responses. If the NetLinx client does not return a ping response within this amount of time, the RMS application suite server assumes the connection has been lost and the NetLinx system is offline. The default ping timeout time is 60 seconds.

After completing these settings, click **Next** to continue.

Security

The next system settings section is the MeetingManager Security Settings. Here you can determine if you want to require user authentication to access the RMS application suite administrative web interface. If you want user authentication, check the *Enable User Account Management* option.

If the *Enable User Account Management* option is checked, you can also choose to allow anonymous access to view the RMS application suite administrative web interface. To enable anonymous access, check the *Allow Anonymous Access* option.

After completing these settings, click **Next** to continue.

Administrator

NOTE

This screen may be skipped if you choose not to enable User Account Management.

If User Account Management is enabled, the Configuration Wizard automatically configures the default administrator account. The default administrator user name is *Admin*. You must enter the desired default administrator password in the field provided.

It is important to record this administrator username and password in a safe location. Once the default administrator account has been established, you cannot return to this step to alter it.

If the default administrator account has already been configured and you return to this step, the Configuration Wizard indicates *The Administrator account has already been configured* and does not allow you to alter the account.

Click **Next** to continue.

Scheduling

If the *Internal Appointment Management/Scheduling System* option was selected on the *Appointment Management/Scheduling System* step, then you will only need to enter a default master appointment password. This password is used to gain access to any user created appointment record in the system.

Appointment Modification Master Password	
Master Appointment Password	Type a password in the field provided. If this password is blank, there is no master password for modifying appointments. The default password is 1988.

Click **Next** to continue.

If the *External Appointment Management/Scheduling System* option was selected on the *Appointment Management/Scheduling System* step, then you need to configure which RMS application suite scheduling plug-in interface you wish to use with the RMS application suite.

For specific details on each scheduling plug-in, see the documentation that is associated with that plug-in.

After you have selected and registered the desired scheduling plug-in, click **Next** to continue.

Appointments

If the *Internal Appointment Management/Scheduling System* option was selected on the *Appointment Management/Scheduling System* step, you are presented with the dialog below.

Internal Appointment Options	
Keep Expired Appointments For	After appointments have expired, the RMS application suite automatically remove them from the system after this elapsed time. The default setting is 90 days.

After completing these settings, click **Next** to continue.

If the *External Appointment Management/Scheduling System* option was selected on the *Appointment Management/Scheduling System* step, then you are presented with the dialog below.

External Appointment Options	
Keep Expired Appointments For	After appointments have expired, the RMS application suite automatically removes them from the system after this elapsed time. The default setting is 90 days.
Appointment Synchronization Refresh Rate	The RMS application suite scheduling service attempts to connect to your third-party scheduling system at this time interval to update all new, modified, and deleted appointment records. The default setting is 15 minutes.
Web Mail URL	If your third-party scheduling system has a web based interface, you should enter the web path in the web mail URL field. If your third-party scheduling system does not have a web based interface, make sure this field is empty. After entering the web path, you can click the Test button to verify the path.

After completing these settings, click **Next** to continue.

SMTP

SMTP or Simple Mail Transport Protocol is the standard for sending email on the Internet. The RMS application suite uses SMTP for sending email notifications to users.

Enter all the appropriate SMTP settings.

SMTP Settings	
SMTP Enabled	Check this item to enable SMTP email delivery.
Server	Enter the IP address or host name of the SMTP server. IP port 25 is used for all SMTP communications.
Server Required Authentication	Check this item if your SMTP server requires a username and password authentication.
Username	Enter a valid username on the SMTP server.
Password	Enter the password for the username on the SMTP server.
Email Address	Enter an email address that all notifications from the RMS application suite will be sent on behalf of.
Reply Email Address	Enter the replay-to email address. Typically this is the same as the Email Address.
Friendly Name	Enter the display name you want to appear as the sender for notification emails.

You can test these SMTP setting using the **Test** button.

If you press the **Test** button, an SMTP Test dialog appears. Enter the email address you wish to send the test message. You can optionally modify the subject and message to send. When ready, press the **Send Test Message** button to send the text message.

When you have competed testing, click **Close**.

Click **Next** to continue.

SNPP

SNPP or Simple Network Paging Protocol is an alternative method to SMTP for delivering text-based messages to alphanumeric pager and cellular phones. If your wireless provider supports SNPP messaging, the RMS application suite can send notifications messages to users using SNPP. SNPP is preferred over the standard SMTP method of delivering text messages to wireless devices, as it is more direct and efficient.

SNPP Settings	
Enable SNPP Paging	Place a check in the box to enable SNPP Paging.
SNPP Default Provider	Make a selection from the list.
Add	If your SNPP provider is not in the provider list, you can add additional providers.
Remove	Remove an SNPP provider from the list.

If you wish to use SNPP paging, check the **Enable SNPP Paging** option and select a default SNPP provider from the provider list. If your SNPP provider is not in the provider list, you can add additional providers using the **Add** button.

You can test these SNPP settings using the **Test** button. If you press the **Test** button, a SNPP Pager Test dialog will appear. Enter the pager id for the mobile device you wish to send the test message. You can optionally modify the text message to send. When ready, press the **Send Test Message** button to send the text message.

When you have completed testing, click **Close**.

After you have finished setting the desired SNPP options, click **Next** to continue.

SNMP

The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor rooms, systems, and devices in the RMS system.

SNMP Settings	
Enable RMS SNMP Services	Place a check in the box to enable SNMP Services.
SNMP Agent Port (161 default)	Type the port number to use for SNMP.

SNMP Settings (Cont.)	
SNMP Community	The group to which devices and management stations running SNMP belong.
SNMP Trap Community	An alert that is sent to a management station by agents.
SNMP Trap Recipients	The name or IP address of hosts to which traps are to be sent.
Add	Adds a new recipient.
Remove	Removes selected recipient.

Logging

The RMS application suite can record room device and parameter changes to an internal database log as well as the Windows event log.

Logging Options	
Enable Internal Log	Select this option to enable internal logging.
Maximum Log Entries	Enter the number of messages. If you would rather base the Internal Log size on dates of messages, set this value to 0 and set *Delete Log Entries After*.
Delete Log Entries After	Enter the number of days. If you would rather base the internal log size on number of messages, set this value to 0 and set *Keep Maximum Log Entries*.
Enable Windows Event Log	Select this option to enable event logging.
Log Informational Messages	If this option is selected, the RMS application suite server logs all informational type messages to the windows event log. It is not recommended to use this option, if a large number of messages are posted to the event log.
Log Warning Messages	If this option is selected, the RMS application suite server logs all warning type messages to the windows event log. It is recommended to use this option to record any warning level notifications.
Log Error Messages	If this option is selected, the RMS application suite server logs all error type messages to the windows event log. It is recommended to use this option to record any error level notifications.

After you have selected the desired logging options, click **Next** to continue.

Syslog

Syslog logging can also be used to log messages. You need to supply the Syslog Server IP Address or hostname and the Syslog IP Port to enable communication.

The default syslog IP port is 514 and does not need to be changed unless you have a custom Syslog configuration.

SYSLOG Options	
Enable SYSLOG Messaging	Select the Enable SYSLOG Messaging to enable Syslog messages.
Syslog Server Address/Port	Enter the IP address or host name for the Syslog server. Enter the IP port for the Syslog server.
Syslog Facility ID	Select the facility from the drop down list.
Test Message Severity	Select from the drop-down list the message level severity.
Test Message	Text field for the message to be sent.

You can test Syslog messages by setting some sample text in the *Test Message Severity* field, and clicking the **Test** button.

After you have selected the desired Syslog options, click **Next** to continue.

Reporting

The RMS application suite can provide detailed reporting on room device and parameter changes based on a tracked history.

Place a check next to *Enable Reporting* to allow for this function. You must also specify the number of days for the RMS application suite to track. Note, the larger the number of days, the greater the number of records the database needs to store and the longer report queries take to run. The default is *90* days.

After you have selected the desired reporting options, click **Next** to continue.

Time Sync

The RMS application suite can maintain time and date synchronization between the RMS server and the remote NetLinx systems.

Synchronize NetLinx System Time/Date: if this option is enabled, the RMS application suite server synchronizes the time and date on NetLinx systems upon connection and subsequently once each evening. This option is recommended to maintain a consistent time and date throughout the system.

Synchronize Server Time/Date: if this option is enabled, the RMS application suite server connects to an Internet time synchronization server once per evening and synchronizes the server local time and date. This option is recommended only if the server is not already synchronized by other means such as a network time synchronization program. When selecting this option you can select a NIST time server from the NIST Time Server drop-down list or type in your own NIST time server address. You can click the **Synchronization** button to test the time synchronization process.

After you have selected the desired time synchronization options, click **Next** to continue.

Name & Logo

The RMS application suite allows user customization of the web page title and web page logo graphic.

To change the web page title, please enter the desired name in the *Application Title* field.

Selecting one of the logo options below can customize the web page logo:

- **Default Logo** - If this option is selected, the RMS application suite uses the default logo graphic.
- **User Defined Logo** - If this option is selected, you can browse to select an image file of your choice.
- **Custom Created Logo** - If this option is selected, the RMS application suite uses a custom implemented logo image. This option provides the user a method to create a logo image that seamlessly matches the graphic style of the web pages without the need for a border or background color. For more information, please click the *How to Create Custom Logo?* link on this page of the Configuration Wizard.

Creating A Custom Logo

1. Open the "logo_custom.GIF" in your favorite graphics manipulation software. This file can be found in the "C:\Program Files\AMX Resource Management Suite\Web\App_Themes\MeetingManager\images" directory (if you used the default installation location).

NOTE

The pixel dimensions for the logo are 147x101.

2. Add the logo to the image.

3. Save the logo to the "C:\Program Files\AMX Resource Management Suite\Web\App_Themes\MeetingManager\images" directory, make sure you save it as a .gif file and retain the name "logo_custom.GIF".
4. Use the configuration wizard to select "Custom Created Logo".

Finished

Congratulations you have completed the configuration wizard. You can return to the configuration wizard at any time to update or modify the RMS application suite settings.

Now that the RMS application suite server is fully configured, the administrative web pages are ready to use and the server is ready to accept NetLinx connections. If the *Launch RMS application suite Admin Web Page* option is selected, after closing the configuration wizard, the administrative web pages are automatically loaded. You now need to add users (*Creating a new User* section on page 87 of the *RMS Administrator's Guide*), add rooms (*Creating a new Room* section on page 80 of the *RMS Administrator's Guide*) and create notifications (*Creating a Notification* section on page 97 of the *RMS Administrator's Guide*).

Database Wizard

Overview

The AMX RMS application suite includes a utility program called *RMS Database Wizard*. The *RMS Database Wizard* tool performs the following:

- Tests the RMS application database connection.
- Modifies the RMS application database connection settings.
- Creates new RMS application databases.
- Removes RMS application databases.
- Imports data to an RMS application database.
- Exports data from an RMS application database.
- Backs up an RMS application database.
- Converts the RMS application database to another database platform.
- Applies updates to the RMS application database.

During installation, the RMS Database Wizard will be used to create the RMS database on one of the following supported database platforms:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005 Standard Edition
- Microsoft SQL Server 2005 Enterprise Edition
- Microsoft SQL Server 2005 Express Edition

Starting the Database Wizard

To access and perform the Database Wizard tasks, the RMS application services must first be stopped. If one of more of the RMS services are running when the Database Wizard starts, it will prompt you to stop the services before continuing.

1. Click the **Stop Services** button and wait for all the services to stop.
2. Click **Next** to continue.

First, the *RMS Database Wizard* checks the existing RMS application database connection. If a connection error is detected, you are prompted to re-configure the database connection settings. (see *Configuring Connection Settings* section on page 39 of the *RMS Administrator's Guide*).

Otherwise, click **Next** to continue to the main menu.

Main Menu

The Database Wizard main menu allows you to select the desired database operation to perform.

1. *Create new database / Remove existing database*

Select this option to create a new RMS application database or to remove an existing RMS application database.

2. *Import / Export data from MeetingManager database*

Select this option to import data into or to export data from the configured RMS application database. You can use the export option to backup the data in your RMS application database.

NOTE

The export function of the Database Wizard should not be used as a replacement for standard network and systems backup procedures typically performed by an IT department, but rather in addition to standard backup procedures. The export function creates a snapshot of the data contents in the RMS database, but does not backup the database file nor the database server.

3. *Convert RMS Database*

Select this option to convert the currently configured database to an alternate database platform.This option automates the process of creating a new database on the Microsoft SQL Server, migrating the data from the existing database to the new database, and re-configuring the RMS application's connection settings to use this new database.

4. *Apply RMS Update Script.*

Select this option if you have a database update script that you need to apply to your database. Database update scripts are created by AMX to provide a means of updating the existing database in place.

Configure Connection

Select this button to re-configure the RMS application database connection settings.

Create / Remove Menu

1. *Create new database.*

Select this option to create a new RMS application.

2. *Remove / Delete existing database.*

Select this option to delete an RMS application database file or remove an RMS application database from a database server.

Import / Export Menu

1. *Import to RMS database.*

Select this option to import data into the configured RMS application database.

2. *Export Data from RMS database.*

Select this option to export data from the configured RMS application database. You can use the export option to backup the data in your RMS application database.

NOTE

The export function of the Database Wizard should not be used as replacement for standard network and systems backup procedures typically performed by an IT department, but rather in addition to standard backup procedures. The export function creates a snapshot of the data contents of the RMS database, but does not backup the database file nor the database server.

Create A New Database

The *RMS Database Wizard* can create a new RMS application database for the following database platforms:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005

You need to provide the following information:

- Microsoft SQL Server Address
- Use Windows Authentication

  or

- Use SQL Server Authentication
  - Microsoft SQL Server Username

    - Microsoft SQL Server Password
- RMS application Database Name

Click **Next** to begin creating the new database.

The *RMS Database Wizard* creates the database structure of tables, then imports all of the default data into the new database. When the processes have completed, the *RMS Database Wizard* automatically reconfigures the RMS application connection settings to point to this new database.

Click **Next** to continue.

The *RMS Database Wizard* performs a database connection test and then returns to the main menu.

Remove A Database

The Database Wizard can remove an existing RMS application database for the following database platforms:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005

You need to provide the following information:

- Microsoft SQL Server Address
- Use Windows Authentication

  or

- Use SQL Server Authentication
    - Microsoft SQL Server Username
    - Microsoft SQL Server Password

1. Select the desired RMS application database to remove.
2. Click **Next** to continue.

The *RMS Database Wizard* can only remove RMS application databases. If you attempt to remove another database, an error is returned and no action taken.

As a final confirmation to remove the database, you are prompted to enter the word **destroy** to confirm that you are certain about removing the database. Once a database has been removed, it cannot be recovered.

Enter **destroy** and click **OK** to continue.

After the database has been removed, the *Database Wizard* performs a database connection test and then returns to the main menu.

Importing Data

The *RMS Database Wizard* can import data files that were exported using this tool. This data file is an XML formatted collection of all the records in the database. This process is useful if you have created a new database and want to import data from an existing alternate database.

After selecting *Import* from the *Import / Export* menu, you are prompted to select the import file. After selecting the import file, click **Next** to begin the import process.

After the import file has been processed, the Database Wizard will return to the main menu.

Exporting Data

The *RMS Database Wizard* can export all records in a database to a data file. This data file is an XML formatted collection of all the records in the database. This process is useful if you want to migrate to another database platform and want to export all records from your existing database. It can also be used to store backups of the data in your database.

After selecting *Export* from the *Import / Export* menu, you are prompted to select the export file. After selecting the export file, click **Next** to begin the export process.

After the export file has been completed, the *Database Wizard* returns to the main menu.

Converting A Database

The Database Wizard can fully automate the steps required to migrate from an existing database to an alternate database platform. The *RMS Database Wizard* can migrate between any of the following database platforms.

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005

The steps required to migrate are as follows:

Read the corresponding sections for more information about each specific step.

1. *Export all data from existing RMS database.*
2. *Create new RMS database.*
3. *Import RMS data into new database.*
4. *Configure RMS access to new database.*

Click **Next** to continue.

After the migration process has completed, the *RMS Database Wizard* performs a database connection test and then returns to the main menu.

Applying Update Scripts

The *RMS Database Wizard* can perform database maintenance and updates of the configured RMS application database using Update Scripts. Database update scripts are created by AMX to provide a means of updating the existing database in place.

1. Select the desired update script.
2. Click **Next** to continue.

If the *Configuration Wizard* detects that the database must be upgraded, it automatically launches the *Database Wizard Update Script* dialog.

The *RMS Database Wizard* tests to ensure that the update script can be applied to the existing configured database. It also ensures that the update script has not already been applied to the database. If these tests are passed, you are prompted with the *Ready To Update* message. If the update script does not pass these tests, an error message is displayed and you are not able to apply the update script.

Click **Next** to continue.

After the database script has been applied successfully, click **Next** to continue.

The *RMS Database Wizard* performs a database connection test and then returns to the main menu.

Configuring Connection Settings

You can use the Database Wizard at anytime to configure the RMS application database connection settings. The RMS application uses a DSN-less connection, and thus stores all the database connection settings internally.

Database Server:

Enter the database server IP address or hostname.

Use Windows Authentication

Enable Windows Authentication or,

Use SQL Server Authentication

- **Username**:

  Enter the database username (*if needed*).

- **Password**:

  Enter the database password (*if needed*).

Database Name:

Enter the database file name.

After configuring the RMS application database connection settings, the *RMS Database Wizard* performs a database connection test and then returns to the main menu.

93-3002-08 REV: C

It's Your World - Take Control™

3000 Research Drive, Richardson, TX 75082 USA • 800.222.0193 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support •
www.amx.com