

# Database Administrator's Guide **RMS**

# Resource Management Suite<sup>®</sup> (v3.3 or higher)



**Enterprise Applications** 

Last Revised: 4/15/2011

# **AMX 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. This license does not grant Licensee the right to create derivative works of the
  AMX Software. 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. AMX Dealer, Distributor, VIP or other AMX authorized
  entity shall not, and shall not permit any other person to, disclose, display, loan, publish, transfer (whether by sale, assignment,
  exchange, gift, operation of law or otherwise), license, sublicense, copy, or otherwise disseminate the AMX Software. Licensee
  may not reverse engineer, decompile, or disassemble the AMX Software.
- ACKNOWLEDGEMENT. You hereby acknowledge that you are an authorized AMX dealer, distributor, VIP or other AMX authorized entity in good standing and have the right to enter into and be bound by the terms of this Agreement.
- 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 REA-SON 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 GA 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 (other than pre-release code) 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 LIM-ITED WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS. Any supplements or updates to the AMX SOFTWARE, including without limitation, any (if any) service packs or hot fixes provided to Licensee 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 Licensee's 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 in accordance with AMX's current return policy. 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 DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE.
- 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 ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.
- SOFTWARE AND OTHER MATERIALS FROM AMX.COM MAY BE SUBJECT TO EXPORT CONTROL. The United States
  Export Control laws prohibit the export of certain technical data and software to certain territories. No software from this Site may
  be downloaded or exported (i) into (or to a national or resident of) Cuba, Iraq, Libya, North Korea, Iran, Syria, or any other country to which the United States has embargoed goods; or (ii) anyone on the United States Treasury Department's list of Specially
  Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. AMX does not authorize the downloading or
  exporting of any software or technical data from this site to any jurisdiction prohibited by the United States Export Laws.

This Agreement replaces and supersedes 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. For any questions concerning this Agreement, or to contact AMX for any reason, please write: AMX License and Warranty Department, 3000 Research Drive, Richardson, TX 75082.

i

# **Table of Contents**

RMS Database Administrator's Guide	.1
Overview	. 1
Additional Documentation	. 2
System Requirements	. 2
Minimum Hardware Requirements	. 2
Supported Platforms	. 2
RMS Supported Databases	. 2
RMS Supported Scheduling Interfaces	. 3
RMS Supported Web Browsers	. 3
RMS SDK Support	. 3
Additional System Requirements	. 3
Database Authentication	.5
Overview	. 5
SQL Login	. 5
1) Add SQL Login Account to SQL Server	. 5
2) Add SQL Login Account to RMS Database	. 7
3) Configure RMS to use SQL Login	. 9
Windows Authentication	10
1) Create Domain User Account	10
2) Add Domain User Account to SQL Server	12
3) Add Domain User Account to RMS Database	14
4) Configure RMS for Windows Authentication	16
a) RMS NT Services	17
b) RMS Web Application (ASP.NET)	21
Add "NT AUTHORITY\NETWORK SERVICE" Account to SQL Server	21
Add "NT AUTHORITY\NETWORK SERVICE" Account to RMS Database	23
Add "NT DOMAIN\RMSServerMachineName\$" Account to SQL Server	25
Add "DOMAIN\RMSServerMachineName\$" Account to RMS Database	27
c) RMS Configuration Wizard & RMS Database Wizard	29 29
Database User Permissions	21
	24
	31
Hexible Access	31
Restrictive Access	31
Database Installation	33
Overview	33

Manual Database Installation	
Overview	37
Manual Installation Steps	
Database Backup	41
Overview	41
Additional Online References	41
Installing SQL Server 2005 Express Edition	43
Overview	43
Installation	43
Setup	

# **RMS Database Administrator's Guide**

### **Overview**

The AMX Resource Management Suite (RMS) is a line of software solutions designed for IT professionals, facility managers and meeting/classroom users looking for a way to manage, monitor and/or schedule up to 1,000 rooms and an unlimited number of assets.

The RMS application is a client/server application where the NetLinx system acts as the client and the RMS application server listens for connections from NetLinx systems. NetLinx and the RMS application server communicate using TCP/IP sockets. In order to establish communication, each NetLinx system must be able to resolve and connect to the RMS application server. This can be accomplished with a variety of Network configurations including local area networks (LAN), wide area networks (WAN), and the Internet.

This document outlines the installation prerequisites, installation guidelines, database access permissions and other important database related information for the RMS database installation.

- **1.** RMS must be installed on a Microsoft SQL server. The list below includes the supported version of SQL servers.
  - a. Microsoft SQL Server 2008
  - **b.** Microsoft SQL Server 2005
- **2.** RMS can utilize the Microsoft SQL Express edition database at no cost for small installations with a limited number of rooms and users.

The following guidelines should be considered when evaluating if your site is a candidate for using the Microsoft SQL Express edition.

If your RMS installation is planned to exceed 300 rooms, the Express edition should not be used.

The guidelines listed above are general recommendations for most users; however may not apply to all customers where certain sites may require more advanced database services.

- Consult the Microsoft SQL Server Web site for a full listing of the feature comparison and feature limitations imposed by the SQL Express edition. http://msdn.microsoft.com/en-us/library/cc645993.aspx
- For instructions on installing SQL express, refer to the *Installing SQL Server 2005 Express Edition* section on page 43.
- 3. It is important to note that RMS does not require a dedicated Microsoft SQL server.

The RMS database catalog may be installed into an existing Microsoft SQL server or cluster as long as it meets the minimum requirements outlined above.

**4.** Installation of RMS requires an administrative account on the local RMS server and database administrative access.

The RMS installation, RMS Configuration Wizard, and all other RMS maintenance tools must be run on the RMS server while logged on with an administrative account.

**5.** If your company has a staffed Database Administrator (DBA) who will be responsible for the RMS database, it is important to provide this document to them and that they carefully review the installation requirements and database access requirements for RMS.

#### **Additional Documentation**

Refer to the following supplemental RMS documents (available to view/download from www.amx.com):

- **RMS Installation Checklist** The RMS Installation Checklist is provided to ensure all the necessary prerequisites are met and all the necessary configuration option are identified prior to the installation of the RMS server.
- **RMS IT Administrator's Guide** This document outlines the installation prerequisites, installation guidelines, server access permissions and other important IT related information for the RMS application server installation.
- **RMS Administrators Guide** This document provides information and instructions for the RMS System Administrator.
- **RMS NetLinx Programmers Guide** This document provides detailed NetLinx programming information for RMS systems.
- **RMS Plug In Installation Guides** A separate installation guide is provided to describe installing each of the RMS plug-ins (i.e. *EMS Scheduling Plug-in, Exchange Mailbox Plug-in, Groupwise Mailbox Plug-in, Lotus Notes Appointment Interface Plug-in, Outlook Scheduling Plug-in, PeopleCube Scheduling Plug-in, Planon Scheduling Plug-in, R25 Scheduling Plug-in, etc.)*
- **RMS Quick Start Guide** This document provides basic instructions for getting started with RMS.
- RMS User Manual This document describes various end-user functions of RMS.

# System Requirements

#### **Minimum Hardware Requirements**

- Processor: Intel Pentium IV 3 GHz (x86) or Intel Pentium Dual/Quad Core 2.0 GHz
- Memory: 2 GB
- **Display**: 1280x1024 resolution
- Hard Disk: 500 MB available space



RMS must be installed on a dedicated server class machine.

#### **Supported Platforms**

- Windows Server 2003 Standard (SP2; 32-bit only)
- Windows Server 2003 Enterprise (SP2; 32-bit only)
- Windows Server 2008 Standard (32-bit only)
- Windows Server 2008 Enterprise (32-bit only)

#### **RMS Supported Databases**

- Microsoft SQL Server 2008 Express Edition (for systems with less than 300 rooms only; download available free from Microsoft)
- Microsoft SQL Server 2008 Standard Edition
- Microsoft SQL Server 2008 Enterprise Edition
- Microsoft SQL Server 2005 Express Edition (for systems with less than 300 rooms only; download available free from Microsoft)
- Microsoft SQL Server 2005 Standard Edition
- Microsoft SQL Server 2005 Enterprise Edition



For RMS systems with more than 300 rooms, the database must be installed on an external database server and not installed on the same server machine as the RMS software.

#### **RMS Supported Scheduling Interfaces**

Scheduling Interfaces have been removed from the standard RMS installation. Please visit www.amx.com for specifications and ordering information.

pported Scheduling Systems	
licrosoft Exchange	
licrosoft Outlook	
otus Notes	
Groupwise	
MS	
25	
eoplecube	
lanon	



RMS is capable of supporting multiple (up to 12) instances of Scheduling on a single NetLinx Master. If you intend to run multiple instances of Scheduling on a Master, then that Master should be dedicated solely to RMS Scheduling.

For instructions on installing and configuring the various scheduling plug-ins available for RMS, refer to the Installation Guide provided with your particular Plugin. RMS Scheduling Plugin documentation is also available to view/download from **www.amx.com**.

#### **RMS Supported Web Browsers**

Windows Platform

- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7
- Mozilla FireFox 2.0

Macintosh Platform

• Mozilla FireFox 2.0

#### **RMS SDK Support**

- All NetLinx hardware platforms
- Touch panel files for G4
- NetLinx modules (RFID supported only on Duet-enabled NetLinx hardware)

#### **Additional System Requirements**

- Microsoft .NET Framework 2.0
- Internet Information Services (IIS) 6.0 (for Windows 2003 servers)
- Internet Information Services (IIS) 7.0 (for Windows 2008 servers)
- Adobe Acrobat Reader 7.0.5 or later

RMS Database Administrator's Guide

# **Database Authentication**

## **Overview**

The RMS service and RMS website can access the RMS database using one of the two following authentication methods.

• **SQL Login**: This option provides the simplest configuration requirements. A dedicated user account for RMS is defined directly in the SQL server.

The username and password for this dedicated user account must be configured in the RMS Configuration Wizard. Once configured, RMS will use these account credentials for all RMS database operations.

• Windows Authentication: This option is a bit more complex to setup and configure but permits you to use Windows Active Directory domain authenticated permissions rather than a direct SQL username and password login account. This option may be required under the policies of your Information Technology department.

# **SQL** Login

To configure the RMS software for use with a SQL login account, please follow the instructions below.

#### 1) Add SQL Login Account to SQL Server

- 1. Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- 2. Expand the Security folder, right-click the Logins folder, and select New Login (FIG. 1).



FIG. 1 Logins > New Login

This opens the New Login dialog (FIG. 2):

				_ 🗆 ×
式 Script 🝷 🚺 Help				
Login <u>n</u> ame:	rms			S <u>e</u> arch
C Windows authentication				
SQL Server authentication				
Password:				
Confirm password:	•••••			
Specify old password				
<u>O</u> ld password:				
Enforce password polic	ÿ			
Enforce password expire	ration			
🔲 User must change pass	sword at next login			
C Mapped to certificate	ſ		<b>v</b>	
C Mapped to asymmetric key			-	
Map to Credential			<b>Y</b>	Add
Mapped Credentials	Credential	Provider		
	J			Remo <u>v</u> e
Default <u>d</u> atabase:	master		•	
Default language:	<default></default>		•	
			0K 1	Coursel 1
			UK	Lancel

FIG. 2 New Login dialog

- **3.** In the *Login Name* field, enter the new RMS **Login name**.
- **4.** Next, make sure the SQL Server Authentication option is selected and enter the login account password. Ensure the *Enforce password expiration* and *User must change password at next login* options are not checked.
- **5.** Click **OK** to save the new user account.

#### 2) Add SQL Login Account to RMS Database



If the RMS database has not yet been installed on your SQL server, then you may need to install the RMS database and then come back to this step to complete the permissions configuration for the RMS SQL Login.

With the RMS user account added to the SQL database server in the previous step, we now need to add the RMS user and grant permissions to the RMS database.

- 1. Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- **2.** Expand the *Databases* folder and find the RMS database.
- **3.** Expand the *RMS* folder, and the *Security* folder.
- 4. Right-click the *Users* folder and select **New User** (FIG. 3).



FIG. 3 Users > New User

This opens the New User dialog (FIG. 4):

**5.** Enter the "RMS" login name and the local SQL login name of "RMS" as shown in FIG. 4. You can use the search button to locate the SQL login account if needed.

			_ 🗆 ×
<u> S</u> cript 👻 🚺 Help			
User name: © Login name: © Certificate name:	RMS RMS		
C Key name:			
C <u>₩</u> ithout login			0
<u>D</u> efault schema:			
Schemas <u>o</u> wned by this user:			
Owned Schemas			
db_ddladmin     db_denydatareader     db_denydatawriter     db_owner     db_securityadmin     guest     NT AUTHORITY\NETWOP	ik service		
Role Members		 	
db_datareader         db_datawriter         db_ddladmin         db_denydatareader         db_denydatawriter         db_denydatawriter         db_denydatawriter         db_denydatawriter         db_denydatawriter         db_securityadmin			
		ОК	Cancel

FIG. 4 New User dialog

- 6. Select the *db\_owner* role under **Database Role Membership**.
- 7. Click OK to save the user account and permissions to the RMS database.



The **db\_owner** privilege will grant the RMS user account full permissions over the RMS database. If you require more restrictive access, refer to the Database User Permissions section on page 31.

#### 3) Configure RMS to use SQL Login

**1.** In the RMS Configuration Wizard, on the database configuration step, enter the **RMS** user account and password under the *Use SQL S* - *Server Authentication* database connection option (FIG. 5).

esource Management Sui	te Configuration Wizard		
Velcome Database Connection Configuration Updates	Database Server:	Ver Database Connection	Settings
Product Selection     Web Services     Services     Licensing     OS Permissions     System Settings     Finished	<ul> <li>Use SQL Server A Username: Password: Database Name:</li> </ul>	Authentication Ims INNERNALINALINAL RMS	
<⊛			New Connection

FIG. 5 RMS Configuration Wizard - Configure SQL Server Database Connection Settings

**2.** Click **Next** to test the database connection.

If the database connection is successful, then the following dialog will be displayed (FIG. 6):

Welcome Database	Database	
Connection Configuration Updates Product Selection Web Services	Connected to dat	abase successfully.
Services	Database Name:	RMS
Licensing	Database Version:	3.0.7 (3/28/2008 12:00:00 PM)
OS Permissions	DB Server Name:	Microsoft SQL Server
System Settings	DB Server Version:	10.00,1600
al rinsticu	DB SQL Support:	283

FIG. 6 RMS Configuration Wizard - Connected to database successfully

• If the database connection fails, re-check the SQL login account password and assigned permissions to the RMS database.

• Once connected successfully, you can proceed with the RMS configuration; no other settings or configuration is required for database authentication.

# Windows Authentication

The second authentication method supported is *Windows Authentication*. Under this configuration, each RMS process will attempt to access the RMS database using the Windows Active Directory account under which that process is running.

This connection method is also known as "Trusted Connection" and "SSPI" (Security Support Provider Interface).

When opting to use Windows Authentication, a domain user account must be created in the Active Directory. This user account must explicitly be granted user permissions to the RMS database. This same domain user account should also be configured as an Administrator on the local RMS server by adding the domain account to the Administrators group on the RMS server.

Please note, this does not mean that this RMS user account must be a member of the Administrator's group in the Active Directory domain.

In addition to the RMS domain user account, the computer that is running the RMS server must also have a computer account defined in the Active Directory domain and the SQL server hosting the RMS database must be a server computer defined in the domain.



The instructions and screenshots provided here may vary depending on the version and edition of Windows Server you may be using.

#### 1) Create Domain User Account

To create a new domain user account, you must log on to a domain controller server with a Domain Administrator account.

- 1. Open the *Active Directory Users* and *Computer configuration utility* from the **Start > Administrative Tools** menu.
- 2. On the *Users* folder, right-click and select New > User (FIG. 7):



FIG. 7 Active Directory Users and Computers - New > User

This opens the first New Object - User dialog (FIG. 8):

First name:	rms		Initials:	
– Last name:				-
Full n <u>a</u> me:	rms			-
User logon name				
rms	<u>.</u>	@company.c	om	-
User logon name	(pre- <u>W</u> indows	2000):		
osenogonname	(pre <u>w</u> indows	2000).		-

FIG. 8 New Object - User dialog 1

- **3.** Enter the username and login credentials.
- 4. Click Next to continue to the next New Object User dialog (FIG. 9).

w Object - User	_	_	
😴 Create in: com	pany.com/Users		
<u>P</u> assword:	•••••		
<u>C</u> onfirm password:	•••••		
User must change passw	ord at next logon		
User cannot change pas	sword		
✓ Password never expires			
Account is disabled			
		1	
	< <u>B</u> ack	<u>N</u> ext >	Cancel

FIG. 9 New Object - User dialog 2

- **5.** Enter a password for the new user account.
  - Since this is a user account that will run the RMS services in an unattended mode, make sure to select the *Password never expires* option.
  - Also uncheck the *User must change password* at next logon option.

Click Next to continue. Proceed until the user has successfully been added to the Active Directory.



If your active directory is configured to use Microsoft Exchange, then you will be prompted to create an Exchange mailbox while you are cresting this new RMS user account.

If you intend to interface the Resource Management Suite product with your Exchange system, then you will want to create the mailbox account for this new user.

#### 2) Add Domain User Account to SQL Server

- 1. Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- 2. Expand the Security folder, right-click the Logins folder, and select New Login (FIG. 10).



FIG. 10 Security > Logins > New Login

This opens the Login - New dialog (FIG. 11).

Login, new				
Select a page	Script - 🚺 Help			
Server Roles	Login name:	COMPANY\RMS		Sgarch
Y User Mapping Securables Status	<ul> <li>Windows authentication</li> <li>SQL Server authentication</li> <li>Bassword</li> <li>Confirm password</li> <li>Specify old password</li> <li>Specify old password</li> <li>Bertorce password polic</li> <li>Enforce password polic</li> <li>Enforce password expirition</li> <li>User must change pass</li> <li>Mapped to ceptificate</li> <li>Mapped to asymmetric key</li> <li>Map to Credential</li> </ul>	y ation word at next login		× Add
Connection	Mapped Credentials	Fredential	Provider	=
Server: (local) Connection: View connection properties Progress				Remove
Beady		[marter	4	-
S. J.	Default language:	<default></default>		1

FIG. 11 Login - New dialog

- **3.** In the *Login Name* field, enter the new RMS domain user account.
  - Since this is a domain account and not a local computer account you will need to enter the account login name in the form of "**domain**\user".
  - Also, make sure the *Windows Authentication* option is selected.
- 4. Click **OK** to save the new user account.

#### 3) Add Domain User Account to RMS Database



If the RMS database has not yet been installed on your SQL server, then you may need to install the RMS database and then come back to this step to complete the permissions configuration for the RMS SQL Login.

With the RMS domain user account added to the SQL database server in the previous step, we now need to add the RMS domain user and grant permissions to the RMS database.

- 1. Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- **2.** Expand the *Databases* folder and find the RMS database.
- **3.** Expand the RMS database folder and the *Security* folder.
- 4. Right-click the *Users* folder and select New User (FIG. 12).



FIG. 12 Databases > Security > New User

This opens the New User dialog (FIG. 13):

			_ 🗆 ×
🖇 Script 👻 📑 Help			
User name:	RMS		
Login name:	COMPANY\RMS	3	
C Certificate name:			
C Key name:			
C Without login	1		
Default schema:	r		
Derault schema.			
Schemas <u>o</u> wned by this user:			
Owned Schemas			<b>_</b>
🔲 db_ddladmin			
🔲 db_denydatareader			
🔲 db_denydatawriter			
🔲 db_owner			
🗖 db_securityadmin			
🔲 guest			-
Database role <u>m</u> embership: Role Members			
☐ db datareader			
□ db_datawriter			
🗖 db ddladmin			
└── _ └── db_denvdatareader			
db denydatawriter			
✓ db owner			
db_securityadmin			-
L-			
		OK	Cancel

FIG. 13 Add Domain User Account to RMS Database

- 5. Enter the RMS login name and select the domain user account RMS as shown above.
  - The domain user account should be defined in the form of **domain**\user.
  - You can use the search button to locate the domain user account if needed.
- 6. Select the db\_owner role under *Database Role Members*.
- 7. Click OK to save the user account and permissions to the RMS database.



The **db\_owner** privilege will grant the RMS user account full permissions over the RMS database. If you require more restrictive access, refer to the Database User Permissions section on page 31.

#### 4) Configure RMS for Windows Authentication

**1.** When configuring the database connection in the RMS Configuration Wizard, select the *Use Windows Authentication* option to use windows database authentication (FIG. 14).

Welcome	Configuration Wizard	ver Database Connection Settings
Connection	Database Server:	.\sglexpress
Updates	C Use Windows Aut	thentication
Product Selection Web Services Services Licensing OS Permissions System Settings Finished	C Use SQL Server A Username: Password: Database Name:	Authentication       RMS       New Connection

FIG. 14 Use Windows Authentication

2. If the database connection is successful, then the following dialog will be displayed (FIG. 15).

Database	
Connection Configuration Updates Product Selection Web Services	
Services Database Name: RMS	
OS Permissions DB Server Name: Microsoft SOL Server	DO PM)
System Settings DB Server Version: 10.00.1600	
Finished     DB SQL Support: 283	

FIG. 15 Connected To Database Successfully

• If the database connection fails, please recheck the domain user account assigned permissions to the RMS database.

• When configuring the database connection in the RMS Configuration Wizard, if the option to *Use Windows Authentication* is selected, then the following warning message will be displayed (FIG. 16).

source management sur	te Configuration Wizard
Database	Attention
Connection Configuration Updates	Using Windows authentication for database access requires that each RMS service and the RMS ASP.NET web application each are configured with an account that has database access.
Web Services Services Licensing	RMS NT Services: When registering each RMS NT Service, you must assign the "Log On As" user account with an account that has Windows authentication permissions to the RMS database.
System Settings Finished	RMS ASP.NET Web Application: By default, the RMS ASP.NET web application uses specialized domain accounts. These domain accounts must be granted access to the RM database on the SQL database server.

FIG. 16 Database Windows Authentication - Warning

This warning message is provided to help identify that choosing the Windows Authentication option for the database connection will have additional configuration requirements that must be setup correctly to ensure that RMS can successfully communicate with the RMS database.

For Windows Authentication to work properly and permit the RMS processes to access the RMS database, it is important to understand and identify each of the RMS processes and how they interact with the RMS database. RMS processes run under distinct principal user contexts each requiring access to the database server.

#### a) RMS NT Services

RMS contains 4 Windows NT services. Each of these service run under their own unique process and all must be configured to use a user account that has Windows Domain permissions to the RMS database.

- AMX RMS Server
- AMX RMS NetLinx Connection Manager
- AMX RMS Communication Manager
- AMX RMS Scheduling Manager

When attempting to Register the RMS services in the RMS Configuration Wizard, the user will be prompted to provide a user account for each RMS service, in the *Register Service* dialog (FIG. 17).

	RMS Server Serv	ice
f using Windows Authe must configure a "Log nas NT domain / Activ are using a SQL Expres as the RMS application without requiring a cust	Intication to connect to t In As" user account bel a Directory permissions to is database server install b, then the "Local System om user account.	the RMS Database, then you low with a user account that o the RMS database. If you led locally on the same server " account should work
Log on as.		
C Local System a	count	
	DHC	
	нмэ	
Ihis account: Password:	HM3  xxx	

FIG. 17 Register Service dialog

- If you are using RMS with SQL Express and the SQL Express database server is installed on the same server, then the "Local System" account may be used.
- If you are using RMS with a remote SQL server, then you must provide a domain user account that has access to the RMS database.
- You may enter a domain account in the form of: domain\user.



The drop down list will not contain domain user account, only accounts on the local computer. However, you can type in the domain\user account directly in the text entry field of the drop down box.

Alternatively, the RMS NT services can also be configured manually via the "Services" manager under "*Administrative Tools*" on the Windows server (FIG. 18).

Name 🗡	Status	Startup Type	Log On As
🏶 AMX RMS Communications Manager	Started	Automatic	Local System
🏶 AMX RMS NetLinx Connection Manager	Started	Automatic	Local System
🆏 AMX RMS Scheduling Manager	Started	Automatic	Local System
🎇 AMX RMS Server	Started	Automatic	Local System

FIG. 18 "Services" manager under "Administrative Tools" (on the Windows server)

1. Select each RMS NT service and edit the properties to display the *Server Properties* dialog. Use the options on the *Log On* tab to specify the computer or domain account to use for each service (FIG. 19).

AMX RMS Server Proj	perties (Local Computer)	? 🛛
General Log On Rec	overy Dependencies	
Log on as: Local System accou	unt interact with desktop	
⊙ <u>I</u> his account:	RMS	Browse
Password:	•••••	
<u>C</u> onfirm password:	•••••	
You can enable or disal	ble this service for the hardware	profiles listed below:
Hardware Profile		Service
Profile 1		Enabled
	Enable	<u>D</u> isable
	OK Can	cel <u>A</u> pply

FIG. 19 Server Properties dialog (Log On tab)

**2.** After making the changes to each of these NT services and configuring the **Log On As** account with the new dedicated RMS domain user account, re-run the RMS Configuration Wizard to correct any NTFS file permissions.

🕫 Resource Management Su	ite Configuration Wizard 🛛 💽 🖃 🔀
Resource Management Suite	Configuration Wizard
	OS Permissions Configuration (Web/IIS/ASP.NET)
terender Herrichter H	Operating system permissions must be configured for:
Product Selection     Web Services     Services     Iccensing     OS Permissions     Web User     Web User     Finished	User Accounts: IUSR_RSAVAGE5224 ASPNET NETWORK SERVICE MeetingManager Resources: MeetingManager Temporary Files Directory Permissions Are Set MeetingManager Dynamic Images Directory Permissions Are Set
дмх®	
	< <u>B</u> ack <u>N</u> ext > E <u>x</u> it

FIG. 20 RMS Configuration Wizard - Use SQL Server Authentication

3. Open the RMSDCOMConfig.EXE tool in the RMS program installation directory.

**4.** Run this tool and make sure the new dedicated RMS domain user account list included in the list of accounts (FIG. 21).

AMX Resource Management Suite Service Registration	
AMX Resource Management Suite DCOM Permissions Configuration Util	ity Restrict
This utility program will automatically configure the proper DCOM permissions configuration settings neccessary for the RMS application IUSR_RSAVAGE5224	tion.
	Remove
View Permissions Grant Permissions Remove Permis	sions
Back.	(E <u>x</u> it

FIG. 21 AMX Resource Management Suite DCOM Permissions Configuration Utility

5. Next, select View Permissions.

If any item in the result list displays "*Permission Not Set*", then you will need to select the "*Grant Permissions*" option to apply the correct DCOM permissions for all the user accounts.

**6.** After granting the proper permissions, select **View Permissions** to visually confirm that all accounts now have the proper DCOM permissions.



In RMS installations that are integrating with Microsoft Exchange, the NT service account for the RMS Scheduling Manager service must use a domain account with permissions to the Exchange server.

If possible, use the same dedicated RMS domain account that you created for the database permissions.

If it is not possible to use this same dedicated domain account and a unique domain account is required for interfacing to the Exchange system, then this additional user account will also need to be added to the RMS database and granted the proper permissions.

#### b) RMS Web Application (ASP.NET)

The RMS ASP.NET Web application by default runs under the Network Service account.

When configured to use Windows authentication for database access, this account must also be granted access to the RMS database.

If the SQL server is running on the same server computer as RMS (for example if you are running SQL express on the same server), then you can simply add the **NT AUTHORITY\NETWORK SERVICE** account to the database server security logins and then add the account and grant permissions to the RMS database catalog.

#### Add "NT AUTHORITY\NETWORK SERVICE" Account to SQL Server

- 1. Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- 2. Expand the Security folder, right-click the Logins folder, and select New Login (FIG. 22).

<u>Eile E</u> dit <u>V</u> ie	w <u>T</u> ools	<u>W</u> indow	Community	/ <u>H</u> e
일 New Query	D) 🔁	🔁 🌇 🗌	🔓   💕 I	
Object Explorer			÷	Ψ×
Connect •	=	7 💿 🔏		
🖂 🖪 (local) (SC	L Server 10	1.0.1600)	8	
🕂 🧊 (Jocal) (Sq	ases			
🖃 🧰 Securi	ty			
🖂 🗀 🗖	gins			-
2	N	ew Login		##
4	Fi	ļter	•	ŧ
4	SI	art PowerS	hell	E
2 2	R	eports	F	
🧟 ਦ 🗀 Se	rv R	e <u>f</u> resh		
🕀 🛄 Cr	edentials	and the second		52 
🕀 🛅 Cr	yptographi	c Providers		
🕀 🧰 Au	ıdits			
🕀 🚞 Se	rver Audit (	Specification	าร	
🕀 🧰 Servel	Objects			
🕀 🧰 Replic	ation			
🖽 🛄 Manag	lement			
📷 SQL S	erver Ageni	t (Agent XP:	s disabled)	

FIG. 22 Security > Logins > New Login

This opens the Login - New dialog (FIG. 23):

and the second sec			
Reneral	Script - 🚺 Help		
General Server Roles User Mapping Securables Status	Login pame: Windows authentication SQL Server authentication Bassword Contim password Decity old password Qid password Contemport authentication		Sgarch
onnection	Enforce preserved point     Enforce password expiri-     User must change pass     Mapped to ceptificate     Mapped to asymmetric key     Map to Credential     Mapped Credentials	vation word at next login	- - - <u>A</u> dd
Server: (local) Connection:			
Ready Ready	Default gatabase: Default language:	master 2 (default)	Hemoye

FIG. 23 Login New dialog

- 3. In the Login Name field, enter the "NT AUTHORITY\NETWORK SERVICE" user account.
  - Since this is a domain account and not a local computer account you will need to enter the account login name in the form of "domain\user".
  - Also, make sure the Use Windows Authentication option is selected



If you use the Search button to find the account, it will be displayed as NETWORK SERVICE in the search results listing.

4. Click **OK** to save the new user account.

#### Add "NT AUTHORITY\NETWORK SERVICE" Account to RMS Database



If the RMS database has not yet been installed on your SQL server, then you may need to install the RMS database and then return to this step.

With the **NT AUTHORITY\NETWORK SERVICE** account added to the SQL database server in the previous step, we now need to add the **NT AUTHORITY\NETWORK SERVICE** account and grant permissions to the RMS database.

- 1. Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- **2.** Expand the *Databases* folder and find the RMS database.
- **3.** Expand the RMS database folder and the *Security* folder.
- 4. Right-click the Users folder and select New User (FIG. 24).



FIG. 24 Databases > Security > Users > New User

This opens the New User dialog (FIG. 25):

		_ 🗆 🗙
式 Script 👻 🚺 Help		
User name:	INT AUTHOBITY/NETWORK SERVICE	
C Lasia associ		
<ul> <li>Login name.</li> </ul>	NT AUTHORITT WET WORK SERVICE	
C Certificate name:		1
C Key name:		
$oldsymbol{C}$ $$ $\!$		
<u>D</u> efault schema:		
Schemas owned by this user:		
Owned Schemas		
🔲 db_ddladmin		
🔲 🗖 db_denydatareader		
🗖 db_denydatawriter		
db_owner		
🔲 🗖 db_securityadmin		
🔲 guest		-
Database role <u>m</u> embership:		
Role Members		
🗖 db_datareader		
db_datawriter		
🗖 db_ddladmin		
db_denydatareader		
db_denydatawriter		
db_owner		
db_securityadmin		-
	nr	Cancel

FIG. 25 New User dialog

5. Enter the NT AUTHORITY\NETWORK SERVICE user name and select the login name NT AUTHORITY\NETWORK SERVICE, as shown above.

You can use the search button to locate the NT AUTHORITY\NETWORK SERVICE account if needed.

- 6. Select the db\_owner role under *Role Members*.
- 7. Click OK to save the user account and permissions to the RMS database.



The **db\_owner** privilege will grant the NT AUTHORITY/NETWORK SERVICE user account full permissions over the RMS database. If you require more restrictive access, refer to the Database User Permissions section on page 31.

If the SQL server is running on a remote server then you will need to add the RMS server machine account to the database server security logins and then add the account and grant permissions to the RMS database catalog.

The computer domain account is expressed in the form of domain name followed by the computer name with a trailing "\$" character. (e.g. "DOMAIN\RMSServerMachineName\$")

#### Add "NT DOMAIN\RMSServerMachineName\$" Account to SQL Server

- **1.** Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- 2. Expand the Security folder, right-click the Logins folder, and select New Login (FIG. 26).

<u>File Edit Vie</u>	w <u>T</u> ools <u>W</u> indow	<u>Community</u>
🤰 New Query	🗅 🗠 🔂 🐴	
Object Explorer		+ 4 ×
Connect 🕶 🛛 📑	🛃 = 🍸 🛃 🌌	3
🖃 🔼 (local) (SC	Server 10.0.1600)	
🕀 🧊 (local) (sq	ases	
🖃 🧰 Securi	ty	
E 🚞 Lo	gips	
2	New Login	##
4	Filter	• t
2	Start Powers	5 <u>h</u> ell
4	Reports	٠
🛃 🖂 Se	Re <u>f</u> resh	
🕀 🧰 Cr	edentials	20
🕀 🛄 Cr	yptographic Providers	(
🕀 🚞 Au	udits	
🕀 🛄 Se	rver Audit Specificatio	INS
🕀 🚞 Servei	r Objects	
🕀 🦲 Replic	ation	
🕀 🚞 Manaç	jement	
📸 SQL S	erver Agent (Agent XF	's disabled)

FIG. 26 Security > Logins > New Login

This opens the Login - New dialog (FIG. 27):

Login - New			_ 0
elect a page	🔄 Script 👻 🚺 Help		
Tueneral Server Roles User Mapping Securables	Login name:	DOMAIN\RMSServerMachineName\$	Sgarch
Status	C SQL Server authentication     C SQL Server authentication     Cassword:     Confirm password:     Specify old password     Qld password:     Erforce password policy     Erforce password egyin	r abon	
	User must change pass     Mapped to cettificate     Mapped to asymmetric key     Map to Credential	word at next login	N N Add
Connection	Mapped Credentials	Credential Provider	
Server: (local) Connection: <u>Usew connection properties</u>			
Progress			Remoye
C Ready	Default gatabase: Default language:	master   <default></default>	•

FIG. 27 Login - New dialog

- 3. In the Login Name field, enter the "DOMAIN\RMSServerMachineName\$" user account.
  - Since this is a domain account and not a local computer account you will need to enter the account login name in the form of "domain/machinename\$".
  - Also, make sure the *Windows Authentication* option is selected
- 4. Click OK to save the new user account.

#### Add "DOMAIN\RMSServerMachineName\$" Account to RMS Database



If the RMS database has not yet been installed on your SQL server, then you may need to install the RMS database and then return to this step.

With the "DOMAIN\RMSServerMachineName\$" account added to the SQL database server in the previous step, we now need to add the "DOMAIN\RMSServerMachineName\$" account and grant permissions to the RMS database.

- 1. Open Microsoft SQL Server Management Studio and connect to your SQL database server.
- **2.** Expand the *Databases* folder and find the RMS database.
- **3.** Expand the RMS database folder and the *Security* folder.
- 4. Right-click the *Users* folder and select New User (FIG. 28).



FIG. 28 Databases > Security > Users > New User

This opens the New User dialog (FIG. 29):

		_ 🗆 🗙
式 Script 👻 🚺 Help		
<u>U</u> ser name:	DOMAIN\RMSServerMachineName\$	
Login name:	DOMAIN\RMSServerMachineName\$	
C Certificate name:		
C Key name:		
C	,	
Default schema:		
Schemas owned by this user:		
Uwned Schemas		
db_denydatareader		
db_denydatawriter		
db_owner		
db_securityadmin		
guest		-
Database role membership:		
Role Members		
db_datareader		
🗖 db_datawriter		
🗖 db_ddladmin		
🗖 db_denydatareader		
db_denydatawriter		
db_owner		
db_securityadmin		•
		Canad 1
	UK	Lance

FIG. 29 New User dialog

5. Enter the "DOMAIN\RMSServerMachineName\$" user name and select the login name "DOMAIN\RMSServerMachineName\$" as shown above.



You cannot use the Search button to find this account - it must be manually entered.

- 6. Select the **db\_owner** role under *Database role membership*.
- 7. Click OK to save the user account and permissions to the RMS database.



The db\_owner privilege will grant the DOMAIN\RMSServerMachineName\$ user account full permissions over the RMS database. If you require more restrictive access, please see the DATABASE PERMISSION section of this document for more information.

#### **Additional Online References:**

- [MICROSOFT] How To: Connect to SQL Server Using Windows Authentication in ASP.NET 2.0 http://msdn.microsoft.com/en-us/library/ms998292.aspx
- [MICROSOFT] Explained: Windows Authentication in ASP.NET 2.0 http://msdn.microsoft.com/en-us/library/aa480475.aspx

#### c) RMS Configuration Wizard & RMS Database Wizard

The RMS Configuration Wizard and RMS Database Wizard are executable utilities that run under the context of the logged on user account. When attempting to use these administrative tools for RMS server installation or RMS server maintenance the user should logon with a domain user account that has administrative access to the local RMS server and administrative access to the RMS database.

To create a new RMS database or to perform certain database updates, the logged on user account must have database creator privileges on the SQL server.



See the Database User Permissions section on page 31 for information on the required level of access permissions required for these database user accounts.

Database Authentication

# **Database User Permissions**

## **Overview**



To create and configure the initial RMS database catalog, database administrator privileges are required. If you do not have administrative access to the database server where the RMS will be installed, please consult your IT administration or DBA.

The RMS database catalog may be configured under two security models:

## **Flexible Access**

If you wish to provide for the most flexible access to the RMS database, then each user account associated to the RMS database may be granted "**dbo**" (owner) permissions to the RMS database catalog.

If this option is selected, then the RMS services and web site will be able to read/write/execute stored procedures and alter the database schema. Future RMS upgrades may require database schema and data modification and if the users have owner permissions to the RMS database catalog all database updates can be automated via the RMS Server Installation process.

# **Restrictive Access**

RMS can operate with restrictive access permissions. The minimum database permissions that must be granted to all RMS database user accounts are:

- Read (all Tables)
- Write (all Tables)
- Modify (Table Data)
- Delete (Table Data)
- Execute (all Stored Procedures)

If this option is selected, then the RMS services and web site will be able to read/write and execute all stored procedures. Future RMS upgrades that require database schema and/or data modification may require database administrator access to apply the database update scripts.

The automated database update mechanism built into the RMS Server Installation process may fail to apply the database update scripts if the configured user does not have rights to ALTER/CREATE/DROP, etc.

Database User Permissions

# **Database Installation**

## **Overview**



To create and configure the initial RMS database catalog, database administrator privileges are required. If you do not have administrative access to the database server where the RMS will be installed, consult your IT administration or DBA.

The RMS Configuration Wizard and RMS Database Wizard are executable utilities that run under the context of the logged on user account. When attempting to use these administrative tools for RMS server installation or RMS server maintenance the user should logon with a domain user account that has administrative access to the local RMS server.

During the installation process of RMS on the RMS server, the *RMS Configuration Wizard* will provide the options to connect to an existing RMS database catalog or create a new RMS database (FIG. 30).

Resource Management Suite	e Configuration Wizard
Welcome     Database     Connection     Configuration     Updates     Product Selection     Web Services     Services     Licensing     OS Permissions     System Settings     Finished	Database         Resource Management Suite requires a database connection to continue. Please select from the following options:         Image: Create A New RMS Database         Supported Database Servers:         • Microsoft SQL Server 2000         • Microsoft SQL Server 2005         • Microsoft SQL Server 2005 Express Edition         Image: Opprade An Existing RMS 2.3 (or earlier) Database         Image: Connect To An Existing RMS 3.0 (or later) Database
MX®-	< <u>₿</u> ack <u>N</u> ext> Egit

FIG. 30 RMS Configuration Wizard - Create a New RMS Database

If you have an existing RMS database or your RMS database that was installed manually by the DBA, then select the option to "*Connect To An Existing RMS 3.0 (or later) Database*".

- 1. To create a new RMS database, select Create A New RMS Database.
- **2.** Click **Next** to launch the RMS Database Wizard and display the *Database Wizard Create Microsoft SQL Database* dialog (FIG. 31).

Database Wizard			
<b>Database Wizard</b>			Trace of the second
- Create Microsoft SQL Database			
Microsoft SQL Server			
Asqlexpress			Search
🕥 Use Windows Authentica	tion		
Use SQL Server Authentic	cation		
Username: sa			
Password: ****		1	
New Database Name: (C	atalog)		
RMS			
AMX® -	The second of		1
	< <u>B</u> ack	<u>N</u> ext >	Cancel

FIG. 31 Database Wizard - Create Microsoft SQL Database

- **3.** Enter the **Microsoft SQL Server** path, the preferred database **Authentication** method and **User Credentials** (if needed) and the **New Database Name** (**Catalog**) to create.
  - To successfully create a new RMS database the SQL server database account or if using Windows Authentication, the logged on user domain account, must have database creator privileges on the target SQL server.
  - Without the proper database administrative permission, the RMS database will fail to create a new catalog.
- 4. Select Next to proceed and attempt to create the new RMS database catalog.
- **5.** If a successful connection to the database server is established and the RMS Database Wizard can successfully create the new RMS database catalog, then the installation of the database tables, views, stored procedures, and default data will proceed (FIG. 32).

Database Wizard			
Database Wizard			
Database Structure			
Tables:			
Created 57 of 57 tables [RFII	DTagHistory]		
Views:			
Created 6 of 7 views [view_F	restigeLevels]		
Procedures:			
Created 34 of 227 procedure	s [sp_GetUserd	roupByIDJ	
AMX®			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

FIG. 32 Database Wizard - Database Structure

**6.** Once the database installation is complete, the Database Wizard will close and return you to the RMS Configuration Wizard (FIG. 33).

esource Management Sui	te Configuration Wizard	
Velcome     Detabase     Connection     Configuration     Updates     Product Selection     Web Services	Connected to dat	abase successfully.
Services     Licensing     Of Development	Database Name: Database Version:	RMS 3.0.7 (3/28/2008 12:00:00 PM)
- System Settings	DB Server Name:	Morosoft SQL Server
- Finished	DB SQL Support:	283

FIG. 33 RMS Configuration Wizard - Database Installed & Connected

After installing the RMS database, you may need to create database user account and grant specific permissions access.

- Refer to the *Database Authentication* section on page 5.
- Refer to the *Database User Permissions* section on page 31.

After the database installation is complete, if you need to change the RMS database user account to a more restrictive access account than the one that was used to create the RMS database, then in the RMS Configuration Wizard, select **Configuration** under the *Database* node (FIG. 34).

🔏 Resource Management Su	ite Configuration Wi	zard	
Resource Management Suite	Configuration Wizard	ver Database Connection Set	tings
Welcome     Database     Connection     Updates     Product Selection     Web Services     Services     Services     Services     System Settings     Finished	Database Server: C Use Windows Aut C Use SQL Server A Username: Password: Database Name:	Substance connection occurs      Indexpress     Anentication     Imms     Indexpress     RMS     N	ew Connection
AMX®		< <u>B</u> ack <u>N</u> ext :	Cancel

FIG. 34 RMS Configuration Wizard - Configure SQL Server Database Connection Settings

Here you can change the database user credentials as needed.

When complete, select **Next** to test the database connection using the new credential and to proceed with the RMS server configuration.

# **Manual Database Installation**

## **Overview**

Some corporate database policies require that all database installed to their database servers be manually installed from the database scripts. This is to prevent malicious code from running on the database server.

The default method of installing RMS is by using the automated database installer via the RMS Configuration Wizard, however using the steps outlined below, you can use the existing database scripts to manually install the RMS database.

The RMS database installation scripts are located in the following installation path on the RMS server.

#### C:\Program Files\AMX Resource Management Suite\Database

The two script files used to install the RMS database are:

- **ASPNet.sql** this script installs all the Microsoft ASP.NET application database framework tables and stored procedures.
- **RMSDBInstall.sql** this script installs the RMS application database tables, stored procedures, and default data.

You will need Microsoft SQL Enterprise Management Studio, Microsoft SQL Enterprise Manager, or similar SQL database management tool to create a database and apply these script files.

If you do not already have one of these tools, you can download and install the Microsoft SQL Server Management Studio Express (free edition) directly from the Microsoft web site: <u>http://go.microsoft.com/</u> <u>fwlink/?LinkId=65110</u>

## **Manual Installation Steps**

1. Open the SQL database management tool and establish a connection to the SQL server or SQL cluster to which you wish to install RMS.

You will need to connect using **the** sa account or other user account with database creation and database security management privileges (FIG. 35).

🛃 Connect to Database	Engine 🔳	X		
SQL Serve	Windows Server Syst	tem		
Server <u>ty</u> pe:	Database Engine	~		
<u>S</u> erver name:	<database_server>\<database_instance></database_instance></database_server>	*		
Authentication:	SQL Server Authentication	*		
Login:	sa	*		
Password:	****			
Remember password				
<u>C</u> onnect	Cancel Help Options >>			

FIG. 35 Connect to Database Engine



You may not be prompted to connect to the database server until to attempt to open a SQL script file in the next step depending on the SQL database management tool you are using.

**2.** Open the "**ASPNet.sql**" SQL script file in your SQL database management tool (connect to database here if prompted).

This script file contains a variable placeholder token for the RMS database catalog name.

**3.** Perform a global search and replace on the text:

"!!RMS\$PLACEHOLDER\$2112!!"

Replace this text with the name of the RMS database catalog you with to create.

- The default catalog name typically used is simply **RMS**.
- Make sure to replace all instances of this placeholder token, there are a number of locations in this script file where this placeholder text is embedded.



Replace all instances of this placeholder text with the RMS database catalog name you wish to create for the RMS application.

Find and Replace	X
Quick Find 🔹 🐴 Quick Replace	]-
Find what:	
Replace with:	
RMS	
Current Document	<b>~</b>
Find options	
	Find Next Replace
	Replace <u>A</u> ll

FIG. 36 ASPNet.sql" SQL script file

- **4.** After the database catalog name text replacement is complete, you can execute the script. This should create the new database catalog and then create all the necessary ASP.NET related tables and stored procedures.
  - **a.** When the script is complete, make sure the query was executed successfully and there are no errors.
  - **b.** You may now close this SQL script file.
- **5.** Open the **RMSDBInstall.sql** SQL script file in your SQL database management tool (connect to the same database server using the same logon credentials here if prompted).

You will need to select which database catalog that this script will be applied to.

6. Select the RMS database catalog that was created in the previous steps (FIG. 37).



FIG. 37 "RMSDBInstall.sql" SQL script file (RMS database catalog selected)



# This step is very important. If the wrong database catalog is selected you may potentially inadvertently install a number of RMS tables and stored procedures into another applications database catalog.

**7.** With the appropriate RMS database catalog selected, you can execute this script. When the script query had executed successfully you should not see any errors (FIG. 38).

🗏 Microsoft SQL Server Management S	Studio Express				
<u>Eile E</u> dit <u>V</u> iew Query <u>T</u> ools <u>W</u> indov	v <u>C</u> ommunity <u>H</u> el	lp			
😫 New Query 📑 🚰 🛃 🥵 🖺	) 📴 🦉 🛃				
: 🛒 🛃 📆 RMS -	• 🕴 Execute 🗸	= 19 🖌 🖓 🚏 🖷 🍦			
swdblab\\RMSDBInstall.sql		• ×			
Please ensure these ME	TA directives	remain in the file			
Messages					
Command(s) completed successful	1y.	~			
<u>×</u>					
📀 Query exec swdblab\amxdb (9.0 RTM)	SWDBLAB\rsavage	e (58) RMS 00:00:15 0 rows			
Ready Ln 1	Col 1	Ch 1 NS			

FIG. 38 Execute the "RMSDBInstall.sql" SQL script file

After installing the RMS database, you will need to create database user account and grant specific permissions access to these account. RMS supports both SQL login accounts and Windows Authentication. Refer to the following sections for details on user configuration:

- See the *Database Authentication* section on page 5
- See the Database User Permissions section on page 31

This completes the RMS database installation.

You will now need to run the RMS Configuration Wizard to ensure the database connection is configured properly (FIG. 39).

🔏 Resource Management S	uite Configuration Wiza	ırd	
Resource Management Suite	e Configuration Wizard		Rescarce
Welcome     Database     Connection     Configuration     Updates     Ven Services     Services     Licensing     OS Permissions     System Settings     Finished	Database Connected to d Database Name: Database Version: DB Server Name: DB Server Version: DB SQL Support:	RMS 3.0.7 (3/28/2008) Microsoft SQL Server 09.00.3042 283	
AMX®		< <u>B</u> ack <u>N</u> ext>	E <u>x</u> it

FIG. 39 RMS Configuration Wizard - Connected to database successfully

# **Database Backup**

## **Overview**

The RMS database should be incorporated into your organizations regular backup schedule. All RMS usage and room configuration data is stored in the RMS database. RMS does not provide an automated database backup mechanism; if you do not already have a database backup system in place you should highly consider implementing some form of database backup solution. In the event of server hardware failure or data corruption, all RMS data may be lost without a regular backup.

#### **Additional Online References**

[MICROSOFT] Backing Up and Restoring Databases in SQL Server http://msdn.microsoft.com/en-us/library/ms187048.aspx Database Backup

# Installing SQL Server 2005 Express Edition

## **Overview**

This information is intended to assist you in installing and configuring SQL Server 2005 Express Edition for use with the RMS application.

The Network Administrator should perform this type of configuration.



Resource Management Suite<sup>™</sup> does support Microsoft SQL Express 2005 databases; however, the RMS services and website must connect using a TCP/IP connection or named pipes. Connecting to SQL Express 2005 via shared memory is not supported.

## Installation

- 1. Download the SQL Server 2005 Express Edition (SP1 min.) from Microsoft.
- **2.** Run the SQLEXPR.EXE.
- **3.** Follow the default installation except as follows: In the *Feature Selection* window, select *Client Components > Connectivity Components > Entire feature...*

🕼 Microsoft SQL Server 2005 Express Editi	ion Setup 🛛 🔀			
Feature Selection Select the program features you want installed.				
Click an icon in the following list to change how a feature is installed.				
Database Services     Client Components     Connectivity Components     X      Software Development Kit	<ul> <li>Feature description</li> <li>Installs command line tools, connectivity components, programming models, management tools and development tools.</li> </ul>			
	This feature requires 39 MB on your hard drive. It has 1 of 2 subfeatures selected. The subfeatures require 21 MB on your hard drive.			
Installation path c:\Program Files\Microsoft SQL Server\	Browse Disk Cost			
Help < Back	Next > Cancel			

FIG. 40 Feature Selection

4. Finish the default install.

## Setup

- **1.** Go to *Start > Microsoft SQL Server 2005 > SQL Server Configuration Manager.*
- 2. Go to SQL Server 2005 Network Configuration > Protocols for SQLExpress.

SQL Server Configuration Manager			
File Action View Help			
SQL Server Configuration Manager (Local) SQL Server 2005 Services SQL Server 2005 Network Configuration	Protocol Name	Status	
	Shared Memory	Enabled	
	🐨 Named Pipes	Disabled	
	TCP/IP	Disabled	
T. S. Sor Marine Clienc Configuration	<b>VIA</b>	Disabled	

FIG. 41 SQL Server 2005 Network Configuration

- **3.** Right-click *TCP/IP*; select *Enable*.
- **4.** Go to *SQL Native Client Configuration > Client Protocols*. Ensure *TCP/IP* is enabled. If it is not, right-click *TCP/IP*; select *Enable*.

n SQL Server Configuration Manager				
File Action View Help				
← → 🖻 🗗 🔂 🗟				
SQL Server Configuration Manager (Local) SQL Server 2005 Services SQL Server 2005 Network Configuration Protocols for SQLEXPRESS SQL Native Client Configuration Client Protocols	Name	Order	Enabled	1
	🕉 Shared Memory	1	Enabled	
	TCP/IP	2	Enabled	
	🕉 Named Pipes	3	Enabled	
	AIV C		Disabled	

FIG. 42 SQL Native Client Configuration

**5.** Go to *SQL 2005 Services*.

SQL Server Configuration Manager			
File Action View Help (두 - ) 1일 🖾 😰			
SQL Server Configuration Manager (Local) SQL Server 2005 Services SQL Server 2005 Network Configuration Protocols for SQLEXPRESS SQL Native Client Configuration Client Protocols Aliases	Name	State Stopped Running	Start I Other Auton

FIG. 43 SQL 2005 Services

**6.** Right-click (*SQLEXPRESS*); select *Restart*. After the database has restarted, you may exit the SQL 2005 Configuration Manager.

Installing SQL Server 2005 Express Edition



It's Your World - Take Control™