

IT Administrator's Guide

RMS

Resource Management Suite[®] (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 IT Administrator's Guide1	1
Overview 1	1
Additional Documentation 2	2
System Requirements	2
Minimum Hardware Requirements 2	2
Supported Platforms	2
RMS Supported Databases 2	2
RMS Supported Scheduling and Mailbox Interfaces	3
RMS Supported Web Browsers 3	3
RMS SDK Support	3
Additional System Requirements	3
Network Deployment5	5
Overview5	5
Network Infrastructure5	5
Firewall Considerations ϵ	5
Connection Orientation ϵ	5
IP Addressing / DNS	7
DHCP 8	3
Hosting RMS Web Pages Using a Fully Qualified Hostname	3
Server Components11	1
Overview	1
RMS NT Services11	1
RMS ASP.NET Web Application12	2
RMS Utility / Management Programs12	2
Database15	5
Overview	5
Installation	7
Overview	7
Permissions19	?
Overview	7
Database Permissions	7
NT Services	7
IIS / ASP.NET Permissions 22	2
NTFS Permissions	3
DCOM Permissions 24	1

ii

RMS DCOM Permissions Configuration Utility	. 24
DCOMCNFG.EXE Windows Utility	. 26
HTTPS / SSL	.29
Overview	. 29
Install a SSL Certificate	. 29
Modify the Web URL Setting	. 30
IIS Windows Authentication	31
Overview	. 31
Administrative Web Pages	. 31
User Scheduling Web Pages	. 31
Virtual Server	.35
Overview	. 35
Microsoft Cluster Service	37
Overview	. 37
Installation	. 38
System Backup	.43
Overview	. 43
IPSEC System Security	.45
Overview	. 45
System Security - System Level	. 45
System Level Security - IPSec Security Settings	. 46
Appendix A - Install IIS and Configure ASP.NET for Windows 2003 Server	.47
Overview	. 47
Appendix B - Install IIS and Configure ASP.NET for Windows 2008 Server	.49
Overview	. 49
Server Roles	. 49
Application Server	. 53
Web Server (IIS) Settings	. 54
Confirmation, Progress and Results	. 56
Appendix C - Windows Firewall Exception	59
Overview	. 59
Appendix D - Installation of RMS IIS Virtual Directory in Alternate Path	61
Overview	. 61
Update the RMS Server Internal Configuration For The New Path	. 67
Appendix E - Override the RMS FQDN & Web URL Path	.71
Overview	. 71

Appendix F - Verify the RMS Server Info & Web URL Path	73
Verify the RMS Server Info & Web URL Path	

Table of Contents

RMS IT Administrator's Guide

Overview

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, server access permissions and other important IT related information for the RMS application server installation.

- **1.** RMS must be installed on a Microsoft Windows Server. The list below includes the supported versions of Windows servers.
 - a. Microsoft Windows 2003 Server
 - **b.** Microsoft Windows 2008 Server (32-bit only)



Please consult the RMS Administrator's Guide for a detailed listing of supported platforms and hardware.

2. RMS must be installed on a system with the Microsoft .NET 2.0 framework.



Microsoft Windows Server 2008 includes .NET 2.0 by default.

- **3.** RMS must be installed on a Windows Internet Information Server (IIS). The list below includes the supported versions of Windows IIS.
 - a. IIS 6.0 (Windows 2003 Server)
 - **b.** IIS 7.0 (Windows 2008 Server)



ASP.NET must be enabled on the IIS web server.

4. The RMS database must be installed on a Microsoft SQL server. The list below includes the supported versions of SQL servers.

the RMS server while logged on with an administrative account.

- a. Microsoft SQL Server 2008
- **b.** Microsoft SQL Server 2005



For more information on the RMS database requirements please see the RMS Database Administrator's Guide.

5. 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

NOTE

If running RMS on a system with UAC enabled, such as Windows 2008 Server, each RMS utility will require elevated administrative privileges to run properly.

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 Database Administrators Guide** This document outlines the installation prerequisites, installation guidelines, database access permissions and other important database related information for the RMS database 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 and Mailbox Interfaces

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

Supported Scheduling Systems
Microsoft Exchange
Microsoft Outlook
Lotus Notes
Groupwise
EMS
R25
Peoplecube
Planon



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 IT Administrator's Guide

Network Deployment

Overview

The RMS system is a traditional client-server application where the AMX NetLinx masters are distributed clients that each accesses the central RMS server.

Network Infrastructure

The RMS system communicates over TCP/IP on an Ethernet network.

- The RMS server hosts a listener socket on IANA registered port 3839 for all RMS client communication.
- The RMS server hosts an ASP.NET web-based user interface accessible via HTTP or HTTPS (FIG. 1).



FIG. 1 Network Infrastructure (TCP/IP)

Optionally, the RMS server may be multi-homed allowing user web access on a public network interface and restricting controls system communication to a private network interface (FIG. 2).



FIG. 2 Network Infrastructure (Multi-Homed)

Firewall Considerations

If a firewall exists between the RMS server and the RMS clients (NetLinx Masters), then an Exception (Pinhole) must be created to allow the RMS clients to communicate on Port **3839** to the RMS server. The RMS clients will establish a connection to the RMS server (FIG. 3).



FIG. 3 Firewall Considerations



The RMS default port can be changed from port 3839 to a custom user defined IP port in the RMS Configuration Wizard. However, if this port is changed, each NetLinx master will need to be re-configured to communicate on the new custom IP port.

If Windows Firewall is install and enabled on the RMS server, instructions to add the necessary port exception are provided in *Appendix C* - *Windows Firewall Exception on page 59*.

Connection Orientation

The connection orientation of RMS is that of a client-to-server orientation where the RMS client endpoint is responsible for establishing and maintaining a connection to the centralized RMS server. This connection orientation simplifies network configuration for RMS application communication across network routers, firewalls, and NAT devices. The RMS server never attempts to connect to a client endpoint thus the RMS client system does not publish a service interface or host any server listener sockets (FIG. 4).



FIG. 4 Connection Orientation



There is one exception to this connection orientation rule. In the RMS web user interface a few URL links are provided to initiate manual connections back to the NetLinx master to access the TELNET console and the master's web user interface. This is a user initiated action and the connection is established between the user's computer and the NetLinx master, not between the RMS server and the masters.

IP Addressing / DNS

The RMS server acts as a listener for incoming connection from RMS clients (NetLinx Masters), thus each RMS client must be configured with a resolvable address to reach the RMS server.

The preferred server host addressing scheme is to use a fully qualified domain name to reach the RMS server. This implementation requires that a DNS server exists on the network and that each NetLinx master is configured with the DNS server address.

If a DNS server is available on the network and each NetLinx master is configured to use the DNS server then a fully qualified domain name may be configured on each NetLinx master to access the RMS server (FIG. 5).



FIG. 5 DNS

An alternate method for RMS server host addressing is to configure a static IP address on the RMS server. Each RMS client (NetLinx master) would need to be configured with the static IP address of the RMS server. This method may be required if a DNS server is not available on the network (FIG. 6).





DHCP

DHCP servers are commonly used to simplify IP addressing across networked devices. NetLinx masters support DCHP and can be configured to automatically obtain their IP address, subnet mask, gateway address, and DNS server addresses.

If a DNS resolvable hostname is used on the RMS server allowing the RMS clients (NetLinx masters) to establish a connection to the RMS server without manually configuring a static IP address, then the RMS server may also be configured to use DHCP to obtain its IP address and additional network configuration information.

Hosting RMS Web Pages Using a Fully Qualified Hostname

RMS generates URL links embedded in notification emails to provide convenience links to quick access specific content of interest in the RMS web pages. By default, RMS determines the server hostname using the computer name assigned to the server.

However, in certain cases you may want to expose the RMS server using a public fully qualified domain name or in cases where the computer hostname my not be resolvable by all network workstations. This default behavior can be bypasses allowing you to provide a static fully qualified hostname for the RMS configuration.

The instructions below will configure your RMS server to use a custom/static fully qualified hostname and URL:

1. Open the following folder on your RMS server:

C:\Program Files\AMX Resource Management Suite\Scripts

- 2. Locate the "RMS Hostname.vbs" script file and double-click it to launch it.
- **3.** You will be prompted with the option to reconfigure the RMS hostname. Select **Yes** to continue and override the default detected setting (FIG. 7).

AMX Res	source Management Suite 🛛 🕅
?	The RMS Server is currently configured to use the default system's computer name as the connection hostname. Would you like the change the hostname configuration?

FIG. 7 Reconfigure the RMS Hostname

4. Type in the new fully qualified computer hostname then select OK to save the custom setting (FIG. 8).



FIG. 8 Type the New Fully Qualified Computer Hostname



To return the RMS server to the default behavior where the RMS server auto detects the server hostname, simply type '**auto**' in the text prompt and press **OK**.

5. After completing the hostname change, you will need to restart the RMS services to fully propagate the updated setting (FIG. 9).



FIG. 9 Restart the RMS Services

You can use the **Restart Services** option in the RMS Service Manager utility to restart all the RMS services (FIG. 10).

AMX Resource Management Suite Service	E 🛛	
AMX Resource Management Suite Service Man	nager	
Display Name AMX RMS Server AMX RMS Communications Manager AMX RMS NetLinx Connection Manager AMX RMS Scheduling Manager	State Running Running Running Running	St <u>a</u> rt St <u>op</u> Pause Resume
Start Services Stop Services	<u>R</u> estart Services	Egit

FIG. 10 Restart Services Option In the RMS Service Manager

Once the services have restarted, RMS will now use the override hostname setting for all links and URLs.



To override the entire RMS web application URL, see the instructions in Appendix E - Override the RMS FQDN & Web URL Path on page 71.

Network Deployment

Server Components

Overview

The RMS system consists of the following server components that work cooperatively to provide the RMS solution.

- RMS NT Services
- RMS ASP.NET Web User Interface
- RMS Utility/Management Programs

RMS NT Services

The RMS server implements 4 NT services that each provide distinct features and capabilities to the RMS solution (FIG. 11).

Services		
File Action View		
Services (Local)	Name 🔺	Description
	NET Runtime Optimization Service v2.0.507	Microsoft .NET Framework NGEN
	Rea Alerter	Notifies selected users and computers of administrative alerts. If the service
	AMX RMS Communications Manager	AMX Resource Management Suite Communications Manager
	AMX RMS NetLinx Connection Manager	AMX Resource Management Suite NetLinx Connection Manager
	AMX RMS Scheduling Manager	AMX MeetingManager Appointment Trolling Service
	AMX RMS Server	AMX Resource Management Suite Server
	Application Layer Gateway Service	Provides support for 3rd party protocol plug-ins for Internet Connection Sha

FIG. 11 RMS NT Services

The table below identifies each RMS NT service and provides a description on the function it performs in the RMS system.

RMS NT Services	
Service	Description
AMX RMS Service	This service is the central coordination service that manages system configuration, time synchronization, database connection management, and database maintenance.
AMX RMS NetLinx Connection Manager	This service hosts the TCP/IP server providing connectivity and communication for RMS clients (NetLinx masters).
AMX RMS Communications Manager	This service manages system outbound communication and message delivery to SMTP, SNPP, SYSLOG, and SNMP.
AMX RMS Scheduling Manager	This service manages scheduling synchronization between external scheduling systems and the RMS system.
	If the scheduling feature set is not in use, this service must be enabled and running; however, it will remain mostly idle.



For NT service configuration and permissions, see the Installation section on page 17 and the Permissions section on page 19.

RMS ASP.NET Web Application

The RMS system provides an ASP.NET web based user interface hosted by IIS on the RMS server. The web pages and ASP.NET web application must be installed and hosted on the same server as the RMS NT services. The RMS web user interface must be able to directly communicate with the RMS NT services using DCOM. The RMS ASP.NET web application must also be able to access the RMS database.



If you plan to use Windows Authentication for RMS system database access, please see the RMS Database Administrator's Guide for more information on how to properly setup the RMS ASP.NET web application for database access.

Prior to installing RMS, please ensure that *IIS* and the *Microsoft*.*NET 2.0 Framework* are installed on your Windows server.

For instructions on how to install IIS and configure IIS for ASP.NET, see:

- Windows 2003 Server Appendix A Install IIS and Configure ASP.NET for Windows 2003 Server section on page 47
- Windows 2008 Server Appendix B Install IIS and Configure ASP.NET for Windows 2008 Server section on page 49



For IIS and ASP.NET configuration and permissions, see the Installation section on page 17 and the Permissions section on page 19.

RMS Utility / Management Programs

To aid in the setup and management of the RMS system, several utility programs are provided. These utilities provide system level function to simplify the user configuration and require that the logged on user with Administrator privileges of the RMS server machine.

RMS Utility / Management Programs			
Service	Description		
 RMS Configuration Wizard 	This utility program is run immediately after the installer finishes deploying all the files to the RMS server.		
	This utility guides the user through all the necessary steps to setup the RMS database connection, RMS NT services, RMS ASP.NET web application, permissions, and all RMS configuration option.		
	This utility can be run at anytime to reconfigure the RMS system.		
 RMS Database 	This utility is provided to automate the installation of the RMS database.		
Wizard	This utility is also used to apply database update scripts for system upgrades.		
RMS Service Manager	This utility is provided as a convenience tool to manage the starting and stopping of RMS NT services. This utility can be configured to run in the Windows System Tray and display the current status of the RMS NT services.		
RMS Service	This utility is provided to manually register and un-register the RMS NT services.		
Registration	Typically the service registration is automated during the RMS Configuration Wizard initial setup and thus you may never need to use this tool.		
RMS DCOM Configuration	This utility is provided to manually setup DCOM permissions for the RMS NT services. DCOM permissions are typically automatically assigned during the RMS Configuration Wizard initial setup and thus you may never need to use this tool.		
	There are certain circumstances such as configuration of Windows Authentication where this tool may be used to verify the correct DCOM permissions have been applied.		

The table below identifies each utility included in the RMS installation.

RMS Utility / Management Programs (Cont.)			
Service	Description		
RMS Menu	This utility is provided to serve as a launching menu for the RMS Start Menu shortcuts. This utility is not typically accessed by the user directly.		
Scripts	RMS also includes a number of script files in the SCRIPTS folder under the application installation directory.		
	• These scripts may be used by AMX Technical Support to assist in diagnosing issues in the RMS system.		
	These scripts are not typically accessed by the user without Technical Support.		



Under Windows 2008 server or other operating system supporting UAC, if UAC is enabled, then each RMS Utility program accessed must be run with administrative privileges.

You may be prompted for elevated privileges if not running as the system administrator account.

Server Components

Database

Overview

The RMS system requires a database to warehouse all system information and historical data.

RMS provides automated tools to deploy the RMS database to your database server and to configure the RMS server database connection.

- For a listing of supported database platforms, review the RMS Supported Databases section under the **System Requirements** topic in the *RMS Administrator's Guide*.
- For more detailed information on database installation, database permissions, and database configuration, see the *RMS Database Administrator's Guide*.



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 administrator or DBA. Database

Installation

Overview

The RMS installation package provides an automated setup and deployment of RMS system components, RMS database, and RMS system configuration.

After the installation of the RMS files has completed, the RMS installation will automatically launch the *RMS Configuration Wizard* (this may happen after a reboot, if a reboot is required).

The RMS Configuration Wizard will guide you through the necessary steps to complete the setup and select the specific environmental and personal preferences for the RMS system to operate with.

To be prepared for the RMS installation and configuring the RMS system using the RMS Configuration Wizard it is important to first review the following section in the RMS Administrator's Guide:

- **System Requirements** Please review the system requirements to ensure the target hardware and platform meet the minimum hardware requirements and supported operating system platforms. This section will also identify the supported database platforms, external scheduling systems, and web browsers supported.
- Installation / Installation Checklist The installation checklist will help identify all the necessary configuration information that will be necessary during the initial RMS Configuration Wizard setup process.

For a step-by-step walk through of the RMS Configuration Wizard, review the **Configuration Wizard** section in the *RMS Administrator's Guide*.

Installation

Permissions

Overview

The RMS application requires adequate system permissions in order for all of the components to function properly and work together.

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.



If running RMS on a system with UAC enabled, such as Windows 2008 Server, each RMS utility will require elevated administrative privileges to run properly.

Database Permissions

The RMS database is the central storage mechanism for all RMS system activity, data persistence and historical data archival. All component of the RMS system must have adequate database permissions. This includes the RMS NT services, the ASP.NET web application, and the RMS Utilities.

For more detailed information and configuration instructions for RMS database permissions, see the *RMS Database Administrator's Guide*.

NT Services

The RMS NT services must be configured to run using an unattended login account. By default, the **Local System** account is automatically configured for use by the RMS Configuration Wizard. This built-in system account contains the necessary system access permissions required for the RMS NT services (FIG. 12).

AX RMS S	erver	Propertie	es (Local Con	nputer)	?
General Lo	og On	Recovery	Dependencies	Ĭ-	
Log on as: Local S Allog	iystem <u>w</u> servi	account ce to interac	t with desktop		
<u>○ I</u> his ac	count:				Browse
Passwo	ord:				
Confirm	passw	ord:			
You can er Hardwar	nable o re Profi	r disable this e	s service for the l	hardware prof	iles listed below: Service
Profile 1				E	nabled
				Enable	<u>D</u> isable

FIG. 12 AMX RMS Server Properties (Local Computer)

If attempting to configure the RMS system to use Windows Authentication for RMS database access, then the RMS NT services will need to be configured to use a domain account that has the necessary database permissions and must be assigned to the Administrator's group on the local RMS server (FIG. 13).

AMX RMS Server Prop	erties (Local Computer)	? 🛛		
General Log On Reco	overy Dependencies			
Log on as:				
Local System accou	nt nteract with desktop			
	domain/rms	Browse		
Password:	•••••			
Confirm password:	•••••			
You can enable or disat	ole this service for the hardware p	rofiles listed below:		
Hardware Profile		Service		
Profile 1		Enabled		
Enable Disable				
	OK Canc	el <u>A</u> pply		

FIG. 13 AMX RMS Server Properties (Local Computer) - Domain Account

This will ensure the domain user account used by the RMS services has adequate permissions to the local RMS server's resources as well as the RMS database.



For more detailed information and configuration instructions for RMS windows authenticated database permissions, see the RMS Database Administrator's Guide.

The AMX RMS Scheduling Manager NT service may require a unique user account if integrating the RMS system with an Exchange server.

In order to successfully communicate with the Exchange resource mailboxes, the AMX RMS Scheduling Manager NT service must be configured to **Log On As** a domain account, with read and write permissions to each Exchange resource mailbox displayed in the RMS system.

This domain account must also be assigned permissions to the RMS database.



For more information on configuring RMS with Exchange, see the RMS Exchange Plug-in Guide. • Ideally if using both Windows Authentication for database access and integrating RMS with Exchange, you should try to use the same domain user account for both purposes rather than creating two separate domain user accounts (FIG. 14).

AMX RMS Scheduling	g Manager Properties (Lo	ocal Comp <table-cell> 🔀</table-cell>
General Log On Red	covery Dependencies	
Log on as:		
C Local System acco	unt interact with desktop	
	domain/rms	Browse
Password:	•••••	
Confirm password:	•••••	
You can enable or dise	able this service for the hardwar	e profiles listed below:
Hardware Profile		Service
Profile 1		Enabled
	<u>E</u> nable	<u>D</u> isable
	ОК Са	ancel <u>Apply</u>

FIG. 14 AMX RMS Scheduling Manager Properties (Local Computer)

• If configuring the RMS NT service Log On As user accounts in the RMS Configuration Wizard, note that the drop down listing does not include domain accounts.

However, you can manually type the account in and RMS will accept it as long as the password credentials can be verified (FIG. 15).

	RMS Server Service
using Windows Authe iust configure a "Log (as NT domain / Active re using a SQL Expres s the RMS application without requiring a cust	entication to connect to the RMS Database, then you On As" user account below with a user account that e Directory permissions to the RMS database. If you ss database server installed locally on the same server h, then the "Local System" account should work iom user account.
Log on as:	count
 Ihis account: Password: 	domain/tms

FIG. 15 Register Service

IIS / ASP.NET Permissions

The RMS IIS Virtual directory/application requires Read and Execute (Scripts) Permissions (FIG. 16).

Virtual Directory	- Y	
	Documents	Directory Security
When connecting to thi	is resource, the content should corr	ne from:
0	directory located on this computer	
O A	share located on another compute	er
O A	redirection to a <u>U</u> RL	
Lo <u>c</u> al Path: L: Script source access	s Log visits	BIOMSE
Lo <u>c</u> al Path: L: Scrip <u>t</u> source access V <u>R</u> ead Write	Log visits Index this res	ource
Logal Path: C: Script source access Read Write Directory browsing	: V Log visits Index this res	ource
Logal Path: L: Script source access Bead Write Directory browsing Application Settings	Log visits Index this res	ource
Logal Path: L: Script source access Bead Write Directory browsing Application Settings	E Log visits Index this res	ource
Logal Path: L: Script source access Read Write Directory browsing Application Settings Application name: Starting point:	RMS	ource
Logal Path: L: Script source access Bead Write Directory browsing Application Settings Application name: Starting point:	RMS	Browse ource Remove Configuration
Logal Path: L: Script source access Read Write Directory browsing Application Settings Application name: Starting point: Execute Permissions:	RMS Coefault Web S\RMS Scripts only	Browse ource Remove Configuration

FIG. 16 RMS Properties - Virtual Directory

ASP.NET 2.0 must be installed and enabled as a Web Service Extension (FIG. 17).



FIG. 17 Computer Management - ASP.NET 2.0 Web Service Extension

The setup procedure for this differs between IIS 6 (Windows 2003 server) and IIS 7 (Windows 2008 server). Please see the appropriate section below based on your server operating system:

- Windows 2003 Server Appendix A Install IIS and Configure ASP.NET for Windows 2003 Server on page 47
- Windows 2008 Server Appendix B Install IIS and Configure ASP.NET for Windows 2008 Server on page 49

NTFS Permissions

RMS requires the appropriate NT File System (NTFS) permissions for the RMS components to access files on the RMS server. By default the RMS Configuration Wizard sets all the necessary file permissions automatically. However this section will identify all the minimum required NTFS permissions on the RMS server.

NTFS Permissions	
Path:	C:\Program Files\AMX Resource Management Suite
	(including all files & subfolders)
Minimum Permissions:	FULL CONTROL
Users:	• SYSTEM
	ADMINISTRATORS
Dath.	C:\Program Eiles\AMY Desource Management Suite
raui.	(including all subfolders)
Minimum Permissions:	• READ & EXECUTE
	LIST FOLDER CONTENTS
	• READ
Users:	USERS (Any domain user accounts created for use with RMS)
Deth.	C.\Drawram Eilas\AMX Dessures Management Suite\Config
Path:	C: Program Files VAMX Resource management Suite Coning
Minimum Permissions:	
	• RFAD
	• WRITE
Users:	Any domain user accounts created for use with RMS.
Dath:	C:\Program Eiles\AMY Desource Management Suite\Web
ratii.	(including all subfolders)
Minimum Permissions:	READ & EXECUTE
	LIST FOLDER CONTENTS
	• READ
Users:	NETWORK SERVICE (if account exists)
	ASPNET (if account exists)
D -4	• Any domain user accounts created for use with Rivis.
Path:	C:\Program Files\AMX Resource Management Suite\Web\dynamicResources
Minimum Permissions:	
	READ & EXECUTE
	LIST FOLDER CONTENTS
	• READ
	• WRITE
Users:	NETWORK SERVICE (if account exists)
	ASPNET (if account exists)
	 Any domain user accounts created for use with RMS.

DCOM Permissions

RMS requires appropriate DCOM permissions for inter-process communications between the RMS NT services, the RMS ASP.NET web application and the RMS Utilities.

RMS DCOM Permissions Configuration Utility

By default the *RMS Configuration Wizard* sets all the necessary DCOM permissions automatically. However, a utility tool is provided to verify and set additional DCOM permissions.

1. In the main program directory:

C:\Program Files\AMX Resource Management Suite

Find the **RMSDCOMConfig** utility program, and double click the EXE file to start the utility. The utility will list all the known accounts that RMS needs to have DCOM permissions set for (FIG. 18).

AMX Re	source Management Suite Service Registration
IX Resou	rce Management Suite DCOM Permissions Configuration Utility
	This utility program will automatically configure the proper DCOM permissions configuration settings neccessary for the RMS application.
	✓ IUSR_ <machine_name> </machine_name>
	View Permissions Grant Permissions Remove Permissions
<®	Back Esit

FIG. 18 AMX Resource Management Suite Service Registration

- If you need to add an additional user account, use the Add button and enter the account username.
- If configuring any domain accounts for use with the RMS NT services such as the case with Windows authenticated database connections, please add the domain user account to the listing.

2. Select **View Permissions** to view the current assigned DCOM permissions for each RMS NT service (FIG. 19).

AMX Resource Management Suite Ser	vice Registration	E 🛛
AMX Resource Management Suite DCOM Pe	rmissions Configuration Utility	
Getting DCOM permissions for RMSServer RMSNetLinx	user: SYSTEM : [Permission Set] : [Permission Set]	
RMSTroller RMSComm 	: [Permission Set] : [Permission Set] user: NETWORK SERVICE	
RMSServer RMSNetLinx RMSTroller RMSComm	: [Permission Set] : [Permission Set] : [Permission Set] : [Permission Set]	
Getting DCOM permissions for RMSServer RMSNetLinx RMSTroller DMSComm	user: Administrators : [Permission Set] : [Permission Set] : [Permission Set]	Titi
Getting DCOM permissions for RMSServer RMSSNetLinx RMSTroller	user: INTERACTIVE : [Permission Set] : [Permission Set] : [Permission Set]	
AMX®	: [Permission Set]	Exit

FIG. 19 AMX Resource Management Suite Service Registration - View Permissions

- **3.** Click **Back** to return to the main menu.
- **4.** If any permissions are missing and need to be assigned, select **Grant Permissions** to assign the necessary DCOM permissions to each user account for each RMS NT service (FIG. 20).

AMX Resource Management Suite Service Registration	
AMX Resource Management Suite DCOM Permissions Configuration Utility	
Setting DCOM permissions for user: SYSTEM RMSServer : [Granted]	
RMSNetLinx : [Granted] RMSTroller : [Granted] RMSComm : [Granted]	
Setting DCOM permissions for user: NETWORK SERVICE RMSServer : [Granted] RMSNetLinx : [Granted] RMSTroller : [Granted]	
RMSComm : [Granted] 	
RMSNetLinx : [Granted] RMSTroller : [Granted] RMSComm : [Granted]	I
Setting DCOM permissions for user: INTERACTIVE RMSServer : [Granted] RMSNetLinx : [Granted]	
RMSComm : [Granted]	⊻
AMX®Back	Exit

FIG. 20 AMX Resource Management Suite Service Registration - Grant Permissions

5. Once all the DCOM permissions are assigned, click Exit to exit the RMS DCOM configuration utility.

DCOMCNFG.EXE Windows Utility

If you prefer to view or manage the DCOM permissions directly without using the RMS DCOM Configuration utility, you can launch the "**dcomenfg.exe**" Windows utility from the **Start > Run** command tool (FIG. 21).

Run		?
	Type the name of a program, folder, document, o Internet resource, and Windows will open it for y	or ou.
Open:	dcomcnfg	
	OK Cancel Brov	vse

FIG. 21 Run dcomcnfg

- In the Component Services tool, navigate to: My Computer > DCOM Config > RMSServer
- 2. Right-click and select Properties (FIG. 22).



FIG. 22 Component Services - RMS Server - Properties

3. Select the *Security* tab and select the **Edit** button under the *Launch and Activation Permissions* section (FIG. 23).

MSServ	er Prope	rties			?
General	Location	Security	Endpoints	Identity	
Lau	inch and A	ctivation Pe	ermissions		
C	<u>U</u> se Defau	alt			
۲	Customize				Edit
Acc	ess Permis	sions			
۲	Use De <u>f</u> au	ılt			
С	Custo <u>m</u> ize				E <u>d</u> it
	at as				
Cor	nfiguration F	Permissions			
C	Use Defa <u>u</u>	ilt			
	Customize				Edit
		(OK	Ca	incel Apply

- FIG. 23 RMS Server Properties Security
- 4. Select each desired user account and set the Allow attribute for each permissions (FIG. 24).

Permissions



FIG. 24 Launch Permissions - Allow

You can apply the DCOM permissions in this manner for each of the RMS NT services.

HTTPS / SSL

Overview

RMS supports hosting the RMS web application under HTTPS using a secure SSL certificate:

Install a SSL Certificate

1. In the *RMS IIS Virtual Directory Properties* dialog (*Directory Security* tab), select the **Server Certificate** button to install a SSL certificate for this web application (FIG. 25).

HTTP Headers		Custom Errors		P.NET	Server Extensions	
Web Site	ISAPI Filt	ers Home Dire	ctory	Documents	Directory Security	
Anonymou	s access an	d authentication co	ntrol			
	Enable a	nonymous access a	nd edit th	e		
1	authentic	ation methods for th	his resource	ce.	<u>E</u> dit	
 IP address 	and domain	name restrictions				
	Grant or o	deny access to this uses or internet dom	resource	using		
	11 000100	www.serie.com	an munu			
					Edjt	
- Secure co	mmunication	10				
occure con	Bequire s	ecure communicati	ons and	_		
	enable cl	enable client certificates when this		Server	r Certificate	
	resource	is accessed.		⊻iew	Certificate	
					Edit	

FIG. 25 Default Web Site Properties

2. To restrict all access to the RMS web pages to only allow HTTPS secure communication, then also select the **Edit** button and place a check in the *Require secure channel (SSL)* checkbox (FIG. 26).



FIG. 26 Secure Communications

3. Press **OK** to apply the setting.

Modify the Web URL Setting

Next, for RMS to correctly render URLs with the HTTPS protocol prefix in notification messages, the web URL setting in the RMS configuration need to be modified:

- 1. Follow the instructions in Appendix E Override the RMS FQDN & Web URL Path on page 71.
- **2.** However, when prompted for the new fully qualified URL path, make sure to change the URL string from "http://" to "https://" (FIG. 27).

AMX Resource Management Suite	E 🛛
Please enter the desired fully qualified RMS web URL: (i.e. http://rms.company.com/apps/ams/RMS) (Please Note: this path should include the 'http://' or 'https://' header and fully qualified server hostname) Type 'auto' to configure RMS to use the auto detected web URL	OK Clo Cancel
https://server/rms	

FIG. 27 Enter Fully Qualified RMS Web URL Path
IIS Windows Authentication

Overview

RMS supports Integrated Windows Authentication for the ASP.NET web application. The RMS services will automatically detect if the RMS web application virtual directory is configured for Integrated Windows Authentication and apply the following behavior:

Administrative Web Pages

In the RMS administrative web pages, when a request is received, the web application will auto detect the integrated windows username and attempt to authenticate this user account to a user account defined in the RMS database.

- If the username is defined in the RMS database, the user is automatically logged on and the user's security permissions are applied to the user's session.
- If the integrated windows username is not found in the RMS database, a login prompt will be provided to manually log on to the RMS administrative pages.
- If using Integrated Windows Authentication, the user's password in the RMS database need not be synchronized with the actual domain account, this password will not be used in the authentication process.

User Scheduling Web Pages

In the RMS user scheduling web pages, the web application will auto detect the integrated windows username and only allow appointment record modification to appointment records that the user is the organizer of. Attempting to access or modify an appointment created by another user will be restricted.

The integrated windows usernames need not be defined in the RMS database. The web application will simply restrict access to appointments based on the appointments organizer.



As of RMS version 3.0, the Microsoft Exchange scheduling plug-in supports the population of the organizer username field in the appointment record.

To enable Integrated Windows Authentication, after the RMS product installation and completion of the RMS Configuration Wizard:

- 1. Open the IIS manager from Control Panel / Administrative Tools / Internet Information Services.
- 2. Expand the Web Sites and navigate to the RMS web application (FIG. 28).



FIG. 28 Internet Information Services - RMS

- 3. Right-click on the RMS web application and select Properties.
- **4.** Select the **Directory Security** tab and click the **Edit** button under *Anonymous access and authentication control* (FIG. 29).

HIIP	Headers	Custom Errors	ASP.NET
Virtual [Directory	Documents	Directory Security
nonymou	s access and auth	entication control	
\$	Enable anonym authentication r	ous access and edit the nethods for this resource	<u>E</u> dt
address	and domain name	restrictions	~~~
8	Grant or deny a IP addresses or	ccess to this resource usin internet domain names.	g
			Edjt
ecure cor	nmunications		
-	Require secure	communications and	Server Certificate
-0	resource is acc	essed.	View Certificate
			Edit
			8

FIG. 29 RMS3 Properties - Directory Security tab

5. Ensure the **Anonymous access** option is disabled and the **Integrated Windows authentication** option is enabled (FIG. 30).

Authenticatio	on Methods				×
	us access				J.
No user nam	erpassword re	quired to acc	cess this resol	irce.	
Account use	d for anonymo	us access:			
<u>U</u> ser name:	IUSR_RMSS	SERVER	î	Browse	
Password:					
	Allow IIS	to control pa	ssword		
Authenticate	daccess				5
For the follow are required - and - act	ing authentica when onymous acce cess is restricte	ation methods ss is disabled ed using NTF	s, user name a I, or S access con	and password itrol lists	
🗌 Djgest au	thentication fo	r Windows d	omain servers		
🔲 Ba <u>s</u> ic aut	hentication (pa	assword is se	nt in clear text	t)	
Default <u>d</u> o	main:			Seject	
<u>R</u> ealm:	A	ΛX		S <u>e</u> lect	
Integrated	d Windows au	thentication	>		
	OK	Cancel		lelp	

FIG. 30 Authentication Methods

6. When done, press OK to save the configuration.

After making these changes, you will need to reset the IIS web application to ensure the new settings are applied:

1. Select the Run option form the Windows start menu and type "IISRESET" and click OK (FIG. 31).

Run	? 🛛
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	iisreset 💌
	OK Cancel Browse

FIG. 31 Run - iisreset

2. After the *IISRESET* process is completed, you will be able to access the RMS web pages using *Integrated Windows Authentication*.



If the RMS server is additionally configured to use Windows Authentication for database access, a specialized machine account must be added to the SQL server. See the RMS Database Administrator's Guide for more information.

To ensure that RMS is properly detecting the Integrated Windows Authentication settings, a script had been included in the RMS Scripts directory:

C:\Program Files\AMX Resource Management Suite\Scripts\ RMS IIS Integrated Windows Authentication.vbs

- 1. Simply double-click the script file RMS IIS Integrated Windows Authentication.vbs to execute it.
- **2.** A message prompt displays the detected state for RMS using Integrated Windows Authentication in the RMS web application (FIG. 32).

RMS Sei	rver Info	×
•	RMS Server detection for Integrated Windows Authentication of the RMS IIS Virtual Direct RMS configured for Integrated Windows Authentication True This value will only return 'TRUE' if 1.) User Account Managment is <enabled> in RMS (Currently Enabled=True) 2.) Integrated Windows Authentication is <enabled> on the RMS Virtual Directory in IIS 3.) Anonymous Access is <disabled> on the RMS Virtual Directory in IIS OK</disabled></enabled></enabled>	ory :

Virtual Server

Overview

The RMS system can be deployed using virtualization on an instance of virtual server.

RMS has been tested using VMWare Server.

The most critical item to ensure is that RMS clients (NetLinx masters) can successfully connect to port **3839** on the virtual network interface.



If the virtual service instance is deployed on a virtual hard disk, there are certain circumstances such as migrating to a new virtual hard drive that may prevent the RMS licensing from being detected properly. Please contact AMX Technical Support to assist in resolving any licensing issues.

Virtual Server

Microsoft Cluster Service

Overview

The RMS system can be deployed on Microsoft Clustered servers to provide a high-availability, redundant solution. MSCS failover capability is achieved through redundancy across the multiple connected machines in the cluster, each with independent failure states.

Redundancy requires that RMS be installed on multiple servers within the cluster. However, RMS is online on only one node at any point in time. As that application fails, or that server is taken down, RMS services are restarted on another node.

Each node has its own memory, system disk, operating system and subset of the cluster's resources. Each node is required to utilize a shared drive which contains the RMS database and licensing. If a node fails, the other node takes ownership of the failed node's resources (this process is known as "failover").



RMS supports Microsoft failover clustering. This does not imply support of load balancing, web farms, etc.

FIG. 33 provides an example of a Clustered File Server:



Network

Administrator

FIG. 33 Clustered File Server

Cluster storage

Clients

Installation

In order to setup RMS for cluster support, it must first be installed on all nodes of the cluster. Once all nodes have RMS installed and configured, you need to have access to the Cluster Administrator application on the active node.

Server and Client licenses are applied to the first node only; each additional node will utilize the licensing stored on the shared drive.

1. Open the **Cluster Administrator** application and select the desired Group under which you want to setup the RMS Services (FIG. 34).

Gluster Administrator - [RMSDE gi Elle View Window Help	VCLUSTER (rmsdevcluster)]					
	Name	State	Owper	Resource Type	Description	
Groups Groups Cluster Group Cluster Configuration RMSDEV1 Active Resources Network Interfaces MNSDEV2 Active Groups Active Groups Active Groups Active Resources Network Interfaces	Disk F: MSDTC IP Address RSDTC SQL IP Address RSDTC SQL IP Address 1 (RMSDEVSQL) SQL Network Name (RMSDEVSQL) SQL Server SQL Server Agent SQL Server FILESTREAM share (MS	Online Online Online Online Online Online Online Online	RMSDEV2 RMSDEV2 RMSDEV2 RMSDEV2 RMSDEV2 RMSDEV2 RMSDEV2 RMSDEV2 RMSDEV2 RMSDEV2	Physical Disk Distributed Tra IP Address Network Name IP Address Network Name SQL Server SQL Server SQL Server Agent File Share		
For Help, press F1					NUM	1.

FIG. 34 Cluster Administrator

- 2. Create a new Resource in the desired Group by selecting *File* > *New* > *Resource*.
- **3.** RMS will need four Generic Service resources created for the cluster. The first Resource is for the **RMS Server** service (FIG. 35).

New Resource	Name: Description: Resource type: Group: Image: To continue, click	rver RMSServer RMSServer Service Group 0 Group 0 urce in a separate Resource Moni	itor
	<	<u>B</u> ack <u>N</u> ext≻ (Cancel

FIG. 35 New Resource

- 4. Enter a Name and Description for the resource and select Generic Service for the Resource Type.
- 5. Click Next to verify and/or add additional cluster nodes as Possible Owners of the resource (FIG. 36).

yecily the possible ⊻ailable nodes:	Owners for this re	source.	Possible owners:	
Name		<u>A</u> dd⇒ <- <u>R</u> emove	Name RMSDEV1 RMSDEV2	

FIG. 36 Possible Owners

6. Click Next to enter the Dependencies (FIG. 37).

- For RMS Server, the only dependency should be the SQL Server if it resides in the same cluster.
- If the SQL Server does not reside on this cluster then there should be no dependency.

Specify the dependencies for Available resources:	or this resou	Irce.	Besource dependencir	×¢.
Resource	B 🔺		Resource	Res
MSDTC MSDTC IP Address RMSDEVMSDTC SQL IP Address 1 (SQL Network Nam SQL Server Agent SQL Server FILEST	D IF N F F	Add > <- <u>R</u> emove	SQL Server	SQL

FIG. 37 Dependencies

7. Click Next to enter the Service Parameters (FIG. 38).

eneric Service Pa	rameters ver			
<u>S</u> ervice name:	RMSServer			
Start parameters:				
I Use Network	Name for compute	er name		
		< <u>B</u> ack	<u>N</u> ext >	Cancel

FIG. 38 Generic Service Parameters

The *Service name* should be the same as the service executable (*RMSServer* in this case) and there are no startup parameters.

8. Click Next to view Registry Replication, which is not necessary for RMS Service resources (FIG. 39).

Registry Replication			
RMSServer			
Programs or services may store data data available on the node on which HKEY_LOCAL_MACHINE that shou	in the registry. The they are running. ! Id be replicated to	refore, it is import Specify the regist all nodes in the c	ant to have this ry keys below luster.
Root Registry Key			
	Add	Modify	Bemove
	< <u>B</u> ack	Finish	Cancel

FIG. 39 Registry Replication

9. Clicking **Finish** returns you to the *Cluster Administrator* (FIG. 40), where you can add the remaining three services (*RMSComm, RMSNetlinx* and *RMSTroller*).

			22		1. W-	
RMSDEVCLUSTER	Name	State	Owner	Resource Type	Description	9
🗄 🦲 Groups	SQL Server FILESTREAM share (MS	Online	RM5DEV2	File Share		
Cluster Group	SQL Server Agent	Online	RMSDEV2	SQL Server Agent		
Group 0	SQL Server	Online	RMSDEV2	SQL Server		
Resources	SQL Network Name (RMSDEVSQL)	Online	RM5DEV2	Network Name		
E Dister Configuration	SQL IP Address 1 (RMSDEVSQL)	Online	RMSDEV2	IP Address		
Active Groups	C RMSDEVMSDTC	Online	RMSDEV2	Network Name		
Active Resources	MSDTC IP Address	Online	RM5DEV2	IP Address		
Network Interfaces	MSDTC .	Online	RMSDEV2	Distributed Tra		
RMSDEV2	Disk F:	Online	RMSDEV2	Physical Disk	a martin martin and	
Active Groups	RM5 Scheduling Manager	Offline	RMSDEV2	Generic Service	RMS Scheduling Communications	
- Active Resources	CORMS Server	Offline	RMSDEV2	Generic Service	RMS Server Service	
- Network Interfaces	RM5 NetLinx Connection Manager	Offline	RMSDEV2	Generic Service	RMS Netlinx Communication 5	
	RMS Communication Manager	Offline	RMSDEV2	Generic Service	RMS Outbound Communications	

FIG. 40 Cluster Administrator

Microsoft Cluster Service

System Backup

Overview

The RMS server should be incorporated into your organization's regular backup schedule. In particular, 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.

System Backup

IPSEC System Security

Overview

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.

IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPSec can be used to protect data flows between the RMS server and each NetLinx System.

This section describes setup for NetLinx systems. For more information, refer to the Web Console & Programming Guide for NI Series NetLinx Integrated Controllers.

System Security - System Level

System Level Security options provide authorized users the ability to alter the current security options of the entire system assigned to the Master.

There are two System Level Security pages, accessible via the **System Security Settings** and **Security Settings** links in the *System Level* tab (FIG. 41):

rstem Level		System Level	up Level 📔 User Levi
PSec Security Details Modify IPSec security settings for the Master	s	system Security Setting	gs IPSec Security Settin
Configure IPSec Settings	Manage Certific	cate Files	
Enabled	Certificates	CA Certificates	CRL Certificates
No CRL Checking CRL Checking CRL Checking (All) Update Settings			Delete File
Upload Configuration File Browse Submit	Upload Certificat	e File Bro	wse Submit

FIG. 41 System Level Security



The **Security Settings** option is only available on the NI-700/900 and NI-X100 series.

System Level Security - IPSec Security Settings

Click the IPSec Security Settings link to access the *IPSec Security Details* page. The options in this page allow you configure IPSec-specific security options on the Master at the System level (FIG. 42).

stem Level	5	System Level Gro	up Level 🔰 User Level
Sec Security Details odify IPSec security settings for the Master	S	ystem Sepurity Setting	IPSec Security Setting
Configure IPSec Settings	Manage Certific	ate Files	
🗖 Enabled	Certificates	CA Certificates	CRL Certificates
 No CRL Checking CRL Checking CRL Checking (All) Update Settings 	Select a file to de Cert1 demoCA cert1 demoCA new.cert.pem new.key.pem	elete. 3subCA1.key.pem 3subCA1.cert.pem	Detete File
Jpload Configuration File Browse Submit		Bro	wse Submit

FIG. 42 System Level Security - IPSec Security Settings

- The Enabled checkbox turns "on" and "off" the entire IPSec feature.
- The **CRL** radio buttons indicate the level of Certificate Revocation List checking that is performed for IPSec connections. **CRL Checking** checks the sources certificate while **CRL Checking** (All) checks all of the certificates in a sources certificate chain.

If either **CRL Checking** or **CRL Checking** (**All**) are selected, then at least one certificate must be present in the CRL Certificates directory on the Master.

• The *Upload Configuration File* section provides the capability to upload the IPSec Config file onto a Master.

Simply browse to the file's location on a PC, select the file, and select **Submit**. The file will be uploaded to its proper location on the Master.

There is no "delete" capability for the Config file. New uploads overwrite the existing Config file.

• The **Certificates**, **CA Certificates** and **CRL Certificates** sub-pages provide the ability to upload certificates, certificate authority certificates and certificate revocation list certificates respectively onto the Master.

Simply browse to the location of the certificate data on the PC, select the file and select **Submit**. The selected file will be uploaded to the appropriate directory on the Master.

To delete a certificate file, simply select the desired file and select **Delete**. This will cause the file to be removed from the Master.

Appendix A - Install IIS and Configure ASP.NET for Windows 2003 Server

Overview

In Windows 2003 server, IIS can be installed using the Add / Remove Programs option in the Control Panel:

1. Select the Add/Remove Windows Components option (FIG. 43).



FIG. 43 Add or Remove Programs

2. Select the Application Service option and press the Details button (FIG. 44):



FIG. 44 Windows Components Wizard

3. In the Application Server dialog, select ASP.NET and Internet Information Services (IIS) (FIG. 45).



FIG. 45 Application Server

4. After installing IIS, next, ensure the ASP.NET 2.0 web service extension is enabled (allowed): Under Administrative Tools / Computer Management, navigate to:

Services and Applications > Internet Information Services > Web Service Extensions (FIG. 46).



FIG. 46 Computer Management

Appendix B - Install IIS and Configure ASP.NET for Windows 2008 Server

Overview

In Windows 2008 server, IIS can be installed using the Server Manager utility under Administrative Tools:

Server Roles

1. Select the Roles item, then select Add Roles (FIG. 47).

Server Manager		
Ele Action View Help		
🗢 🔿 🖄 🛅 🔛		
Server Manager (VM)	Roles	
File Services Hyper-V Fint Services Frint Services Features Diagnostics	View the health of the roles inst roles and features.	alled on your server and add or remove
Configuration Storage	Roles: 3 of 18 installed File Services	Add Roles
	Print Services	

FIG. 47 Server Manager (Roles > Add Roles)

2. Select Next to continue (FIG. 48).



FIG. 48 Add Roles Wizard - Before You Begin

3. Select the **Web Server (IIS)** role (FIG. 49).

Select Serv	er koles	
efore You Begin erver Roles onfirmation rogress esults	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Domain Services Active Directory Edytweight Directory Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DHCP Server DHCP Server DHCP Server DHCP Server Bit Services DHCP Server DHCP Server Services DHCP Server DHCP Server DH	Description: Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
		L3
	More about server roles	

FIG. 49 Add Roles Wizard - Server Roles

4. The Web Server (IIS) Role requires certain features to additionally be installed on the server. When prompted, select the **Add Required Features** option (FIG. 50).

afore You Benin				
Server Roles	Select one or more roles to install o Roles:	n this server.	Description:	
Confirmation Progress	Active Directory Certificate Se	rvices :es	Active Directory Certificate Service (AD_CS) is used to create certificati authorities and related role service	a ion s
Add Roles Wizard			x manag	e
	Process Model Configuration APIs	Add Beoured	Process model, removing HTTP, All the features	
(i) Why are the	e features required?		<i>li</i>	
Why are the	te features required?			

FIG. 50 Add Roles Wizard - Select Server Roles - Add Required Features

5. Select the Application Server role (FIG. 51).

efore You Begin	Select one or more roles to install on this server.	
lerver koles Web Server (IIS) Role Services Joinfirmation Togress Jesuits	Active Directory Certificate Services Active Directory Domain Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DHCP Server DHS Server Fax Server Pile Services Detrory Roley and Access Services Print Services Command Services Vebork Policy and Access Services Print Services Veb Server (IIS) Windows Deployment Services	Application Server provides central management and hosting of high- performance distributed business applications such as those built with Enterprise Services and .NET Framework 3.0.
	More about server roles	

FIG. 51 Add Roles Wizard - Select Server Roles (Application Server)

6. The **Application Server Role** requires certain features to additionally be installed on the server. When prompted, select the **Add Required Features** option (FIG. 52).

erver Roles	Select one or more roles to insta Roles:	all on this server.	Description:
Veb Server (IIS)	Active Directory Certificate	Services	Application Server provides central management and hosting of high-
Role Serv Add Rol	es Wizard		× siness
	INET Framework 3.0 Features INET Framework 3.0 Windows Process Activation Service INET Environment	Microsoft NET Fran power of the NET F new technologies fo that offer appealing your customers' per Add Required	mework 3.0 combines the ramework 2.0 APIs with to building applications user interfaces, protect resonal identity informatio Features Cancel
() V	hy are these features required?	(}	

FIG. 52 Add Roles Wizard - Select Server Roles - Add Required Features for Application Server

Sefore You Begin	Select one or more roles to install on this server.	_
pplication Server Role Services Veb Server (IIS) Role Services Confirmation Yrogress Lesuits	Active Directory Certificate Services Active Directory Domain Services Active Directory Pederation Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DirS Server DirS Server DirS Server Ris Services Network Policy and Access Services Print Services Terminal Services Windows Deployment Services	Application Server provides central management and hosting of high- performance distributed business applications such as those built with Enterprise Services and .NET Framework 3.0.

7. With both the Application Server and Web Server (IIS) roles selected, click Next to continue (FIG. 53).

FIG. 53 Add Roles Wizard - Select Server Roles (Application Server & Web Server selected)

8. Select Next to continue to Application Server (FIG. 54).

Before You Begin Introduction to Application Server Server Roles Application Server hosts and centrally manages applications that interoperate with systems on the network as heterogeneous databases, identity management services, security systems, and Web applications are relieved application Server is such as the .NET Framework 3.0, COM+, Web Server (IIS) Support, and Message Queuing. Web Services Things to Note Confirmation Installing Application Server installs the .NET Framework 3.0 by default. Progress Installing Application Server Results Additional Information Overview of Application Server Role Services. Application Server Role Services. Application Server Role Service Additional Information Overview of Application Server Configurations Application Server Role Services. Application Server Role Services Application Server Role Services. Additional Information Overview of Application Server Operation Server Role Services Application Server Configurations	Application Serve	er
-2	efore You Begin erver Roles pplication Server Role Services Veb Server (IIS) Role Services ionfirmation rogress esults	Introduction to Application Server Application Server hosts and centrally manages applications that interoperate with systems on the network such as heterogeneous databases, identity management services, security systems, and Web applications and services, security systems, and Web applications and services, sepolication Server also support developing Lucture Dusiness applications through integrated services such as the .NET Framework 3.0, COM+, Web Server (IIS) Support, and Message Queuing. Things to Note Installing Application Server installs the .NET Framework 3.0 by default. We recommend that you install Web Server (IIS) Support if you plan to host distributed applications built using ASP.NET or Windows Communication Foundation (WCF). Additional Information Overview of Application Server Application Server Role Services Application Server Configurations
		μ,

FIG. 54 Add Roles Wizard - Application Server

Application Server

1. Add the COM+ Network Access option (FIG. 55). Select Next to continue.

efore You Begin erver Roles pplication Server Role Services /eb Server (IIS) Role Services onfirmation roorress	Select the role services to install for Application Server: Role services: Application Server Foundation Web Server (IIS) Support COM + Network Access TCP Port Sharing Windows Process Activation Service Support Message Queuing Activation Message Queuing Activation	Description: <u>CON4- Network Access</u> enables Application Server to host and allow remote invocation of applications built with CON4- or Enterprise Services components.
esults	IC-Activation Named Pipes Activation Distributed Transactions Outpoing Remote Transactions WS-Atomic Transactions WS-Atomic Transactions	
	More about role services	

FIG. 55 Add Roles Wizard - Application Server > Role Services

2. Make sure all of the following options are selected (FIG. 56).



FIG. 56 Add Roles Wizard - Application Server > Role Services selections

3. Click **Next** to continue to *Web Server (IIS)*.

Web Server (IIS) Settings

1. After completing the Application Role Services, the **Web Server (IIS)** Roles Services installation will begin (FIG. 57).

Ē	Add Roles Wizard		×	ĸ
	Web Server (IIS)			
	Before You Begin Server Roles Application Server Role Services Web Services Confirmation Progress Results	Introduction to Web Server (IIS) Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIB 7.0 also features enhanced security, simplified diagnostics, and delegated administration. Things to Note Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic especially when there are multiple roles on this computer. The default installation for the Web Server (IIS) role includes the installation of role services that enable you to service static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression. Additional Information Overview of Web Server (IIS) Overview of Web Server (IIS) Overview of Available Role Services in TIS 7.0 Overview of WSRM Common Administrative Tasks in TIS		
_		< <p>< Previous</p> Next > Tristall Cancel		-
~	Start	al Configuration T	6 AM	ī

FIG. 57 Add Roles Wizard - Web Server (IIS)

- 2. Make sure all options under Common HTTP Features are selected.
- **3.** Make sure the following options under **Application Development** are selected (FIG. 58).
 - ASP.NET
 - .NET Extensibility
 - ASP
 - ISAP Extensions
 - ISAPI Filters

Before You Begin Server Roles	Select the role services to install for Web Server (IIS): Role services:	1	Description:
Application Server Role Services Web Server (IIS) Role Services Confirmation Progress Results	Web Server Vest Common HTTP Features Static Content Default Document Default Document Directory Browsing HTTP Redirection Application Development Application Dev		Active Server Pages (ASP) provides a server side scripting environment for building Web sites and Web applications. Offering improved performance over CGI scripts, ASP provides IIS with native support for both VBScript and Script. USe ASP if you have existing applications that development, consider using ASP.NET.
	More about role services	-	

FIG. 58 Add Roles Wizard - Web Server (IIS) (Application Development)

- 4. Make sure all options under Security are selected.
- 5. Make sure all options under IIS 6 Management Compatibility are selected (FIG. 59).



FIG. 59 Add Roles Wizard - Web Server (IIS) (Security, IIS 6 Management Compatibility)

6. Click Next to continue to *Confirmation*.

Confirmation, Progress and Results

1. A final confirmation dialog is displayed before starting the installation of server roles and role services (FIG. 60).

efore You Begin erver Roles pplication Server	To install the following roles, role services, or features, click Install. (i) 2 informational messages below	
Role Services /eb Server (IIS)	This server might need to be restarted after the installation completes. Application Server	-
Role Services onfirmation rogress	Application Server Foundation Web Server (IIS) Support COM+ Network Access Windows Process Activation Service Support	
606	Web Server (IIS) Jo Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage	
	Web Server Common HTTP Features Static Content Default Document Directory Browsing	
	HTTP Errors HTTP Redirection Application Development ASP NET	-
	Print, e-mail, or save this information	

FIG. 60 Add Roles Wizard - Confirmation

2. Click **Next** to continue. The installation of server roles and roles services may take several minutes (FIG. 61).

Add Roles Wizard		×
Installation Prog	ress	
Before You Begin	The following roles, role services, or features are being installed:	-
Server Roles	Application Server	
Application Server Role Services	Web Server (IIS)	
Web Server (IIS)	.NET Framework 3.0 Features	
Role Services	Windows Process Activation Service	
Confirmation		
Progress		
Results		
		-
	-	
	Gamma Initializing Installation	
_	A	
	< Previous / Vext > Install	Cancel
灯 Start 🛛 🚠 📰 🖉 Init	ial Configuration T	🕄 🏠 11:47 AM

FIG. 61 Add Roles Wizard - Progress

3. When the installation of server roles and roles services is complete, a dialog is displayed indicating *"installation succeeded"* for both **Application Server** and **Web Server (IIS)** (FIG. 62).

	tesuits	
Before You Begin Server Roles Application Server	The following roles, role services, or fea	stures were installed successfully:
Role Services Web Server (IIS)	Windows automatic updating is Control Panel to check for upda	not enabled. To install the latest updates, use Windows Update in tes.
Role Services Confirmation Progress Results	The following role services were inst Application Server Foundation Web Server (IIS) Support COM+ Network Access Windows Process Activation Se HTTP Activation	alled: revice Support
	Web Server (IIS) The following role services were insi Web Server Common HTTP Features Static Content Default Document Directory Browsing HTTP Errors HTTP Redirection	Installation succeeded aled:
	Print, e-mail, or save the installation rep	ent

FIG. 62 Add Roles Wizard - Results

4. Click Close to complete this step.

Appendix B - Install IIS and Configure ASP.NET for Windows 2008 Server

Appendix C - Windows Firewall Exception

Overview

If Windows Firewall is enabled on your server, then an exception to permit NetLinx communication to the server must be added.



The screenshots below are from a Windows 2008 server but this should serve as a general example of how to perform this task on a Windows server. The exact steps and dialogs may appear different depending on your version of Windows server.

- 1. Select Windows Firewall under the *Control Panel* on the RMS server.
- **2.** To add the exception for RMS, select the **Allow a program through Windows Firewall** option in the left column (FIG. 63).

۲ï	💮 Windows Firewall			۱
1 III IIIII	Turn Windows Firewall on or	Windows Firewall	08	
1	Allow a program through Windows Firewall	Windows Firewall can help prevent hackers or malicious softwar computer through the Internet or network.	e from gaining access to your	•
		How does a firewall help protect my computer?		
		Windows Firewall is helping to protect your compute	r	
		Windows Firewall is on.	Change settings	
		Inbound connections that do not have an exception are blocke	d.	l
		Display a notification when a program is blocked:	No	l
		Network location:	Domain network	l
		What are network locations?		l
	See also			-
	Network Center			
<u>k</u> 79	itart 🛛 🚠 💻 🔰 📑 Initial	Configuration Tasks	💽 🏠 11:55 AM	

FIG. 63 Windows Firewall

3. In the Windows Firewall Settings dialog, select the Add Port button (FIG. 64).

Windows Firewall Settings
General Exceptions Advanced
Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall. <u>Windows Firewall is currently using settings</u> for the domain network location. <u>What are the risks of unblocking a program?</u> To enable an exception, select its check box:
Program or port
BITS Peercaching COM + Network Access Core Networking Distributed Transaction Coordinator File and Printer Sharing iSCSI Service Key Management Service Netdogon Service Network Discovery Performance Logs and Alerts Remote Administration Remote Desktop Remote Event Log Management
Add program Add port Properties Delete
OK Cancel Apply

FIG. 64 Windows Firewall Settings - Add Port

4. Add the RMS exception to TCP port **3839** (FIG. 65).

Add a Port Use these settir port number an service you war	ngs to open a port through Windows Firewall. To find the d protocol, consult the documentation for the program or nt to use.	×
Name:	RMS	
Port number:	3839	
Protocol:	€ TCP	
	C UDP	
What are the ris	ks of opening a port?	
Change scope.	OK Cancel	

FIG. 65 Add a Port (3839)

5. Click **OK** when complete.

Appendix D - Installation of RMS IIS Virtual Directory in Alternate Path

Overview

The following instructions illustrate how to manually configure the RMS IIS Virtual Directory.

- **1.** Open IIS Manager and create a "RMS" virtual directory in the desired path.
 - You can create the new "RMS" virtual directory in a subfolder of any existing IIS folder (FIG. 66).



FIG. 66 Computer Management (Create new Web Directory)

In this example we will create the RMS virtual directory in a deeply nested path: /apps/amx/management/

2. Upon selecting the **New** > **Virtual Directory** option under the IIS folder where you want to create the RMS virtual directory, you will be prompted with the *Virtual Directory Creation Wizard* (FIG. 67).

Virtual Directory Creation Wizard	
Virtual Directory Alias You must give the virtual directory a short n-	ame, or alias, for quick reference.
Type the alias you want to use to gain acce same naming conventions that you would fo Alias:	ss to this Web virtual directory. Use the r naming a directory.
RMS	
]	< Back Next > Cancel

FIG. 67 Virtual Directory Creation Wizard - Virtual Directory Alias

- **3.** Enter the desired web alias name, in this example we will use *RMS*.
- 4. Select Next to continue.
- **5.** The new "RMS" virtual directory should point to the existing RMS web directory in the installation path (FIG. 68):

C:\Program Files\AMX Resource Management Suite\Web

Virtual Directory Creation Wizard	
Web Site Content Directory Where is the content you want to publish on the Web site?	
Enter the path to the directory that contains the content. Directory:	
C:\Program Files\AMX Resource Management Suite\Web	Browse
< <u>B</u> ack <u>N</u> ext>	Cancel

FIG. 68 Virtual Directory Creation Wizard - Web Site Content Directory

- 6. Select Next to continue.
- 7. Select the Read and Run Scripts access permissions (FIG. 69).



FIG. 69 Virtual Directory Creation Wizard - Access Permissions

- 8. Select Next to continue.
- 9. Select the Finish button to complete the virtual directory creation wizard (FIG. 70).



FIG. 70 Virtual Directory Creation Wizard - Flnish

10. Next, right-click the newly created RMS virtual directory and select the Properties option (FIG. 71).



FIG. 71 Computer Management

11. In the **Virtual Directory** tab, ensure the following settings are correct (FIG. 72):

HTTP Headers	Custom Errors	ASP.NET	
Virtual Directory	Documents	Directory Security	
When connecting to this resource, the content should come from:			
•	A directory located on this compute	er	
04	A share located on another compu	iter	
04	A redirection to a <u>U</u> RL		
Logal Path: C: Script source acces: Bead Write	\Program Files\AMX Hesource Ma s	anag Br <u>o</u> wse	
Logal Path: C: Script source acces: P Read Write Directory browsing Application Settings	VProgram FilesVAMX Hesource Miles s	anag Browse	
Logal Path: C: Script source acces: Read Write Directory browsing Application Settings	VProgram FilesVAMX Hesource Mass s	esource	
Logal Path: C: Script source acces: Pead Write Directory browsing Application Settings Application name: Starting point:	Program FilesVAMX Resource M. s	Browse Browse Remove	
Logal Path: C: Script source access Bead Write Directory browsing Application Settings Application name: Starting point: Execute Permissions:	Program FilesVAMX Hesource M. s	Browse esource Remove Configuration	

FIG. 72 RMS Properties - Virtual Directory

If the *Application Settings* section appears disabled, then the RMS IIS Application instance has not been created - select the **Create** button to create the application (FIG. 73).

Application Settings			
Application name:	Default Application		Create
Starting point:	<default site="" web=""></default>		Carlanation
Execute Permissions:	Scripts only	~	Configuration.
Application Protection:	Medium (Pooled)	~	Unload

FIG. 73 Application Settings - Create

12. Select the Documents tab and ensure the default.asp file is listed as a default document (FIG. 74).

RMS Properties		? 🛛
HTTP Headers	Custom Errors	ASP.NET
Virtual Directory	Documents	Directory Security
Enable Default Document Enable Default Ann Default.htm Default.asp index.htm idefault.aspx		Add <u>R</u> emove
Enable Document Footer		Browse
	IK Cancel	Apply Help

FIG. 74 RMS Properties - Documents

13. Select the **ASP.NET** tab and ensure the ASP.NET version is set to **2.0.50727** (FIG. 75).

RMS Properties		?
Virtual Directory	Documents	Directory Security
HTTP Headers	Custom Errors	ASP.NET
Microsoft		
ASP.n.	et	
ASP.NET version:	2.0.50727	
Virtual path:	/apps/amx/manage	ement/RMS
File location:	C:\Program Files\A	MX Resource Management
File creation date:	1/27/2009 9:56:29	AM
File last modified:	5/11/2009 10:13:2	3 AM
	E	dit Configuration
		() (
	OK Cancel	Apply Help

FIG. 75 RMS Properties - ASP.NET

14. Once these settings are verified, select OK to close the IIS virtual directory properties dialog.

You should now be able to open a browser to the new website path. It may take a few minutes for the ASP.NET application to recompile itself for the new location.

http://localhost/apps/amx/management/rms
Update the RMS Server Internal Configuration For The New Path

Once the RMS web pages have successfully opened, we need to get the RMS server to update its internal configuration for the new path.

The steps below will reconfigure the RMS server to determine the new RMS virtual directory:

1. First, stop the RMS Services using the RMS Service Manager (FIG. 76).

IX Resource Management Suite Service Mana	ager	Manag
Display Name	State	Start
AMX RMS Server	Running	Stop
AMX RMS NetLinx Connection Manager	Running	Pause
AMX RMS Scheduling Manager	Running	Resume
Start Services Stop Services	Restart Services	

FIG. 76 AMX Resource Management Suite Service Manager - Stop Services

- **2.** Now run the *RMS Configuration Wizard*.
 - a. Step through the configuration steps until you get to the Virtual Directory page (FIG. 77).

🔏 Resource Management S	uite Configuration Wizard 💀 🖬 🔀
Resource Management S Resource Management Suite Resource Management Suite Resource Management Suite Resource Management Suite Resource Management S Reso	e Configuration Wizard
Corpernissions System Settings Finished	We need to create a virtual web directory in IIS to host the MeetingManager web pages. Virtual Directory Alias Name: apps/amx/management/RMS Web Directory
AWAY	< <u>B</u> ack <u>N</u> ext> E <u>x</u> it

FIG. 77 RMS Configuration Wizard - Virtual Directory

In the virtual directory alias name field, you should now see the full alias path to the RMS website on the IIS web server.

b. Click **Next** to save this detected website alias to the RMS configuration.

3. Continue through the steps in the RMS Configuration Wizard until you reach the *OS Permissions / Web User* page (FIG. 78).

🔏 Resource Management S	uite Configuration Wizard	
Resource Management Suit	e Configuration Wizard	P.NET)
Welcome Database Product Selection Web Services Services Corres Service User Web User System Settings Finished	Operating system permissions must be constructed by the system permission of the system permission of the system of the system permission of the s	Permissions Are Set Permissions Are Set configured.
AMX®	< <u>B</u> ack	<u>N</u> ext > E <u>x</u> it

FIG. 78 RMS Configuration Wizard - Web User

- Make sure the permissions are all applied correctly.
- If any permission is not set, then use the **Set Permissions** button to apply the necessary permissions.
- **4.** Continue through the remaining steps in the RMS Configuration Wizard until you reach the final *Finished* page (FIG. 79).

🔏 Resource Management S	uite Configuration Wizard 💀 🖬 🔀
Resource Management S Resource Management S Resource Management Suite Welcome Database Product Selection Web Services Services Services Licensing OS Permissions System Settings Finished	e Configuration Wizard e Configuration Wizard Finished Congratulations you have completed the MeetingManager configuration wizard. Launch MeetingManager Web Page MeetingManager Web Pages: http://server/angs/ams/management/BMS/
AMX®	< <u>₿</u> ack <u>N</u> ext> <u>F</u> inished

FIG. 79 RMS Configuration Wizard - Finished

Here, you will need to verify that the URL displayed is the correct fully qualified URL for the RMS web application.

- If the URL is incorrect, you may need to provide a manual override to the web path configuration.
- See *Appendix E Override the RMS FQDN & Web URL Path* on page 71 for more information on how to override the web URL.
- 5. Open a new browser window to the new RMS web URL just to maker sure all is still working properly.



With this custom IIS Virtual Directory path, the RMS Configuration Wizard will not be able to DELETE or RE-CREATE this virtual directory in a custom path. If the virtual directory ever gets deleted, it will have to be re-created using these manual steps outlined above.

Appendix D - Installation of RMS IIS Virtual Directory in Alternate Path

Appendix E - Override the RMS FQDN & Web URL Path

Overview

RMS generates URL links embedded in notification emails to provide convenience links for quick access to specific content of interest in the RMS web pages. By default, RMS determines the server hostname using the computer name assigned to the server.

However, in certain cases you may want to expose the RMS server using a public fully qualified domain name or in cases where the computer hostname my not be resolvable by all network workstations. This default behavior can be bypasses allowing you to provide a static fully qualified hostname and URL path for the RMS configuration.

The instructions below will configure your RMS server to use a custom/static fully qualified hostname and URL:

1. Open the following folder on your RMS server:

C:\Program Files\AMX Resource Management Suite\Scripts

- 2. Locate the RMS Set FQDN & URL.vbs script file and double-click it to launch it.
- **3.** You will be prompted with the current RMS configured web URL select **Yes** to provide your own URL to override the default detected settings (FIG. 80).

AMX Res	source Management Suite
?	The RMS Server is currently configured to use the fully qualified web URL path: http://server/RMS/ Would you like to override the current configured web path? Yes No

FIG. 80 Override current configured web path

4. Type in the new fully qualified URL path to the RMS web application and select **OK** to save the custom setting (FIG. 81).



FIG. 81 Enter new web path



To return the RMS server back to it's default configuration where the RMS server attempts to auto detect the RMS web application URL, simply type '**auto**' into the text prompt and press **OK**.

5. After completing the web URL change, you will need to restart the RMS services to fully propagate the updated setting (FIG. 82).



FIG. 82 Restart RMS Services

You can use the **Restart Services** option in the RMS Service Manager utility to restart all the RMS services (FIG. 83).

AMX Resource Management Suite Service	ce Manager	E X
AMX Resource Management Suite Service Ma	anager	
Display Name AMX RMS Server AMX RMS Communications Manager AMX RMS NetLinx Connection Manager AMX RMS Scheduling Manager	State Running Running Running Running	Start Stop Pause Resume
Start Services Stop Services	<u>R</u> estart Services	Exit

FIG. 83 AMX Resource Management Suite Service Manager - Restart Services

Once the services have restarted, RMS will now use the override setting as its web path for all links and URLs.

Appendix F - Verify the RMS Server Info & Web URL Path

Verify the RMS Server Info & Web URL Path

The RMS installation provides a script file that you can run on the RMS server to verify the RMS server's configured hostname, IP address, and web URL path.

Open the following folder on your RMS server:

C:\Program Files\AMX Resource Management Suite\Scripts

Next, locate the "RMS Server Information.vbs" script file and double-click it to launch it.

You will be prompted with the current RMS configured *Hostname*, *IP Address*, *Web Alias*, and *Web Base Path* (fully qualified web URL) (FIG. 84).

ver Info	
RMS Server Information:	
Hostname :	server
IP Address :	192.168.10.13
Web Alias :	RMS
Web Base Path :	http://server/RMS/
OK	
<u>.</u>	
	ver Info RMS Server Inforr Hostname : IP Address : Web Alias : Web Base Path : OK

FIG. 84 RMS Server Info

Appendix F - Verify the RMS Server Info & Web URL Path

Appendix F - Verify the RMS Server Info & Web URL Path



It's Your World - Take Control™