Active Risk Manager

ARM 6: General Availability Release

Installation Guide

November 2012

How to Get in Touch with Active Risk Technical Support

Telephone: +44 (0)1628 582550 (EU) or +1 (703) 673 9582 (US)
Email: support@activerisk.com
Support Portal: http://support.activerisk.com

Trademarks and Copyright

The information contained in this document is © Active Risk Ltd 2012. All Rights Reserved. No part of this material may be reproduced in any form or by any means - for example graphically, electronically or mechanically, including photocopying, recording, taping or otherwise in information storage and retrieval systems - without the prior permission of Active Risk Ltd.

All other product names referenced are believed to be the registered trademarks of their respective companies.

Contents

Purpose

This document describes the installation and upgrade process for the ARM 6 General Availability Release.

Scope

The installation process is described here from the perspective of a System Administrator. This document does not cover information about the software prerequisites required – this information can be found in the ARM 6 System Prerequisites Guide.

1 Hardware Requirements

We recommend that customers work closely with Active Risk during the early stages of implementation to determine the best configuration. It is important to consider both the technical requirements, such as performance and scalability as well as business requirements, such as production, acceptance and training environments. It is also important that customers make adequate provision for high availability and business continuity.

Active Risk can provide technical consultancy to help install and configure new servers with ARM including integration with any supported third party software. Assistance can also be given in performing one-off data migrations from existing systems.

Installation of the ARM application server and database Server on the same machine is not recommended for performance reasons, except for proof of concept installations for a small number of users. Shared database servers should have sufficient capacity for the number of application databases hosted.

1.1 Overview

This document outlines the system requirements for implementation of Active Risk Manager 6 Base. The document does not provide installation instructions for any of the referenced components or recommendations on all technical areas that are affected by ARM. For further advice on installing ARM please contact the Active Risk Support Desk.

1.2 System Pre-requisites

Please see the System Pre-requisites document, available on Active Risk's customer support portal.

1.3 ARM Server Hardware Requirements

Active Risk recommends that the ARM Application, SharePoint, Reporting and Database are deployed to separate servers for medium and large scale production deployments. For small scale "proof of concept" deployments it is possible consolidate physical servers.

1.4 Application Server Requirements

The precise hardware specification will depend on the number of concurrent users. The Application Server requires approximately 1GB of free disk space for an installation of Active Risk Manager, in addition to the third party software and Operating System components.

The following table shows minimum system requirements for the ARM server.

Hardware	Up to 50 users	50 to 200 users	Above 200 users
Processor	2.0 GHz Single Core or faster	2.0 GHz Dual Core or faster	3.0GHz Quad Core or faster * 2
Memory	4GB	6GB	8GB
HDD	10GB free in the System volume 5GB for Data	10GB free in the System volume 8GB for Data	10GB free in the System volume 12GB for Data
NIC	Gigabit	Gigabit	Gigabit

Please note that ARM version 6 is only available for x64 platforms.

ARM 6 runs on 64 bit Windows 2008 R2 [Latest Service Pack] only.

For Production installations we strongly recommend that the ARM Application Server does not host any other business critical applications to avoid configuration management issues, such as application conflict, and operational service restrictions.

1.5 ARM Application Framework Server Requirements

We recommend that large and medium scale implementations host the ARM Application Framework on an existing MOSS server.

A similar hardware specification to that of the application server is recommended. The precise hardware specification will depend on the number of concurrent users and the anticipated utilisation patterns; the following table shows recommended system requirements for ARM Lite on MOSS.

Hardware	Up to 50 users	50 to 200 users	Above 200 users
Processor	2.0 GHz Single Core or faster	2.0 GHz Dual Core or faster	3.0GHz Quad Core or faster
Memory	4GB	6GB	8GB
HDD	10GB free in the System volume 5GB for Data	10GB free in the System volume 8GB for Data	10GB free in the System volume 12GB for Data
NIC	Gigabit	Gigabit	Gigabit

1.6 Reporting Services Server Requirements (MSRS)

We recommend that large and medium scale implementations host Reporting on a dedicated server where reporting is used extensively.

A similar hardware specification to that of the application server is recommended. The precise hardware specification will depend on the number of concurrent users and the anticipated utilisation patterns, e.g. size and complexity of reporting requirements; the following table shows minimum system requirements for the reports server.

Hardware	Up to 50 users	50 to 200 users	Above 200 users
Processor	2.0 GHz Single Core or faster	2.0 GHz Dual Core or faster	3.0GHz Quad Core or faster * 2
Memory	4GB	6GB	8GB
HDD	10GB free in the System volume 5GB for Data	10GB free in the System volume 8GB for Data	10GB free in the System volume 11GB for Data
NIC	Gigabit	Gigabit	Gigabit

1.7 Database Server Requirements

The hardware specification will depend on the number of databases hosted on the database server and the number of concurrent users. The following is a typical specification for a production database server. The following table shows minimum system requirements for the database server.

Hardware	Up to 50 users	50 to 200 users	Above 200 users
Processor	2.0 GHz Single Core or faster	2.0 GHz Dual Core or faster * 2	3.0GHz Quad Core or faster * 2
Memory	4GB	6GB	8GB
HDD	10GB free in the System volume 5GB for Data 5Gb for Logs 5Gb for Backups	10GB free in the System volume 8GB for Data 8Gb for Logs 8Gb for Backups	10GB free in the System volume 11GB for Data 11Gb for Logs 11Gb for Backups
NIC	Gigabit	Gigabit	Gigabit

An example of a dedicated ARM database server to support a mature risk process and risk register for a user base of 350 Production users

For example, HP Proliant DL 580 G6

For a production system, disk space requirements would need to be calculated based on the amount of data required to be stored, the expected growth rate and archiving policy.

An initial ARM database (empty or with demo data) requires approx:

- 10MB to 50MB of disk space (applies to the data file only)

A mature ARM database (Oracle or SQL Server) with a large user population and risk register (approx. 50000 business activities and 25000 risks) built up over approx. 5 years requires approx:

- 1 to 3 GB of storage on disk (again, applies to the data file only)

Please request the ARM Database Sizing Spread sheet from Active Risk Support to help with sizing your ARM database growth.

1.8 Client Hardware Requirements

The recommended minimum client workstation hardware for running ARM 6:

- 2 gigahertz (GHz) or faster 64-bit (x64) processor
- 4 GB RAM
- 20 GB available hard disk space.

4GB of RAM is recommended for intensive application usage, e.g. risk analysis, etc.

As the ARM filter screen is opened from SQL Reporting Services both the ARM URL and the Reporting Services URL **MUST** be in the same internet zone. We recommend adding both to the Trusted Sites in Internet Explorer.

2 Considerations

A TCP/IP connection is required between the client and application server and between the application server and database server. Http and/or https protocols must be supported between the client and application server.

For effective operation, we recommend a LAN, or a WAN with an available bandwidth of 256 Kbps or higher. Operation over lower speed or busy connections is possible, by enabling the advanced caching and compression options, but may still provide unsatisfactory performance.

Encryption of traffic between the client and server is possible if the application server is configured for secure (SSL) operation.

There may be special considerations if there is a firewall or proxy server between the client and the application server, or between the database server and application server.

Where the Application Server and Database Server are installed as separate servers, it is recommended that these are placed in the same location, and ideally on the same switch for optimum network connectivity. Where this is not possible, it is important that a fast network connection, with good available bandwidth, is in place between the two locations. A slow or unreliable network connection between the Application Server and Database Server can have a significant detrimental effect on performance and stability.

2.1 Systems and Software Requirements

ARM 6 works only on x64 platforms. Also see **section 4** if you are upgrading from a previous version of ARM.

The ARM server must be Windows 2008 R2 Standard/Enterprise Edition with the latest service pack. Please refer to the ARM Platform support matrix for more information.

- Before you begin the installation ensure that as a minimum you have the Application Server and Web Server (IIS) roles and role services shown below enabled.

[X] Application Server [Application-Server]
[X] .NET Framework 3.5.1 [AS-NET-Framework]
[ ] Web Server (IIS) Support [AS-Web-Support]
[ ] COM+ Network Access [AS-Ent-Services]
[X] TCP Port Sharing [AS-TCP-Port-Sharing]
[X] Windows Process Activation Service Support [AS-WAS-Support]
[X] HTTP Activation [AS-HTTP-Activation]
[X] Message Queuing Activation [AS-MSMQ-Activation]
[X] TCP Activation [AS-TCP-Activation]
[X] Named Pipes Activation [AS-Named-Pipes]
[X] Distributed Transactions [AS-Dist-Transaction]
[X] Incoming Remote Transactions [AS-Incoming-Trans]
[X] Outgoing Remote Transactions [AS-Outgoing-Trans]
[ ] WS-Atomic Transactions [AS-WS-Atomic]

[X] Web Server (IIS) [Web-Server]
[X] Web Server [Web-WebServer]
[X] Common HTTP Features [Web-Common-Http]
[X] Static Content [Web-Static-Content]
[X] Default Document [Web-Default-Doc]
[X] Directory Browsing [Web-Dir-Browsing]
[X] HTTP Errors [Web-Http-Errors]
[X] HTTP Redirection [Web-Http-Redirect]
[ ] WebDAV Publishing [Web-DAV-Publishing]
[X] Application Development [Web-App-Dev]
[X] ASP.NET [Web-Asp-Net]
[X] .NET Extensibility [Web-Net-Ext]
[X] ASP [Web-ASP]
[ ] CGI [Web-CGI]
[X] ISAPI Extensions [Web-ISAPI-Ext]

[X] ISAPI Filters [Web-ISAPI-Filter]
[X] Server Side Includes [Web-Includes]
[X] Health and Diagnostics [Web-Health]
[X] HTTP Logging [Web-Http-Logging]
[X] Logging Tools [Web-Log-Libraries]
[X] Request Monitor [Web-Request-Monitor]
[X] Tracing [Web-Http-Tracing]
[ ] Custom Logging [Web-Custom-Logging]
[ ] ODBC Logging [Web-ODBC-Logging]
[X] Security [Web-Security]
[X] Basic Authentication [Web-Basic-Auth]
[X] Windows Authentication [Web-Windows-Auth]
[ ] Digest Authentication [Web-Digest-Auth]
[ ] Client Certificate Mapping Authentication [Web-Client-Auth]
[ ] IIS Client Certificate Mapping Authentication [Web-Cert-Auth]
[ ] URL Authorization [Web-Url-Auth]
[ ] Request Filtering [Web-Filtering]
[ ] IP and Domain Restrictions [Web-IP-Security]
[X] Performance [Web-Performance]
[X] Static Content Compression [Web-Stat-Compression]
[X] Dynamic Content Compression [Web-Dyn-Compression]

[X] Management Tools [Web-Mgmt-Tools]
[X] IIS Management Console [Web-Mgmt-Console]
[X] IIS Management Scripts and Tools [Web-Scripting-Tools]
[X] Management Service [Web-Mgmt-Service]
[X] IIS 6 Management Compatibility [Web-Mgmt-Compat]
[X] IIS 6 Metabase Compatibility [Web-Metabase]
[X] IIS 6 WMI Compatibility [Web-WMI]
[X] IIS 6 Scripting Tools [Web-Lgcy-Scripting]
[X] IIS 6 Management Console [Web-Lgcy-Mgmt-Console]

- Customers using an Oracle ARM database will require:
  - Oracle OLEDB Provider, version 11.1.0.6.0 or higher
  - Oracle Service for MTS, version 11.1.0.6.0 or higher
  - Oracle client, version 11.1.0.6 or higher.
- Microsoft Reporting Services 2008 R2 (If running on the ARM server)
- It is highly recommended that the latest Windows and Internet Explorer (version 9) with service packs and security fixes are applied.
- Microsoft Office SharePoint Server 2010 (optional – if ARM Apps are is required)
- Windows .NET Framework Version 3.5 SP1 (includes 2.0, 3.0 and 3.5)

3 New Installations

3.1 Before you begin

- Make sure that your application server meets the requirements set out above in 4.2 Software and System Requirements.
- If there are firewalls in the environment into which you are deploying ARM, make sure you read and understand the section 14 of this document – “Firewall Considerations”
- Make sure the person who performs the installation has system administrator privileges for the ARM server and the DB environment.
- Make sure you have an ARM licence for the ARM server before proceeding with the application server deployment (Section 3.2).

3.1.1 ARM Database Server Requirements

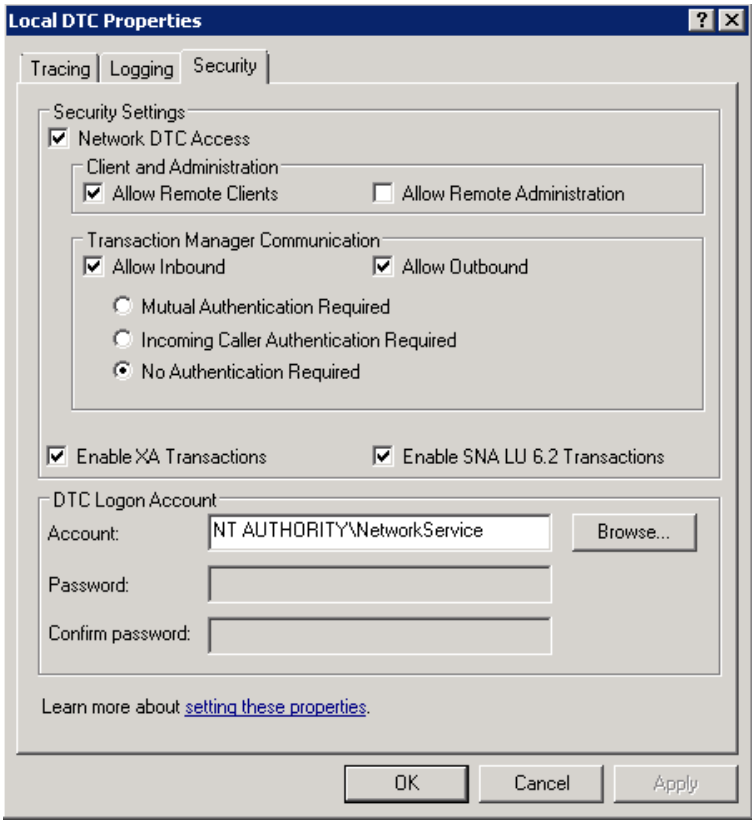
The ARM database should be installed on a separate server to achieve optimum performance. Please refer to the section on Hardware Requirements for further information.

3.1.2 Supported platforms:

- SQL Server 2008 R2 SP2
- Oracle 11g R2(Recommended min 11.2.0.3).

3.1.3 SQL Server Information:

- The Microsoft Distributed Transaction Co-ordinator Service [MSDTC] needs to be running on both the Application and Database servers where ARM Database is going to be hosted. MSDTC Security Configuration tab should resemble screen below:



- SQL Server Clustering is supported.

  The MS DTC service needs to be enabled and running as a clustered resource on all cluster nodes via cluster Manager:

  <***Links not valid, we should embed our support site link for MSDTC Config for clusters, following is example link which I found from Microsoft***>

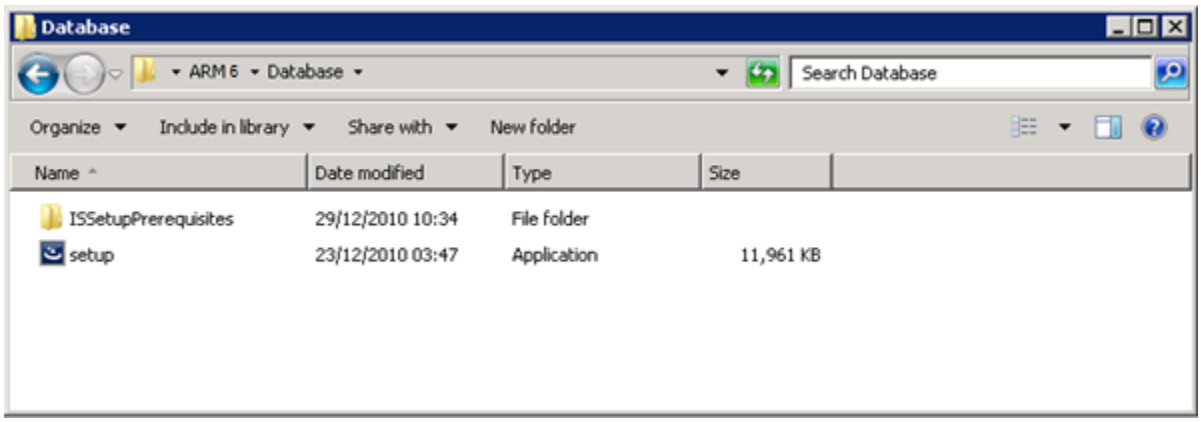
  http://support.microsoft.com/kb/2027550

Please note:**MSDE, MS SQL Express and MS SQL Server Evaluation Edition are not supported database platforms**.

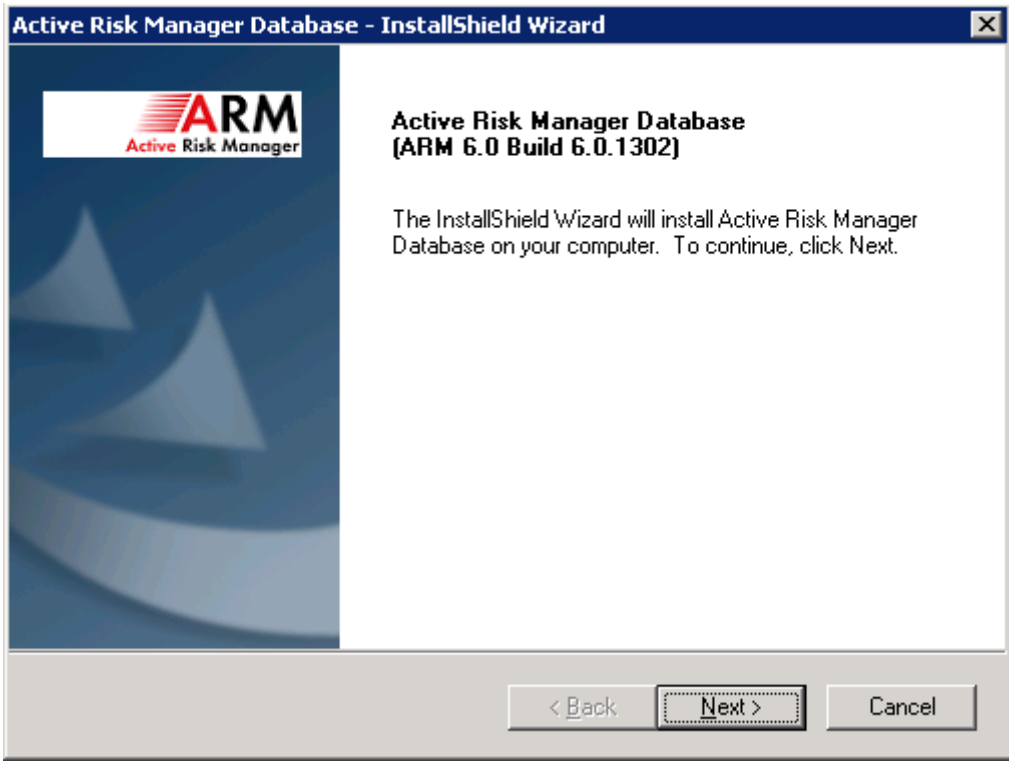
The following steps assume that your database installation wizard is being executed from the ARM application server, please feel free to reference the server where you actually execute the Database Installer.

Note: If using Oracle you need to install the Oracle Client, see **Oracle database Installation** first before continuing with the next step.

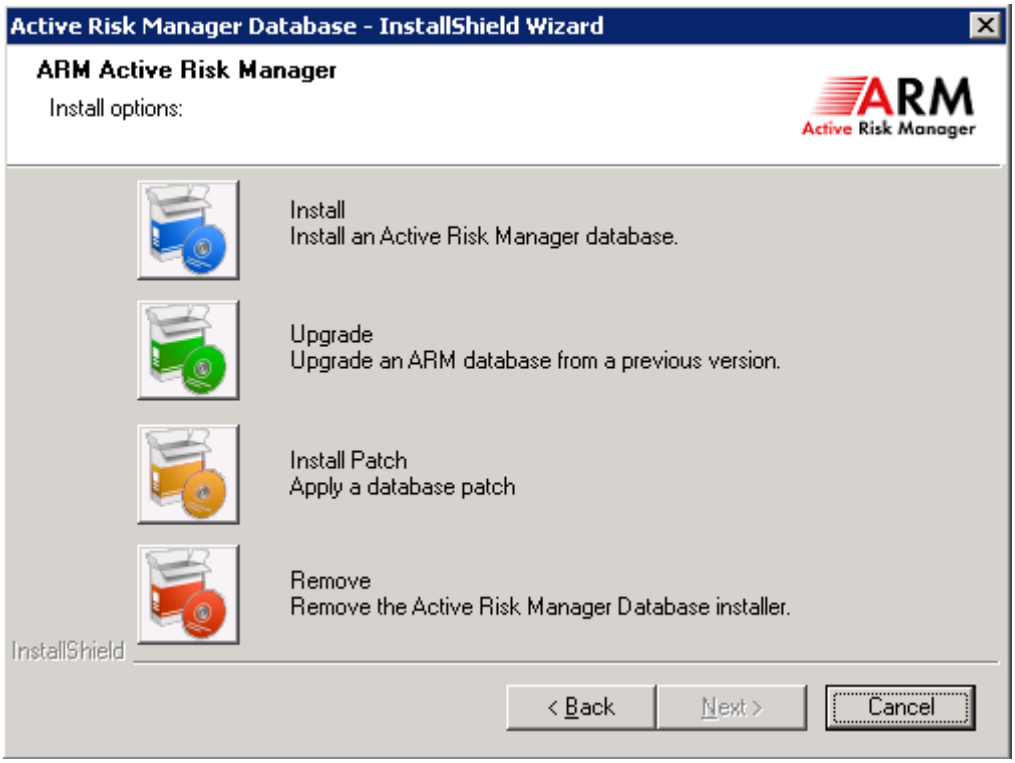
1. Right click on the executable *setup.exe* from the Database folder on the ARM installation media and select "*Run as administrator*" if applicable.



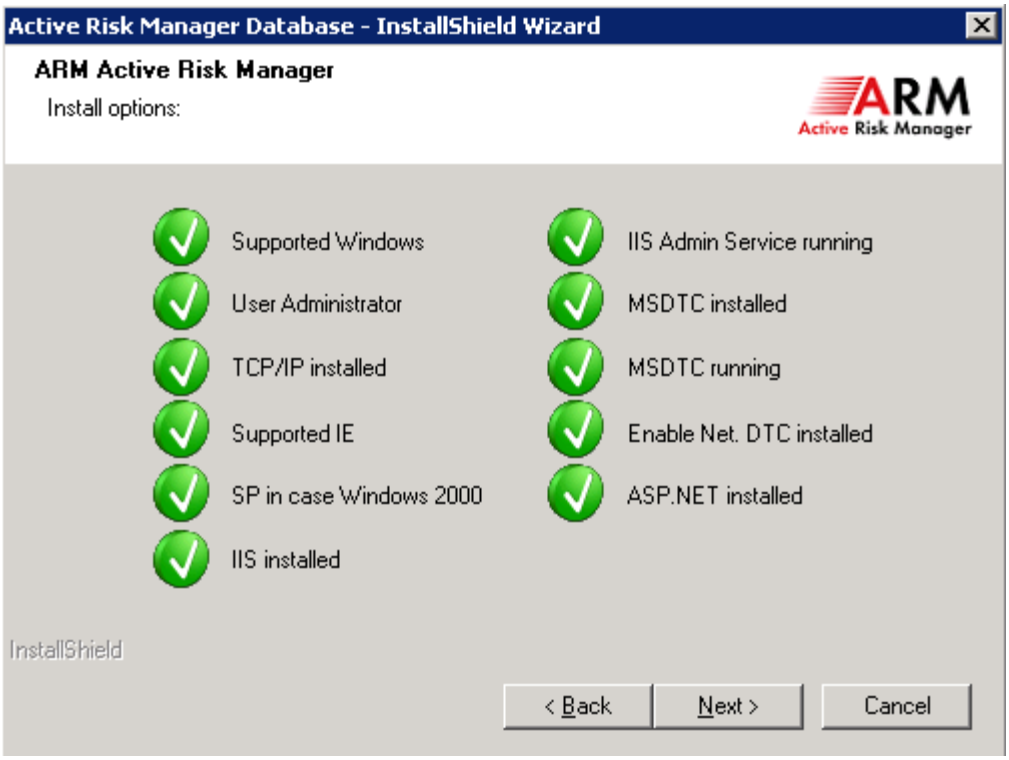
2. Select and click the Next command button on the dialog box presented to you.



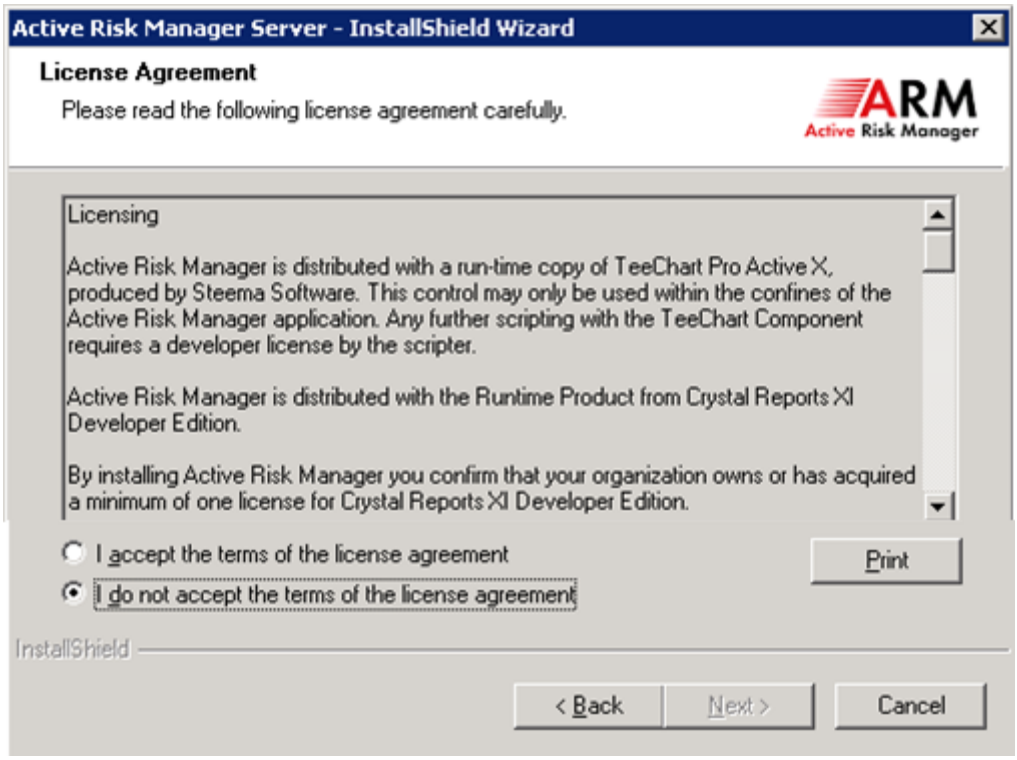
3. Click on Install button to create an empty ARM database schema.



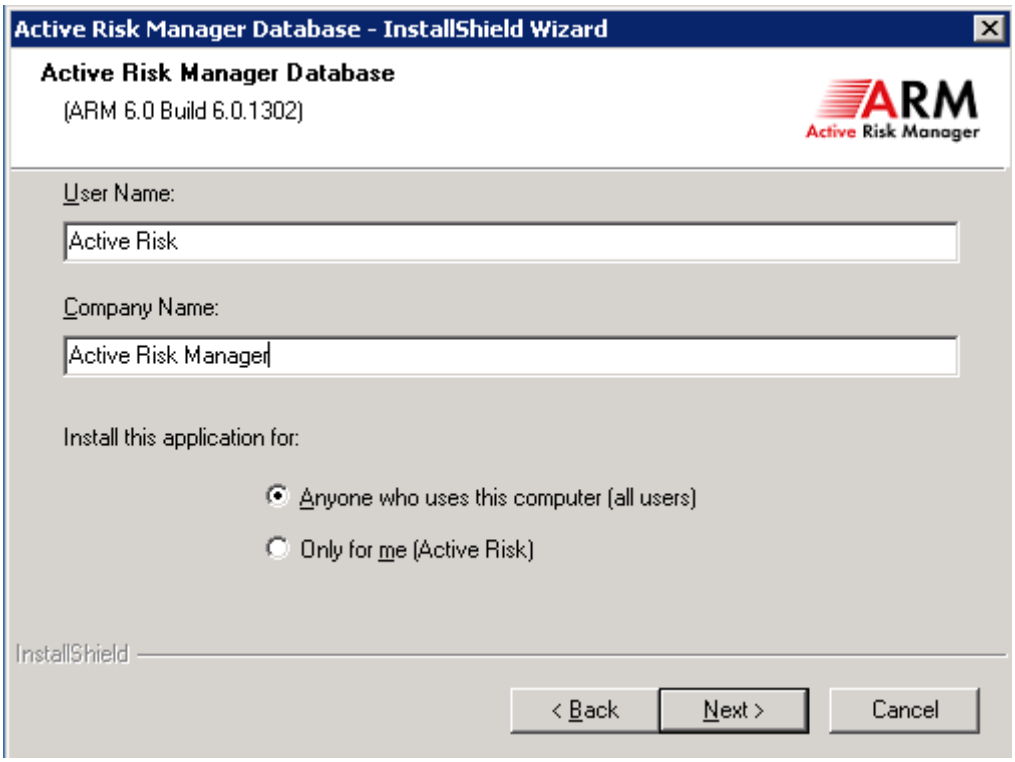
4. Installer is going to perform checks that are common pre-requisite checks performed before commencing further installation. Please click Next once checks are successful.



5. Read and accept the licence agreement to progress further.

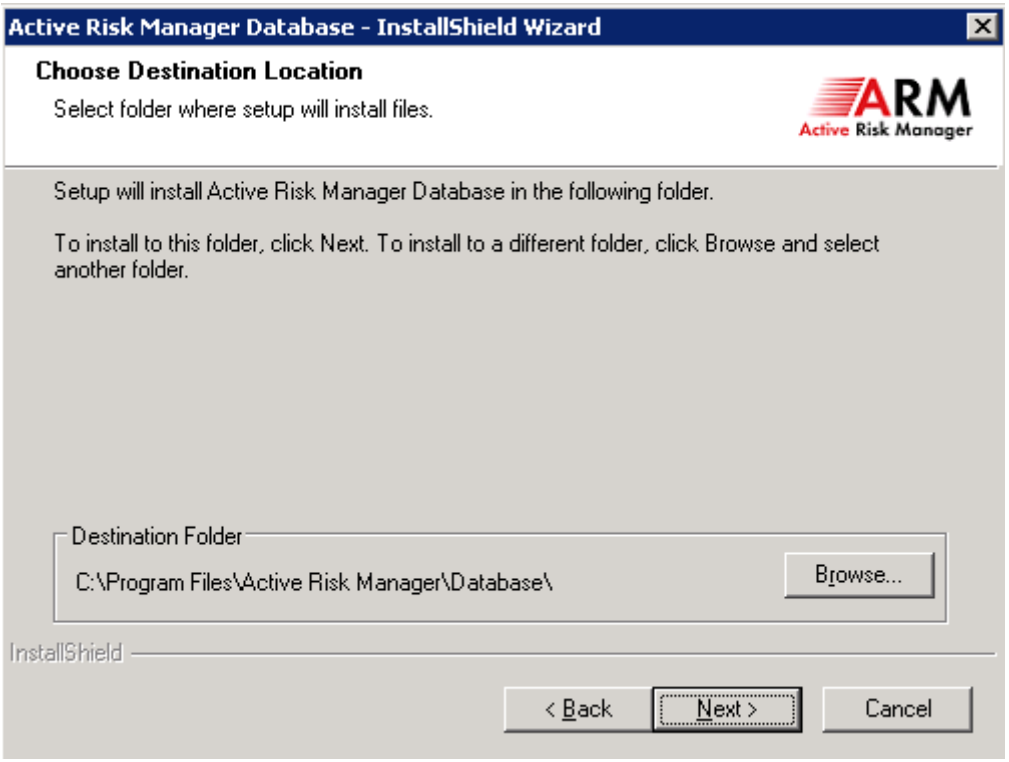


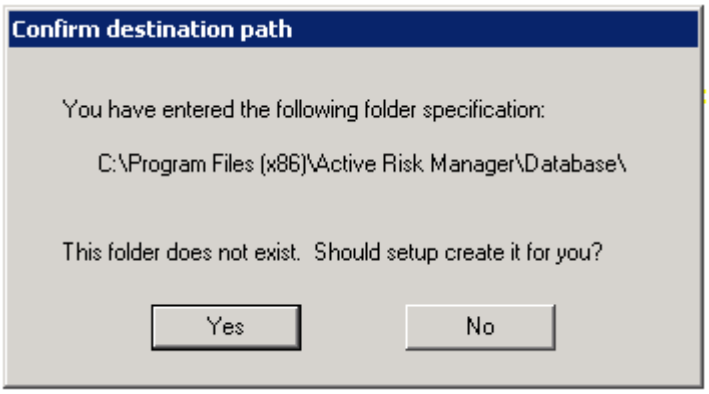
6. Type your User Name and Company Name in to the correct fields. Select who you want the database creation application to be available to.



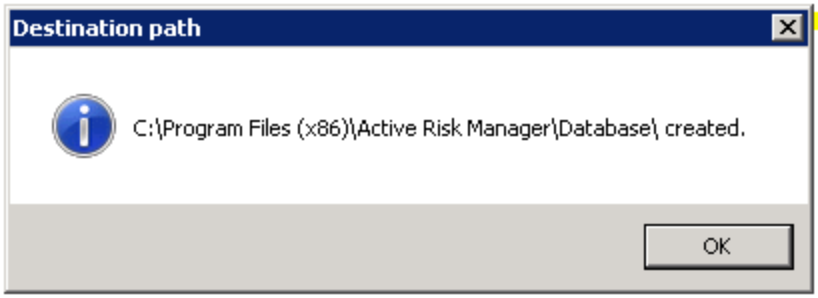
7. Choose the destination for the installation files. We recommend using the default location.

   Note: Database Installation Path is going to appear as c:\Program Files (x86)\.. for x64 servers.



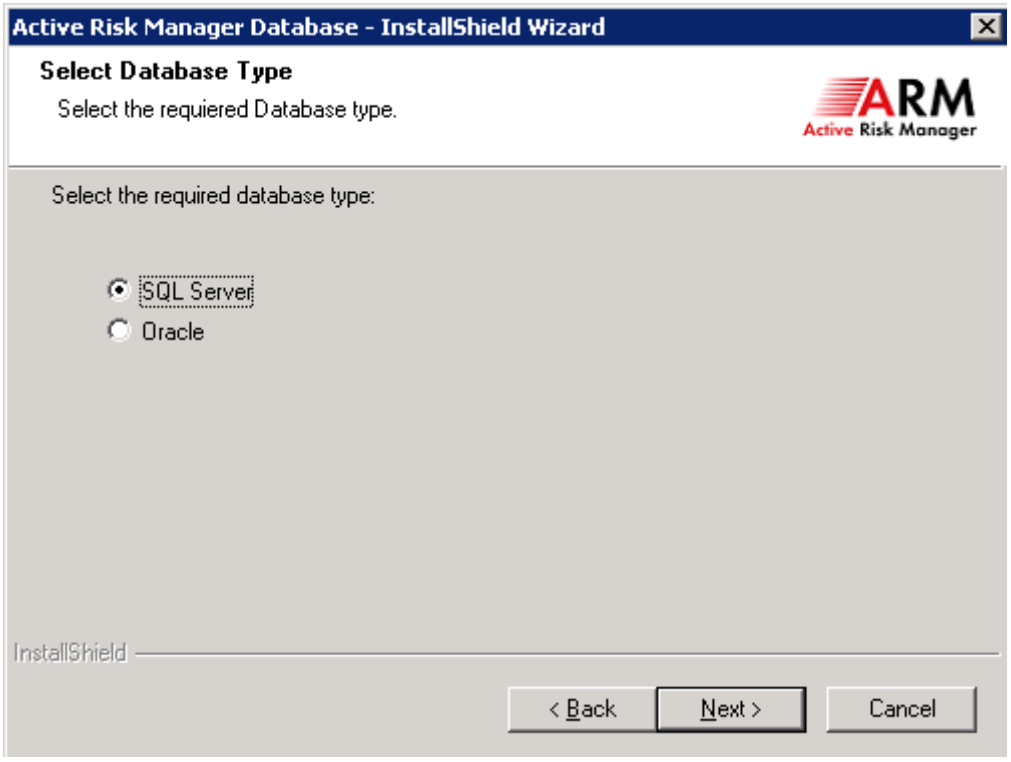


8. Click Yes and then “OK”

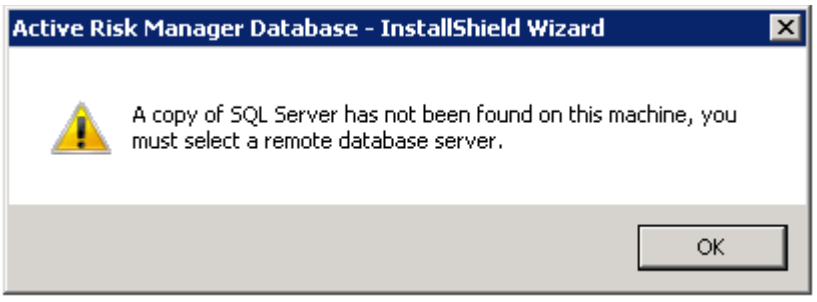


3.1.4 Microsoft SQL database Installation

1. Select respective supported database product that you wish to use. This step is important and if you are intended to use Oracle then go to Oracle database Installation.



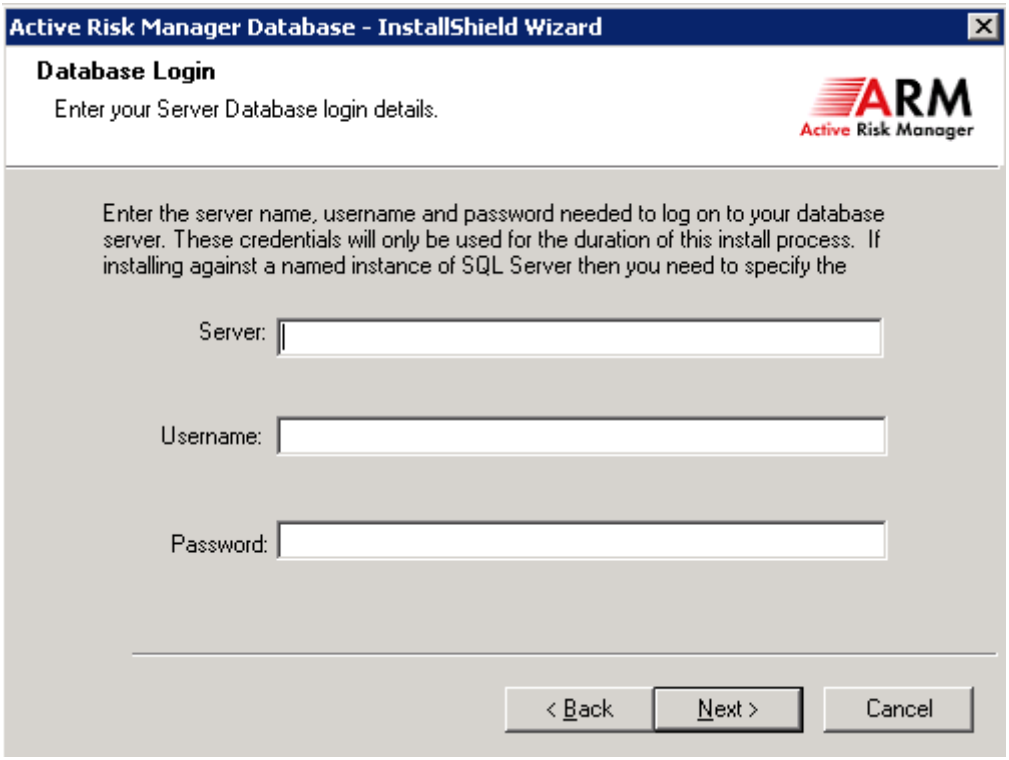
2. If the SQL Server option was selected in the previous step the wizard will check to see if SQL Server has been installed locally.



3. Enter the hostname/FQDN or IP address of the SQL Database server.

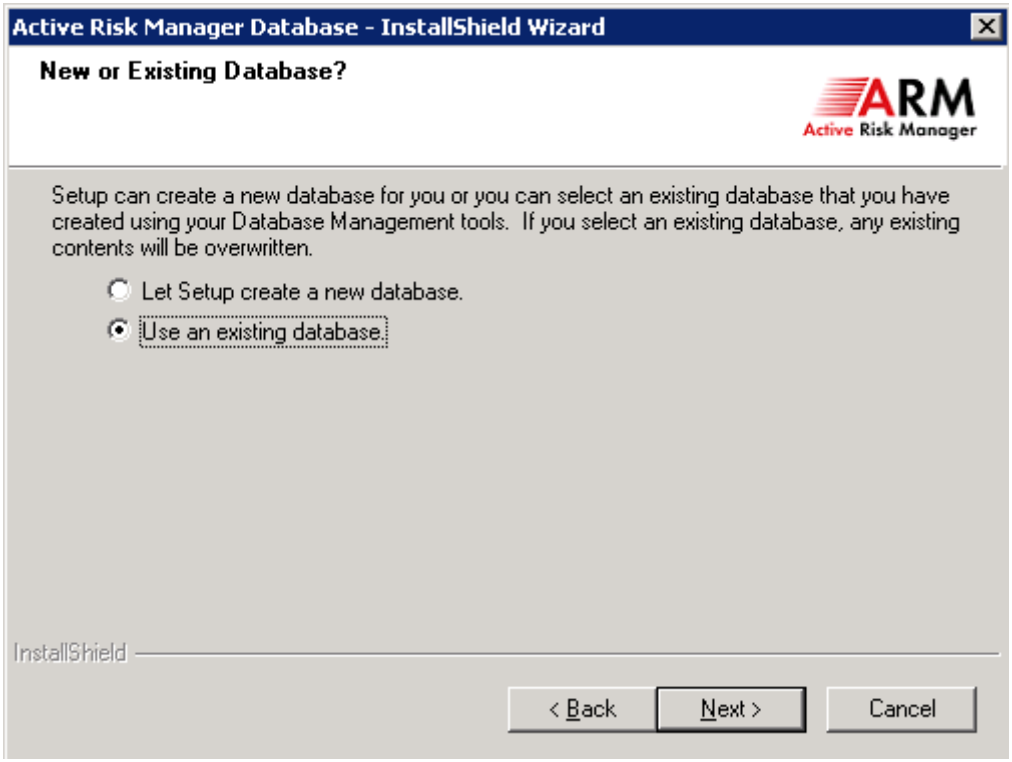
   The credentials provided should be for a SQL server account, **WINDOWS AUTHENTICATION is not currently supported for the database connection**

   If you want to create a new database using this installer the account should have the **dbcreator** SQL Server role as a minimum. If you wish to use a database that has already been created provide the log details for the **dbo** user.

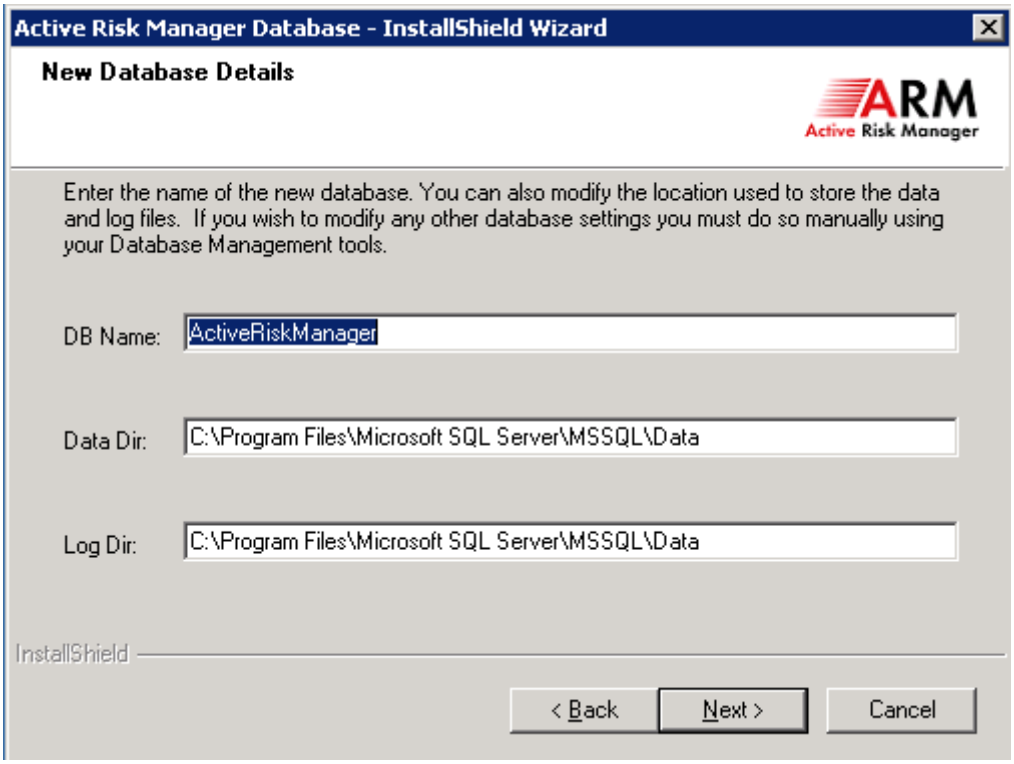


4. To create a new database choose ‘Let Setup create a new database’ and go to step 5

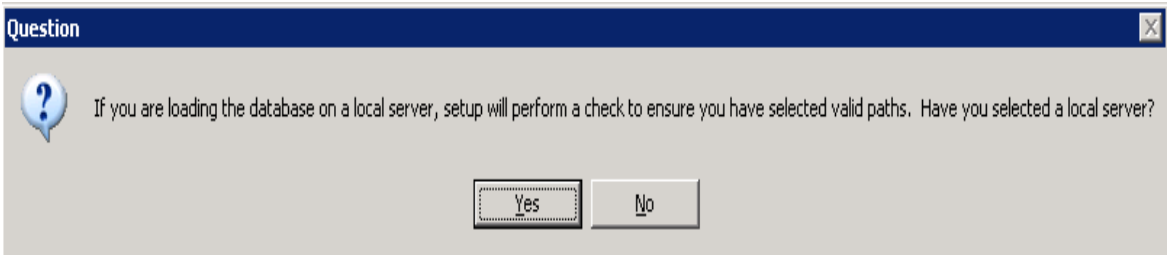
   Alternatively if you have a database already created choose ‘Use an existing database’ and go to step 7



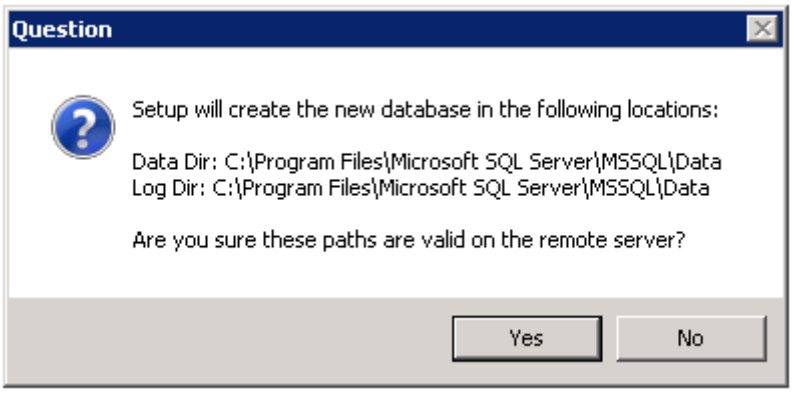
5. Enter a DB Name and check or change the Data Dir and Log Dir to a valid location on the database server.
   NOTE: it is important to ensure that the data and log locations actually exist on the SQL server you are connecting to.



6. A pop up will appear to ask you if the database server is on the local machine or remote server. If the SQL database you are using is on the local machine click YES, if no select NO.

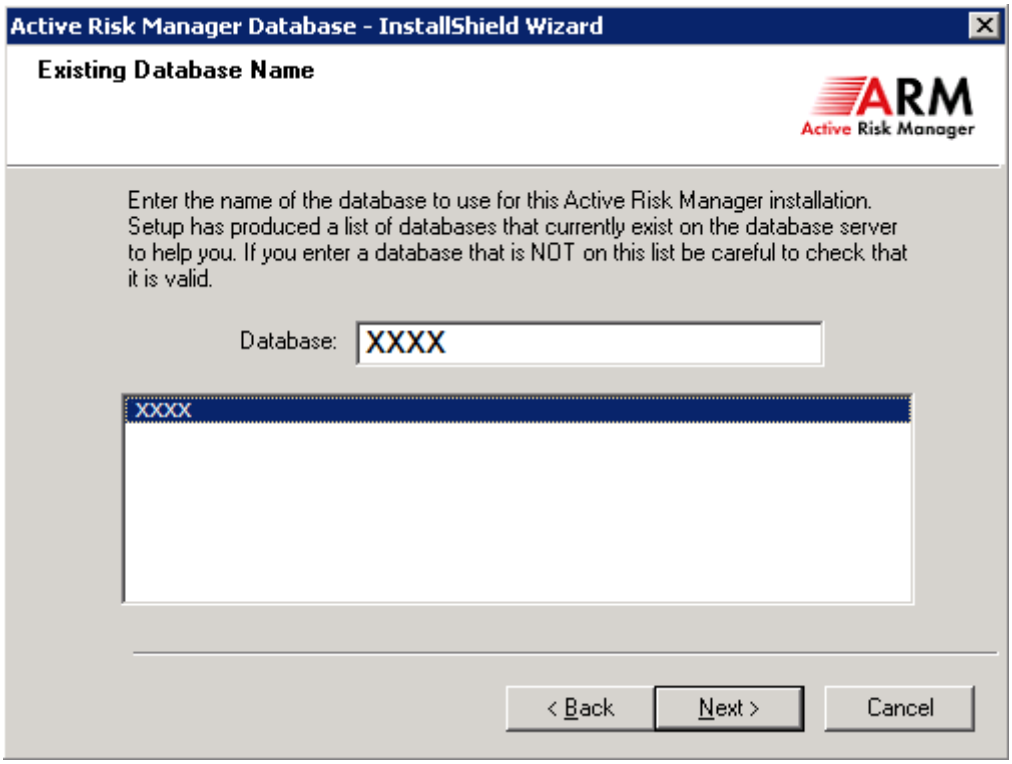


7. Confirm that the data file locations are correct.

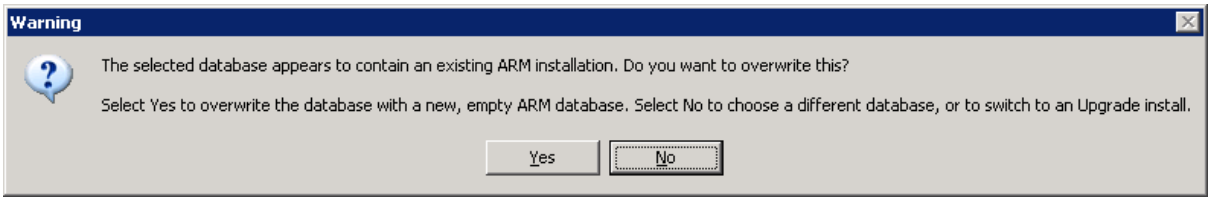


Click next until Finish to complete the installation, and then go to section 4.2 to continue the Application Installation.

8. If you choose to 'Use an existing database' at step 3 you will be given a list of databases to choose from. Select the desired database to continue.



9. Confirm that you are happy to over write the contents of the database.



Click next until Finish to complete the installation, and then go to section 5.2 to continue the Application Installation.

The Next section (5.1.5) covers the Oracle installation only.

3.1.5 Oracle Information:

- Oracle can be installed on all supported operating systems (Windows and UNIX).

- A new database role is created during installation, called ARM_ROLE, and this is assigned to the arm db user. This role must be retained after installation for the correct operation of ARM (no other roles or privileges should be required to run ARM). No existing roles or privileges will be removed during upgrade. The new role will be created and granted to the ARM db user as part of an installation or upgrade, therefore the SYS password will always be required when upgrading to 6 unless the ARM role is manually created first. The sys password should not be needed again for upgrades to subsequent versions.

- The customer can create this role manually to prevent the sys password being required for upgrades. The role must be called 'ARM_ROLE' and have the following 7 privileges: CREATE PROCEDURE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE TRIGGER, CREATE TYPE, CREATE VIEW.

- Oracle Load Balancing (RAC, Real Application Clusters) is not currently supported due to the integration with Microsoft Transaction Services (via the Distributed Transaction Coordinator Service)

- ARM requires that TNSNames is the first entry specified in the names directory path in the SQLNet file. The ARM v6 installer updates the TNSNames file and also specifies that Authentication Services is set to none.

  Users requiring particular character set support should ensure the NLS settings include the required symbols, e.g. UK users requiring the £ symbol should use a character set such as WE8ISO8859P1.

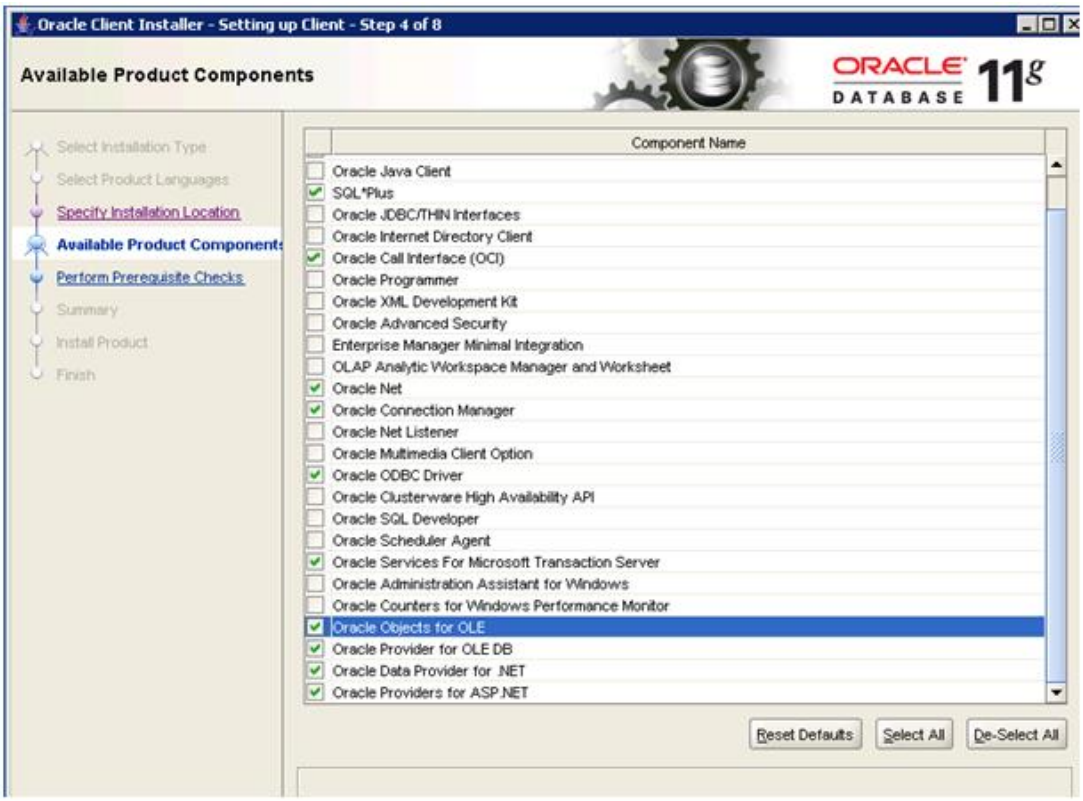
3.1.6 Oracle database Installation

1. Ensure that the Oracle client is installed and setup with a valid TNSNames.ora pointing to your Oracle database server. Check that you can TNSPing the database server from the ARM server.

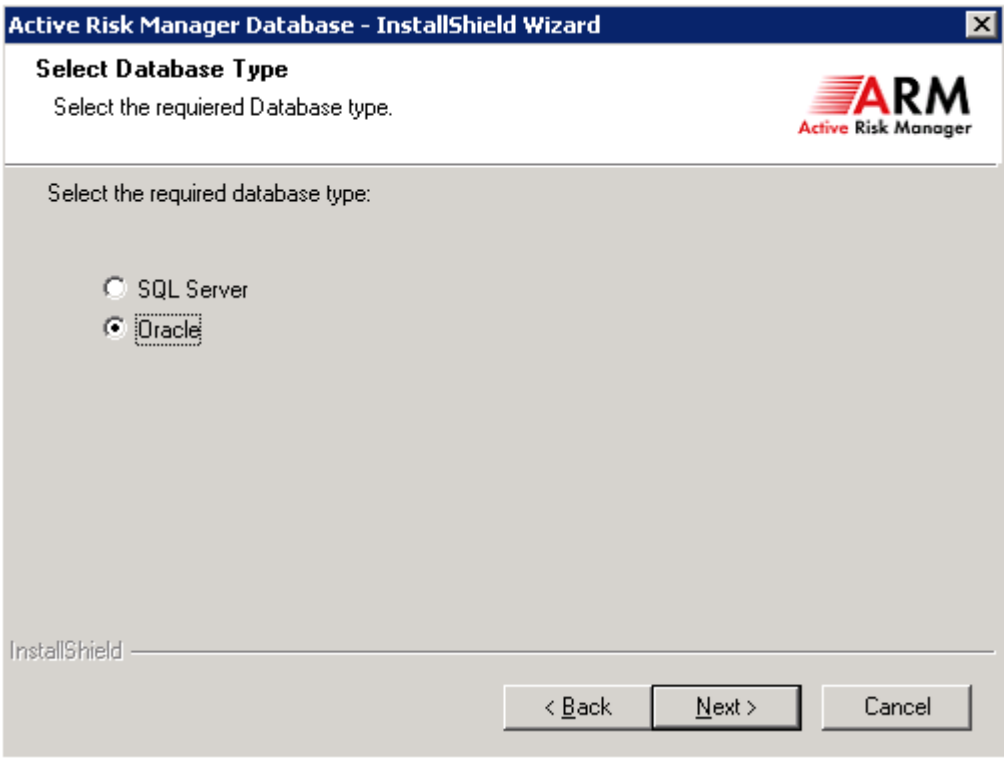
   Note: If the Oracle client is not installed we recommend installing 11.2.0 with the following custom options.

   Run the Oracle Client installer, select Custom. Choose the language and location.

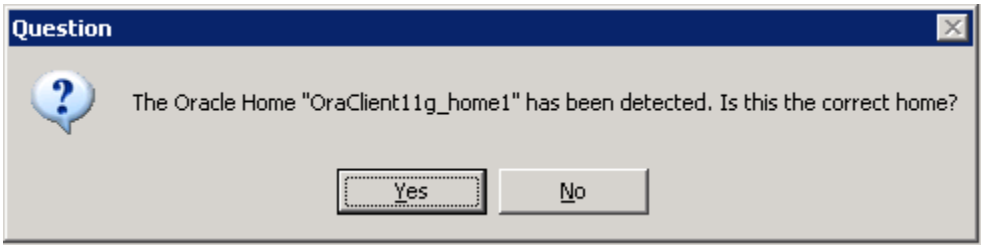
   The following components are required for ARM to work.



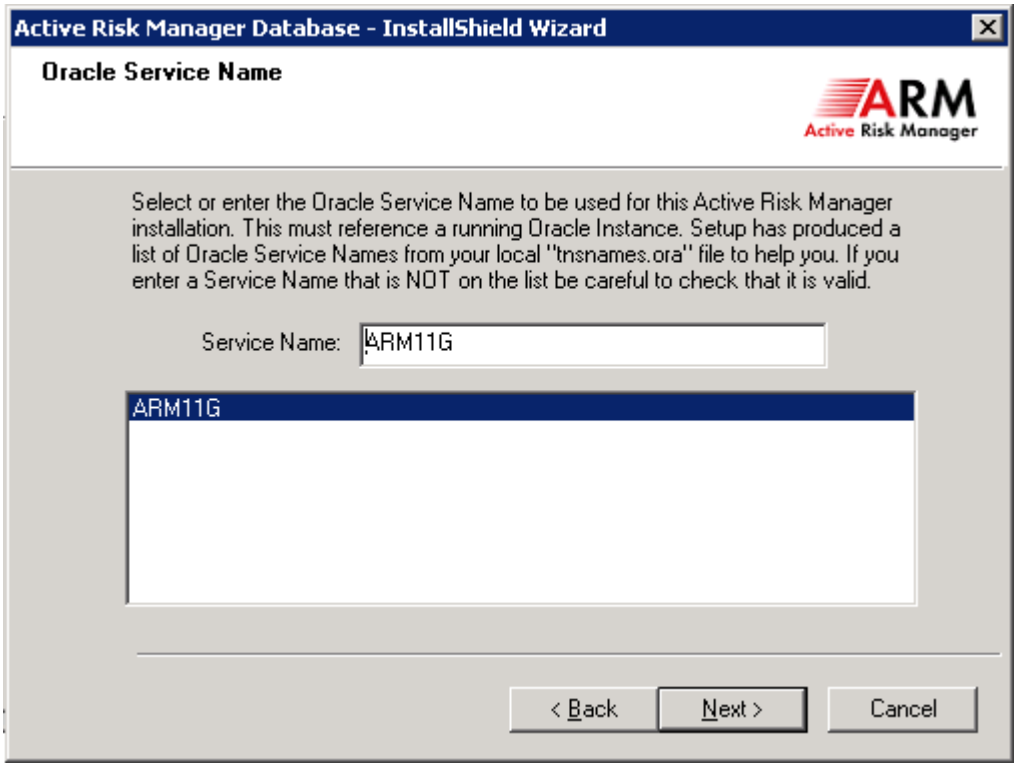
2. To create the ARM schema in an Oracle database choose the Oracle option below.



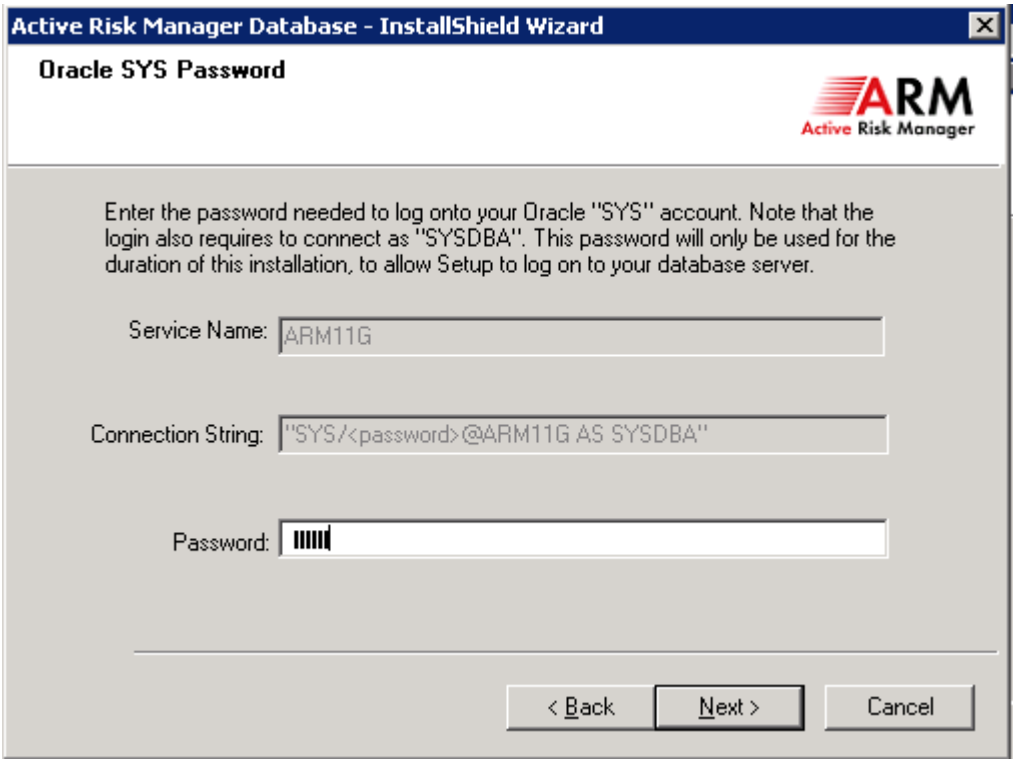
3. A pop up will appear asking you to confirm which Oracle Home to use. If the first one listed is not the one that you wish to use then choose No and then next in the list will be displayed.



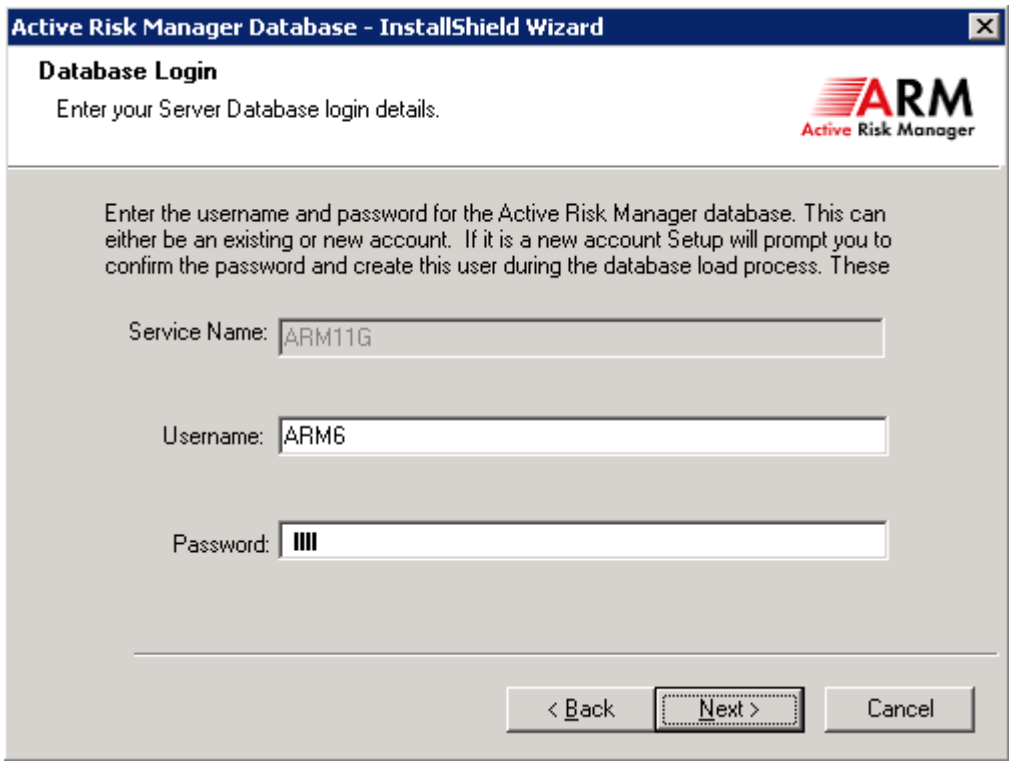
4. The list of Oracle Service Names configured in TNSNAMES.ORA for the home selected will be displayed. Highlight the identifier that references the database to be used for the ARM schema.



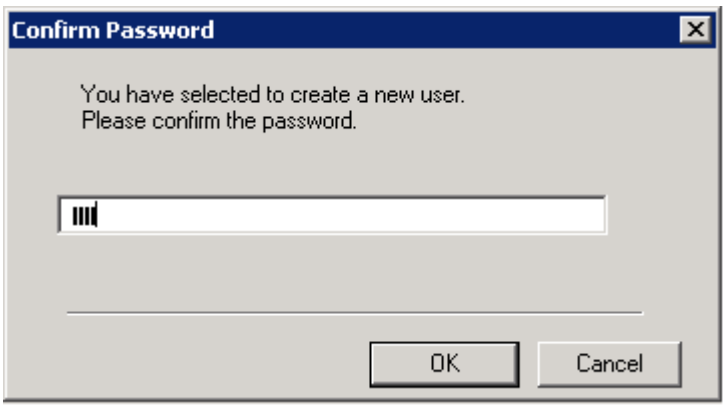
5. To create ARM schema and role, as well as the MTSSYS schema in step 11 the SYS account is required.



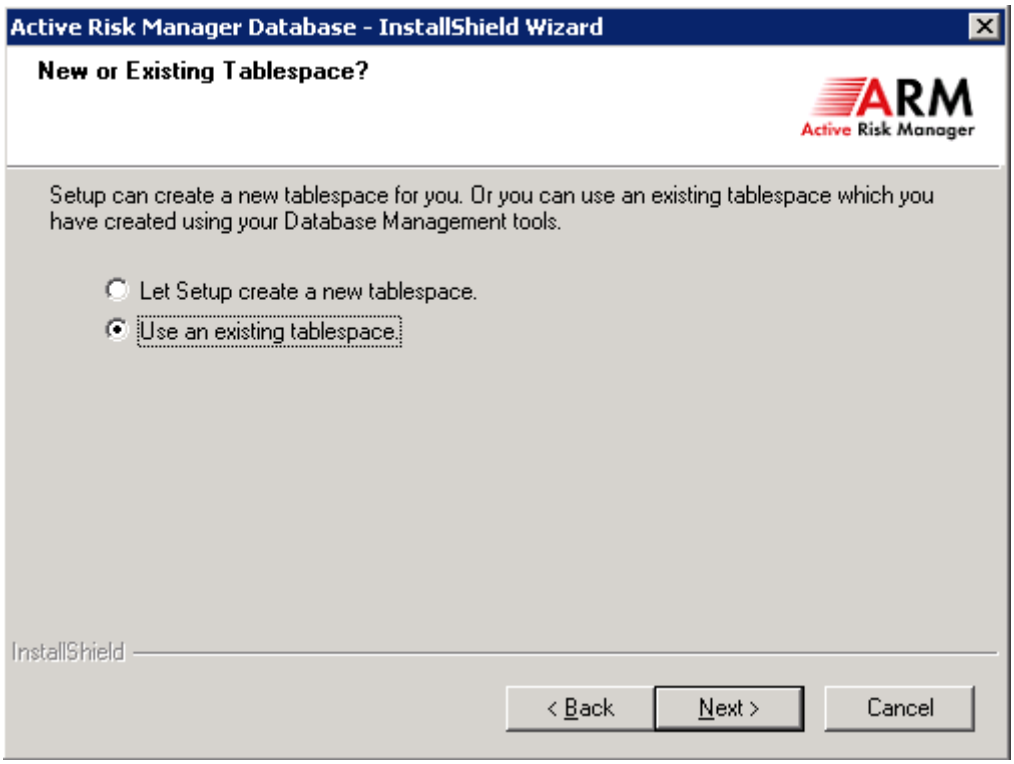
6. Enter the user name and password for the ARM user/schema to be created. The user name should be entered in **CAPITAL** letters.



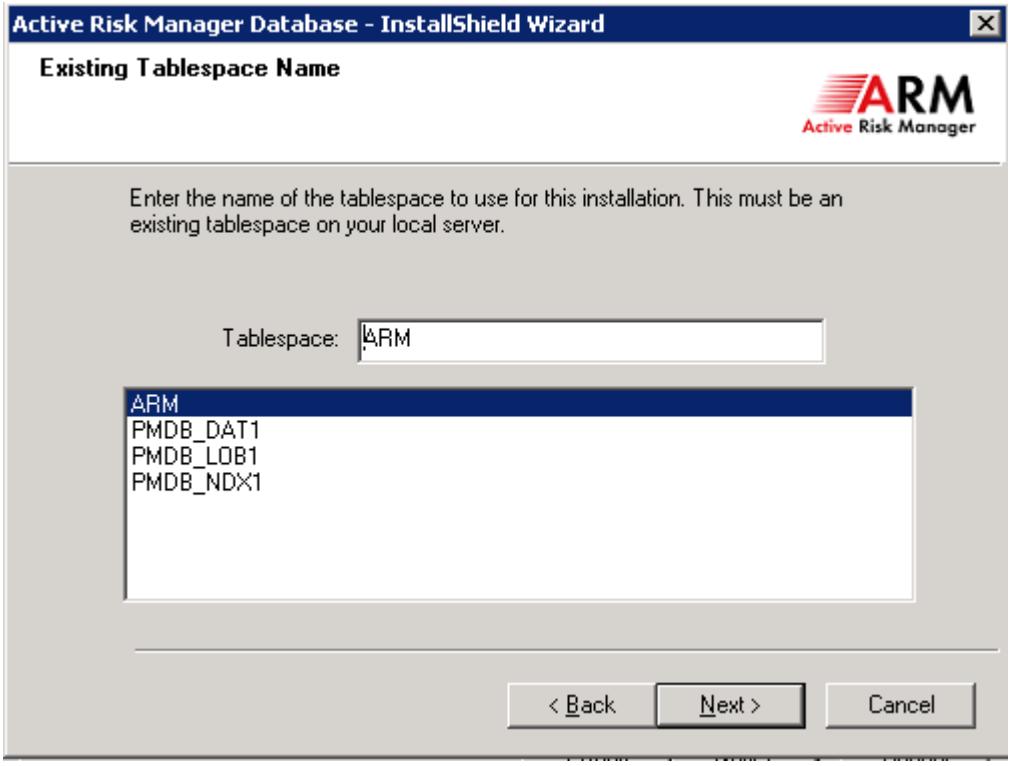
7. Confirm the password.



8. We advise you to create a tablespace in Oracle that meets your local requirements for naming convention and extent management and select ‘Use an existing tablespace’ to continue.



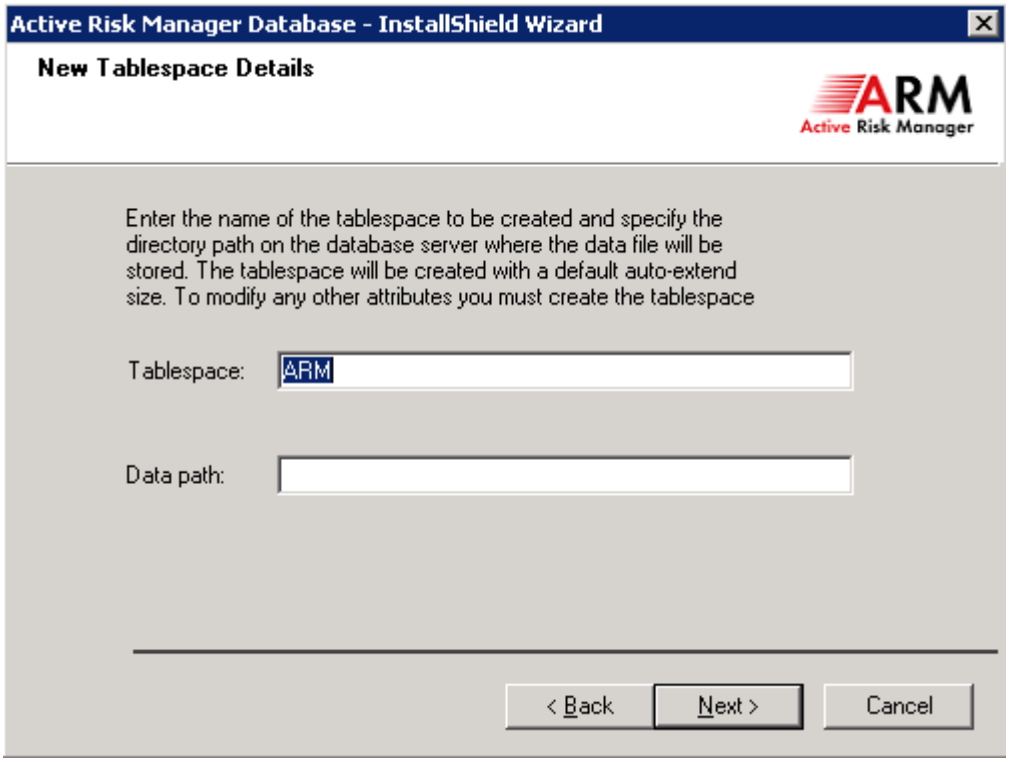
9. Select the tablespace to be used from the list. The USERS tablespace is omitted from the list by default.



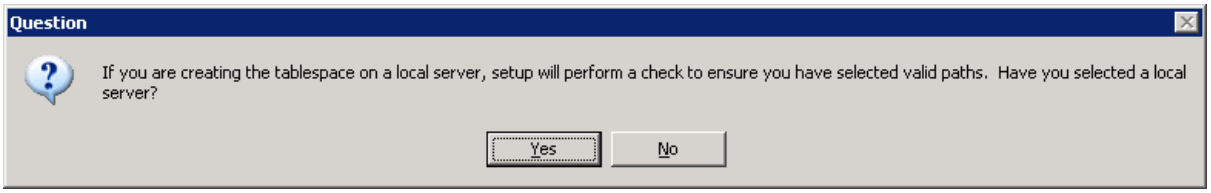
10. If you chose ‘Let setup create a new tablespace’ in step 8, enter the new tablespace name and full data path.

    The following statement will be executed:

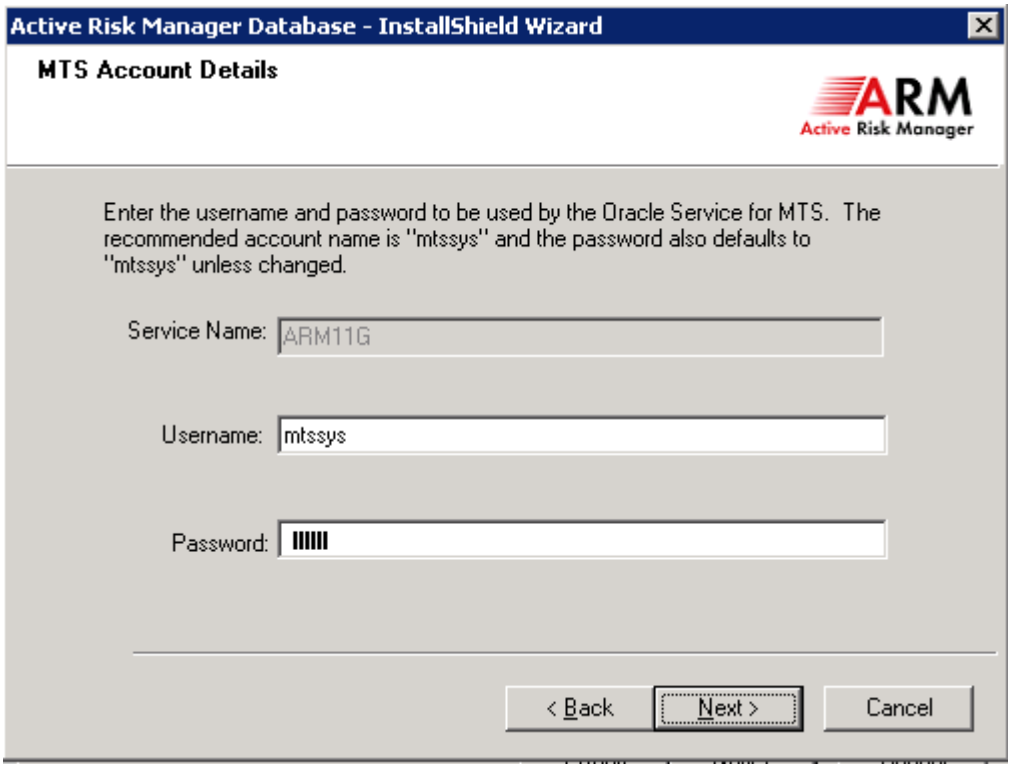
    create tablespace <TABLSPACENAME> datafile <PATH>+<TABLESPACENAME>.ORA' size 30M autoextend on;m



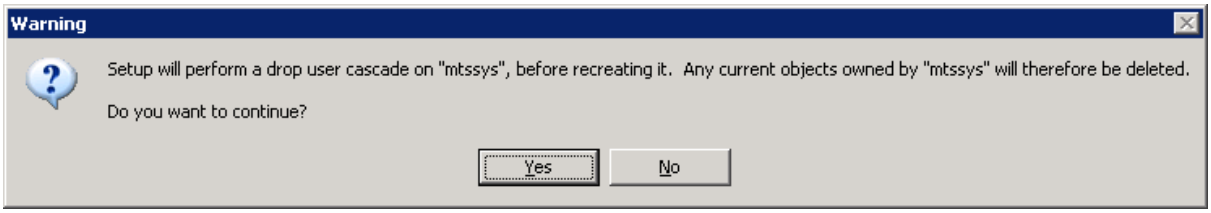
11. Confirm that the path used in the previous step above is valid before continuing.



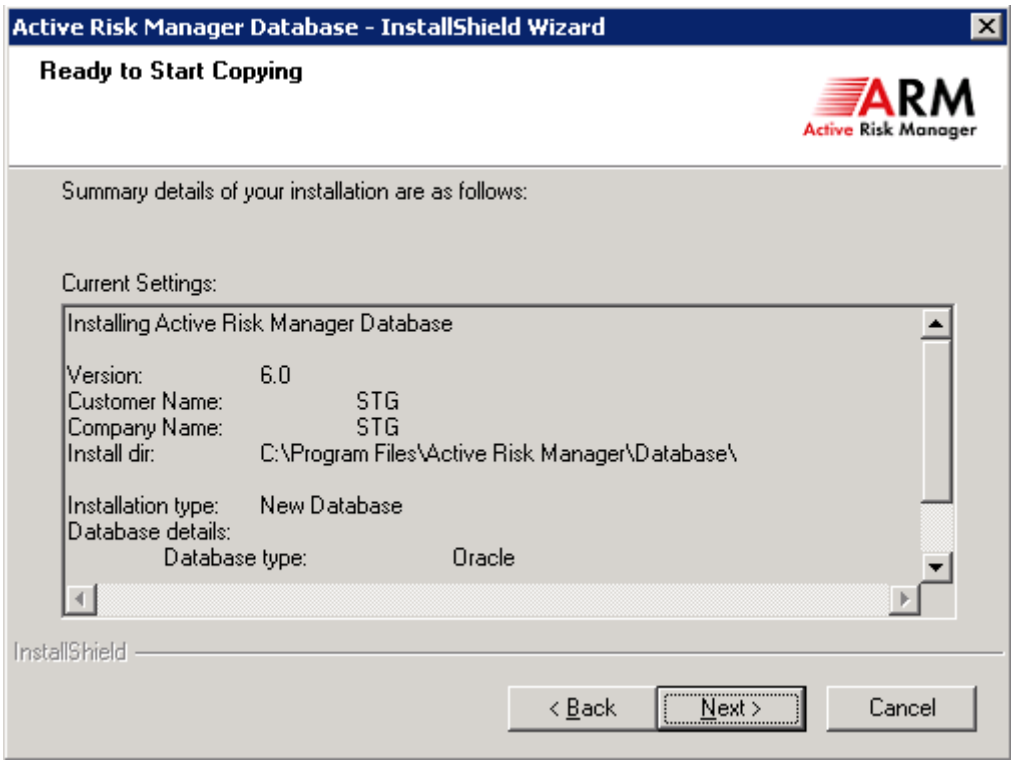
12. Enter the username as password to be used for the MTSSYS (uppercase) schema which controls the distributed transactions with MSDTC. The defaults are MTSSYS/mtsys but these can be changed as required.



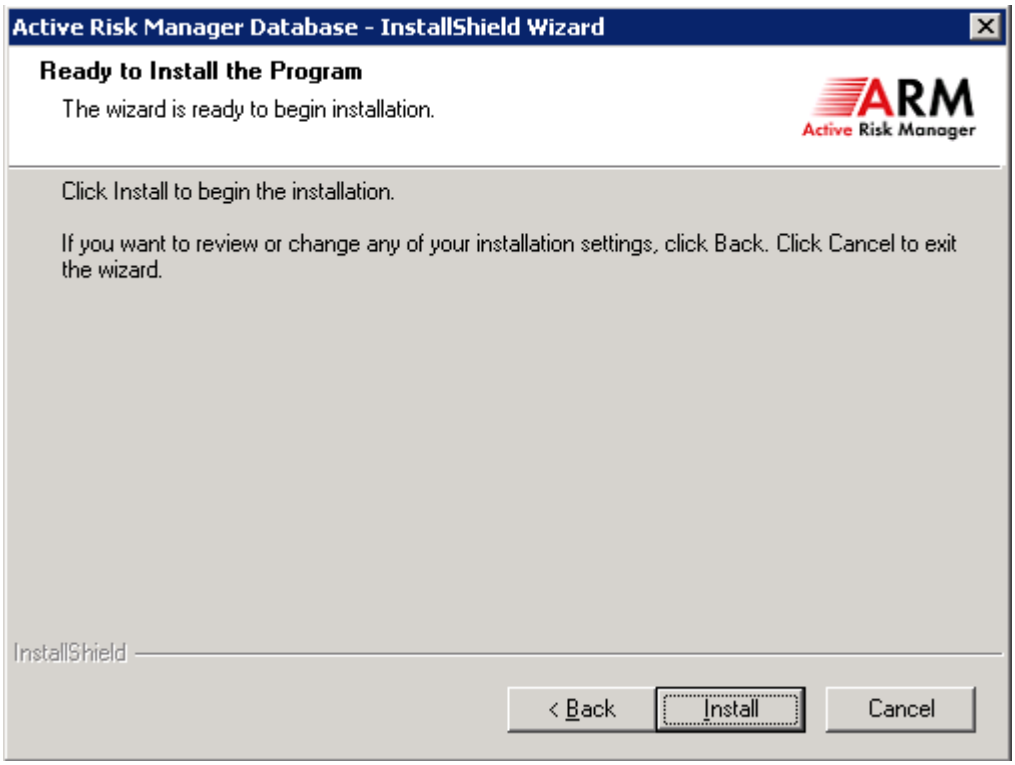
13. If the MTSSYS schema has been created in this database previously you will receive the following message. It is simply warning you that the user will be dropped and recreated; there is no associated risk as long as no users are active in another ARM schema within the same database.



14. Check and confirm the installation options selected.



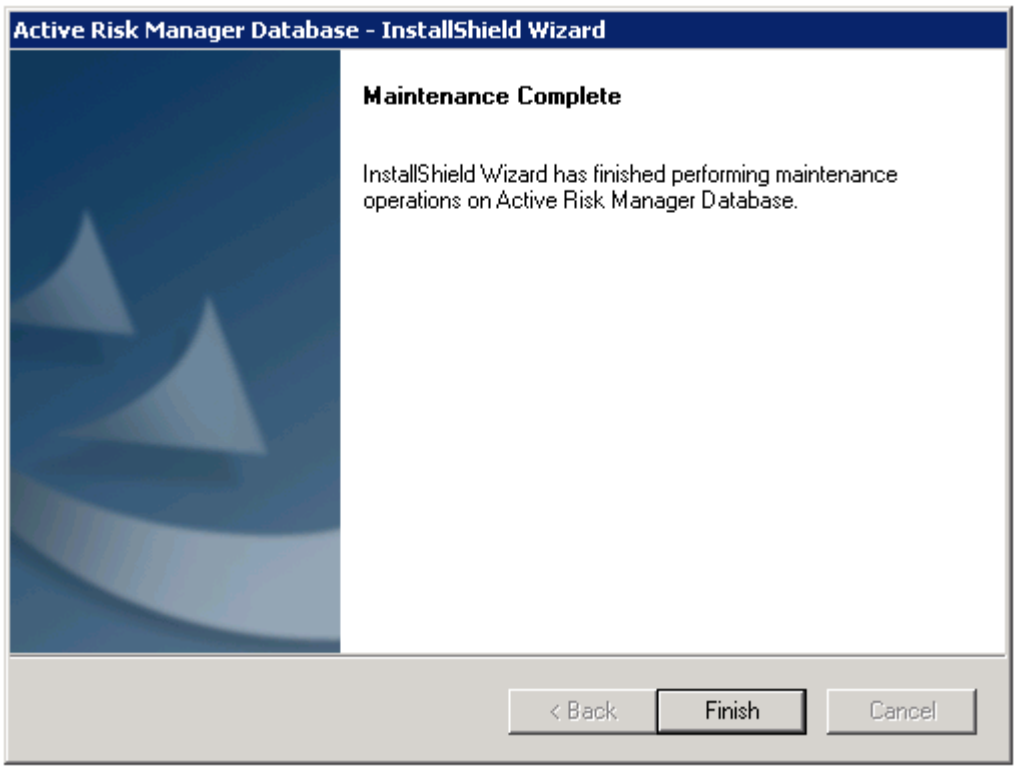
15. Click Install, to begin creating the ARM database schema.



16. Once successfully completed you will be presented with the following pop up message.

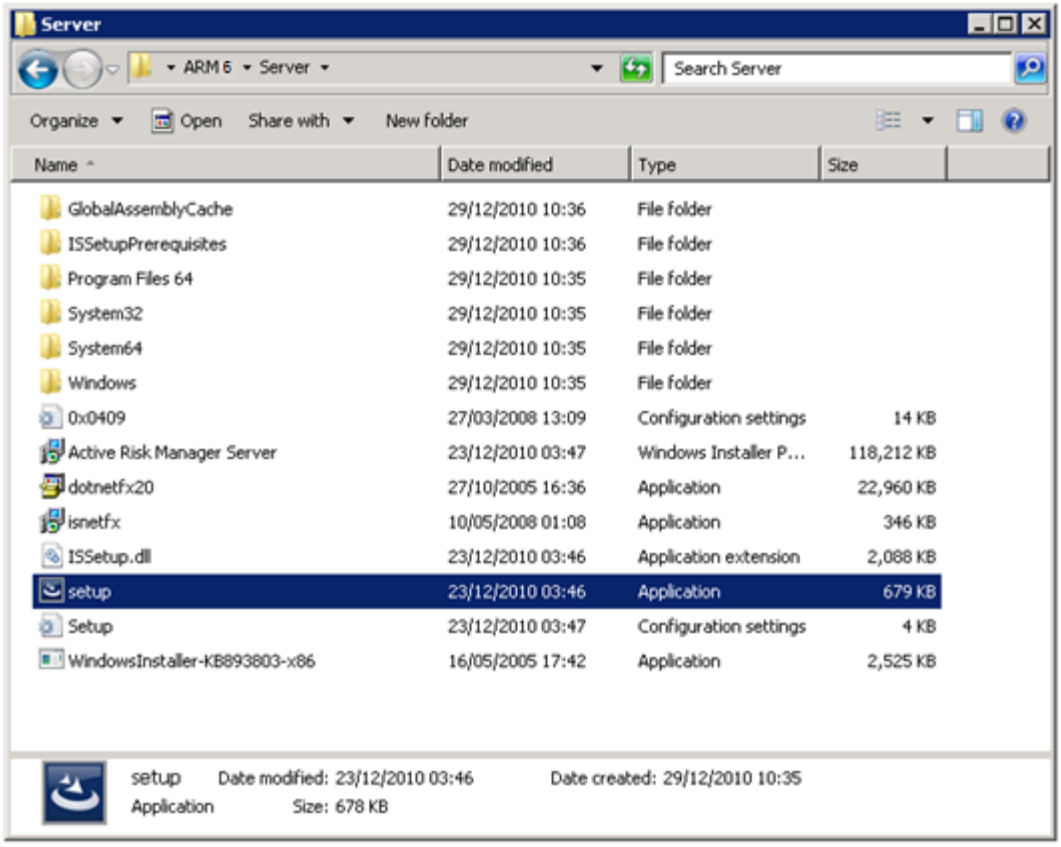
    If any errors are reported please follow the instructions and contact Active Risk Support.

17. Click Finish to exit installation.

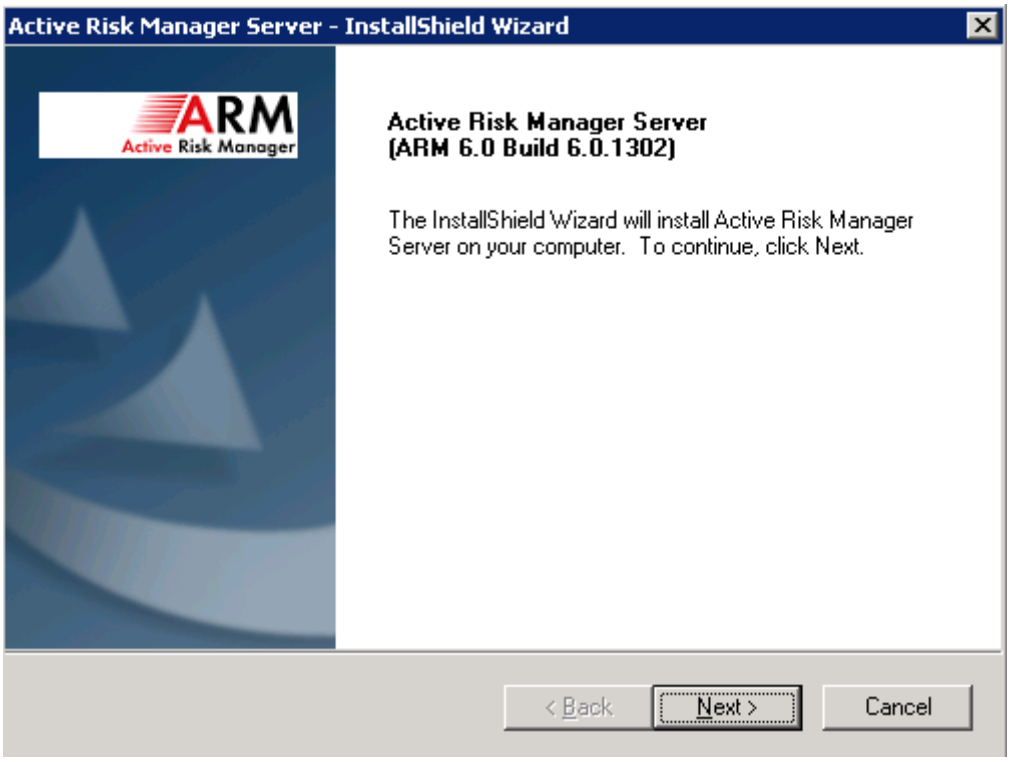


3.2 Application Server Installation

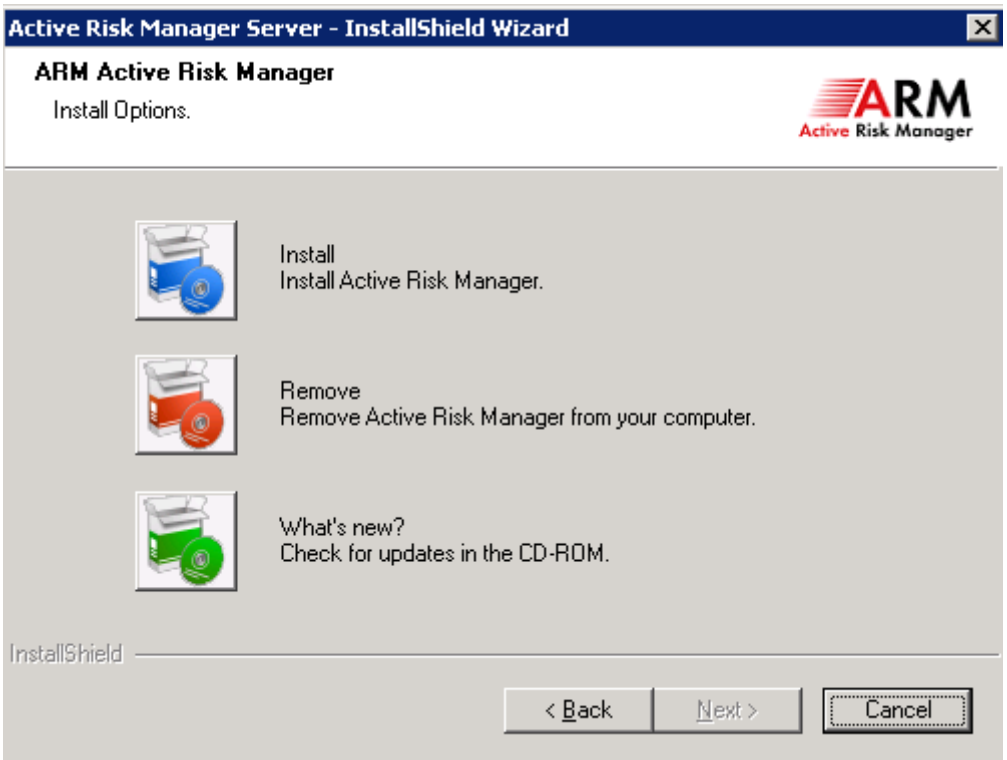
1. This section covers ARM Application installation.
2. Within ARM installation media navigate to the ***Server*** folder and right click on *setup.exe* and select “Run as administrator” if applicable to execute.



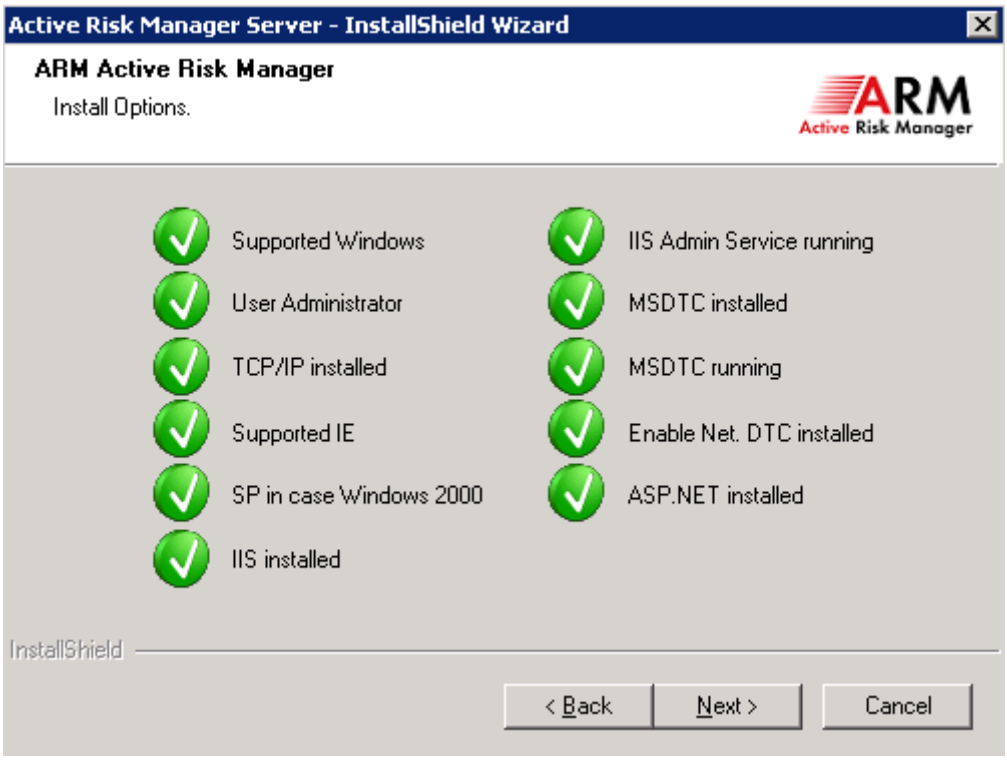
3. Click Next as displayed below to continue with the installation wizard.



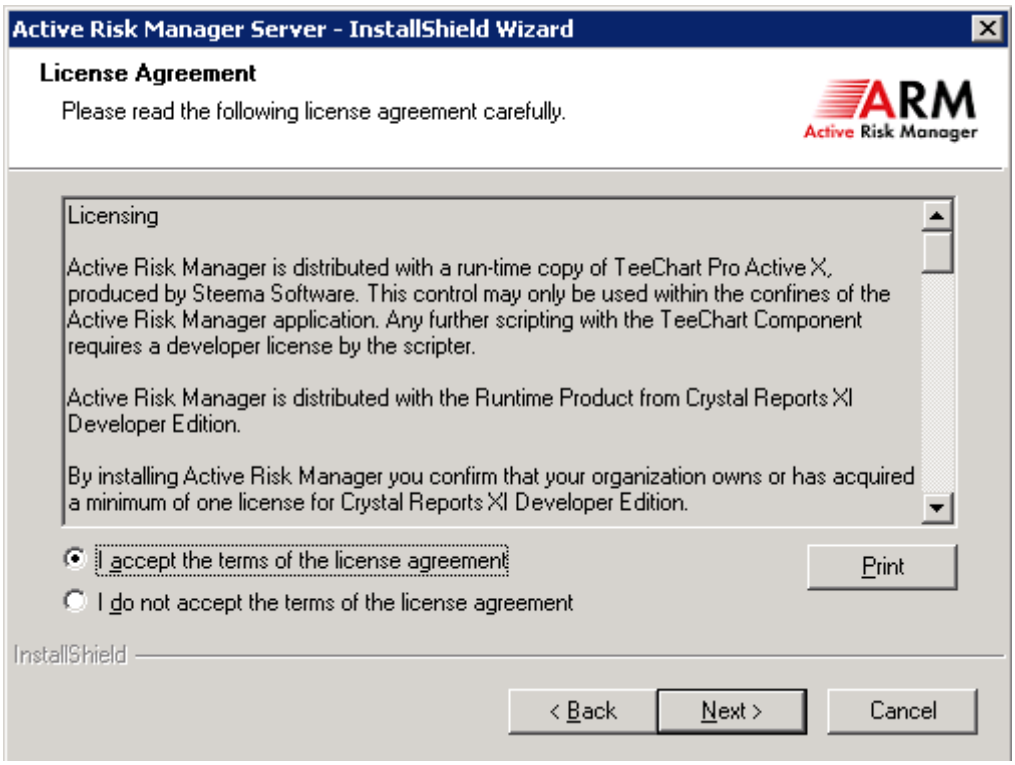
4. Choose the Install option. This is to install a fresh copy of ARM Application Server.



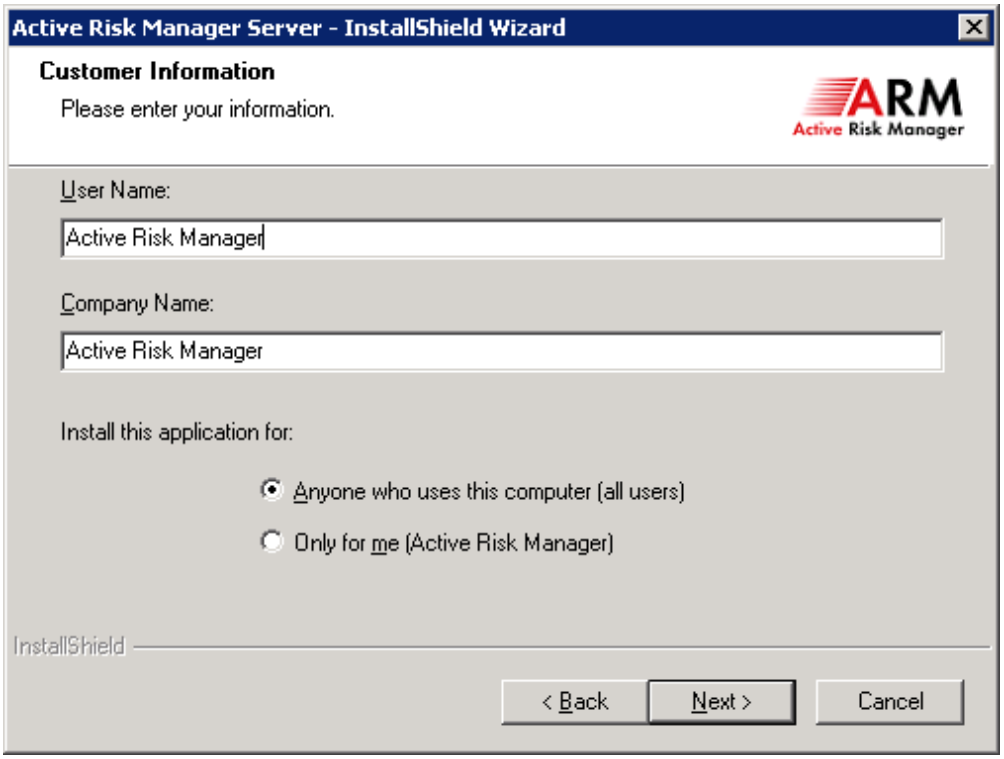
5. The installer will check for the common pre-requisites in the next step. Once completed click Next to continue.



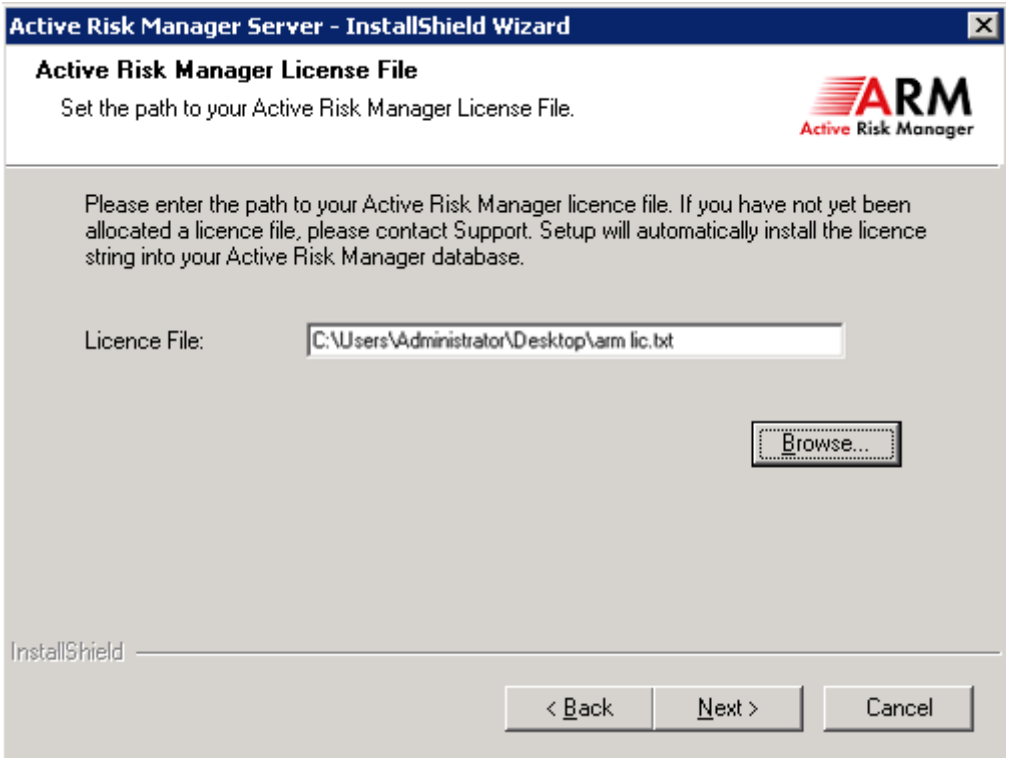
6. Next screen presents license information, read through the licence agreement, accept the terms and click Next to continue.



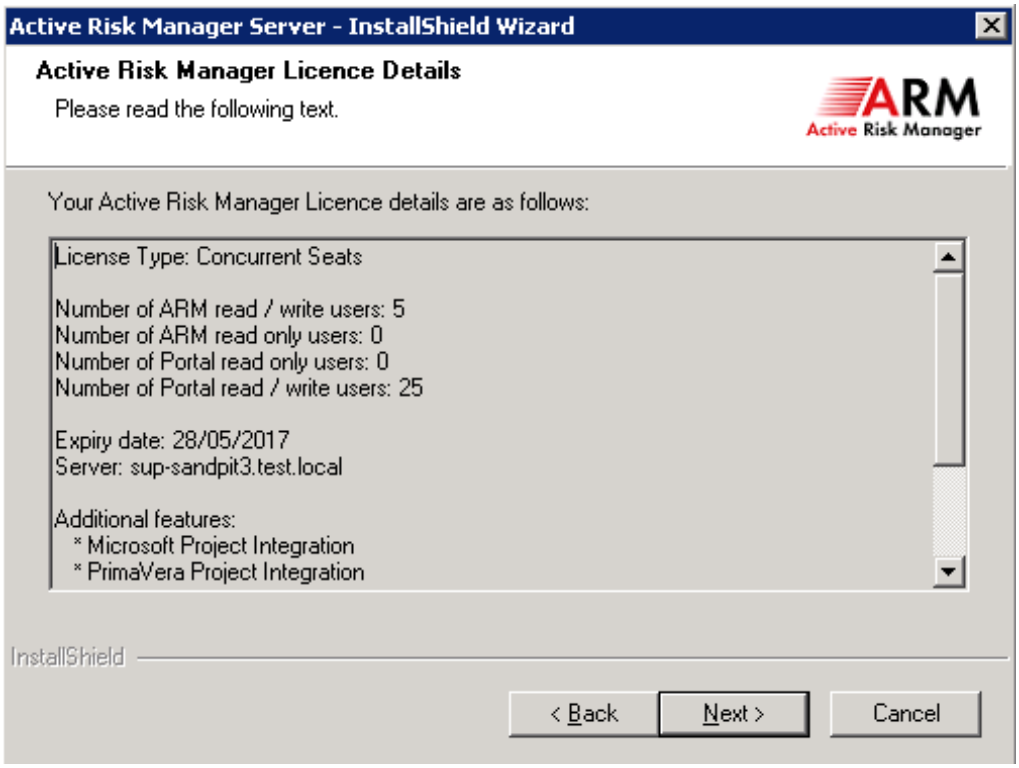
7. Type your User Name and Company Name in to the correct fields. Select who you want the application to be available to.



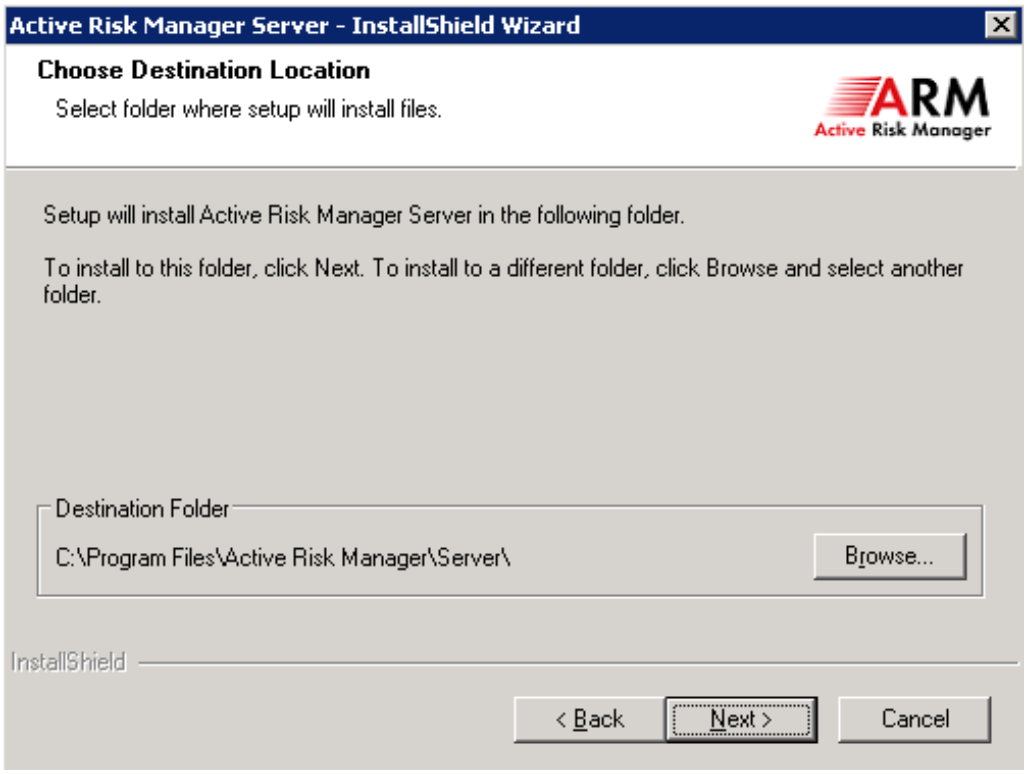
8. Browse and locate the ARM licence file. If you do not have one created yet, please contact your account manager.



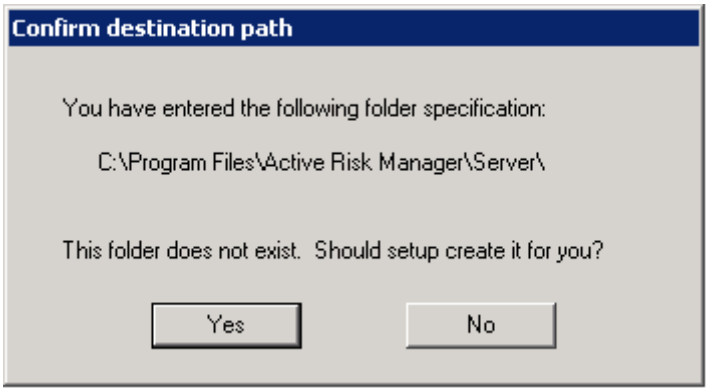
9. Confirm the licence details match your requirements.



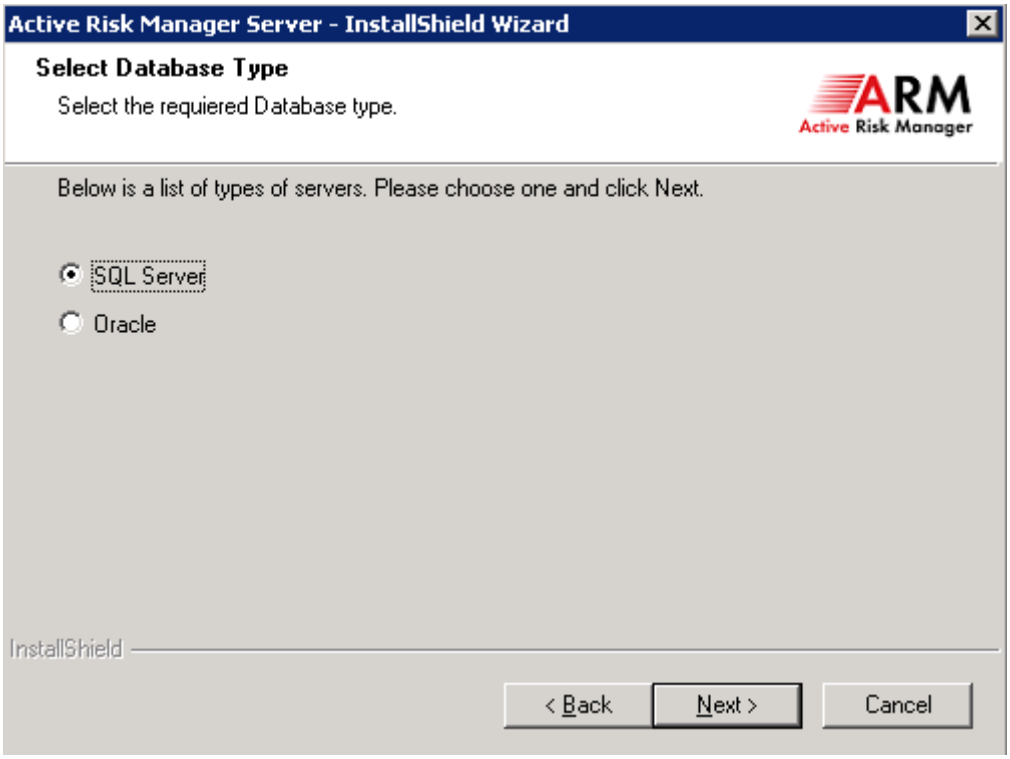
10. Choose a destination for the ARM installation files. We recommend using the default location.



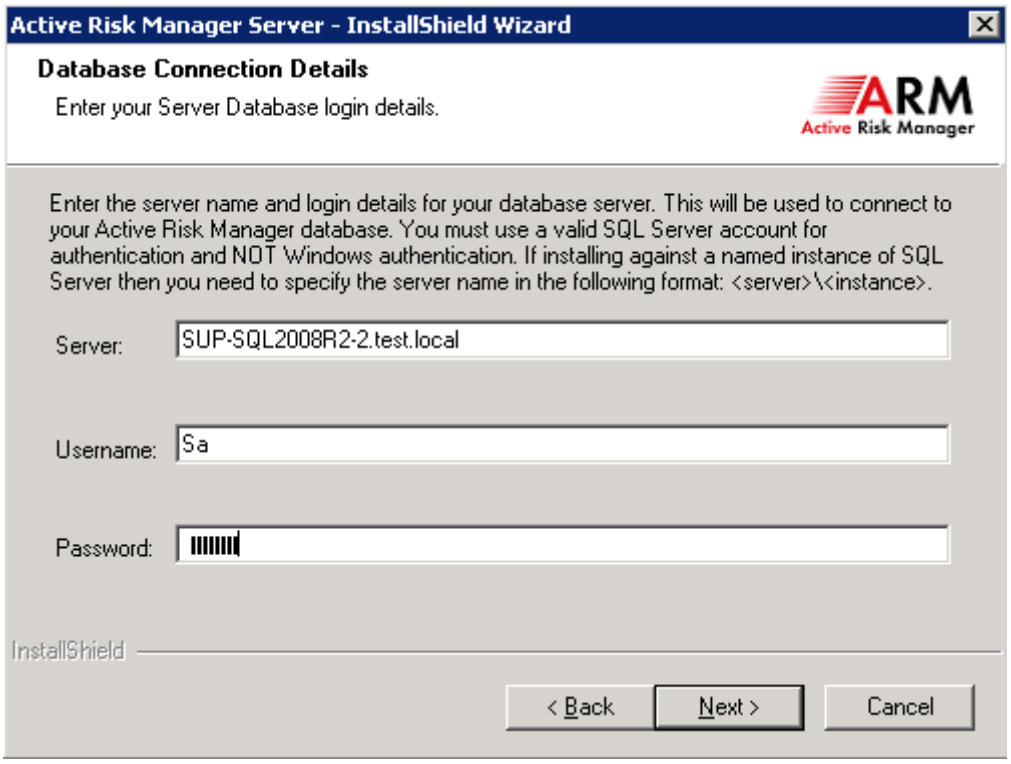
11. You may be asked to create the folder as it does not exist, click Yes to continue.



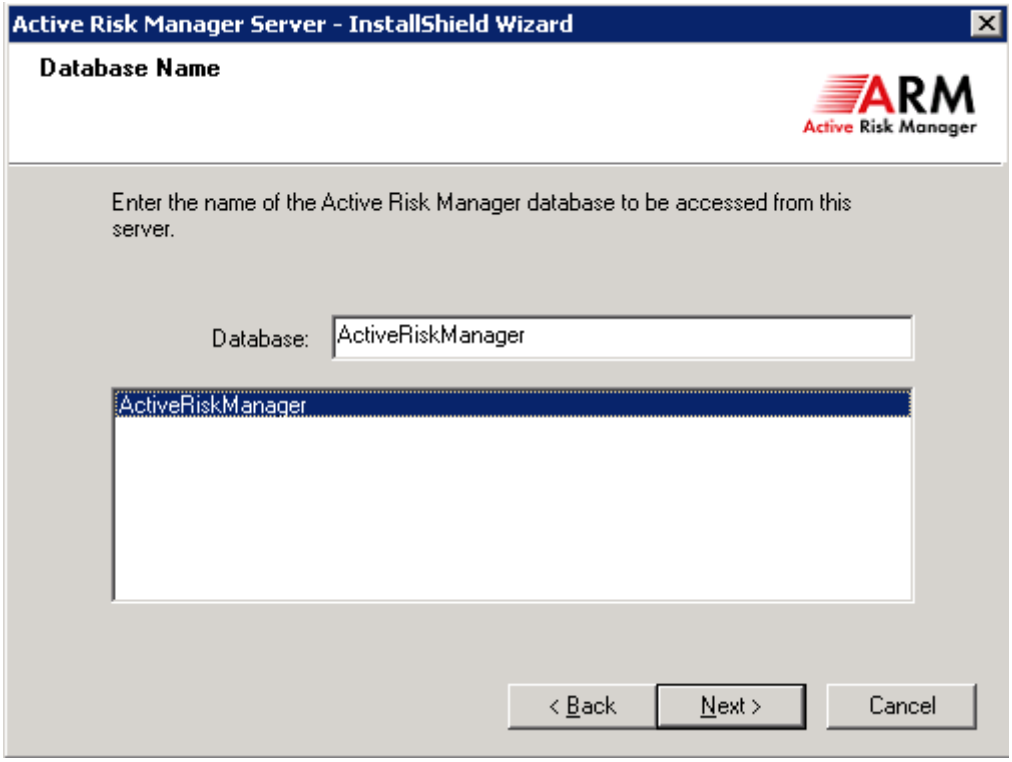
12. Choose between SQL Server and Oracle for the ARM database. For a SQL Server installation remain on this step, for an Oracle installation go to step 13.



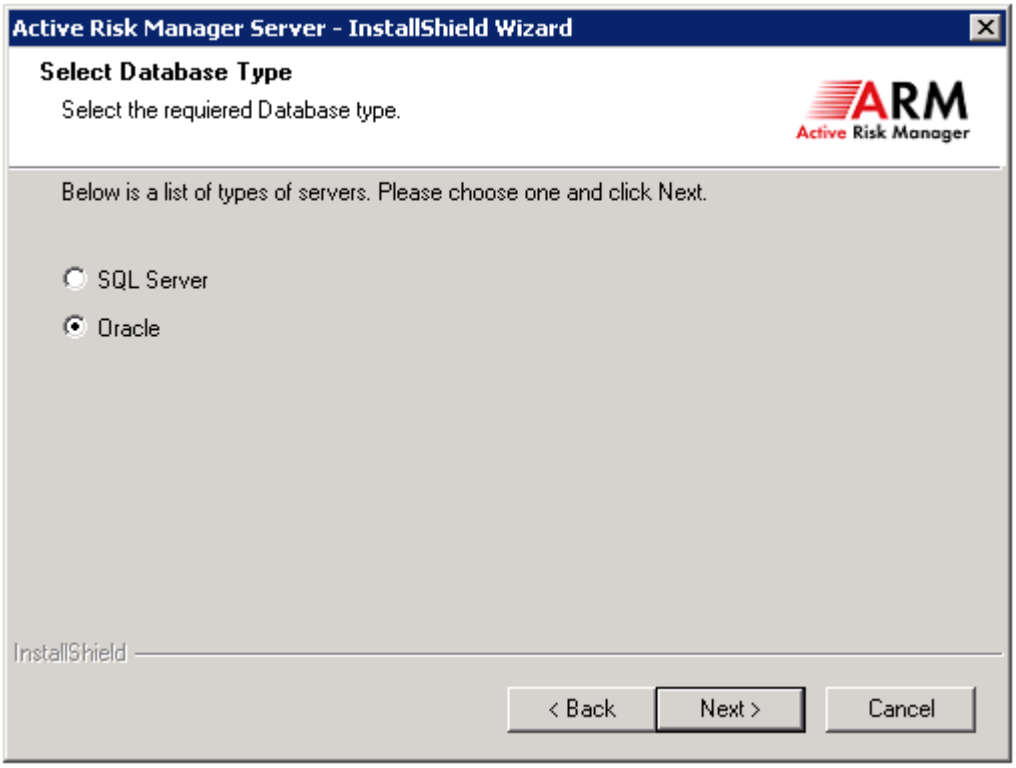
13. Enter the hostname or IP address of the database server and user credentials for the SQL Server database.



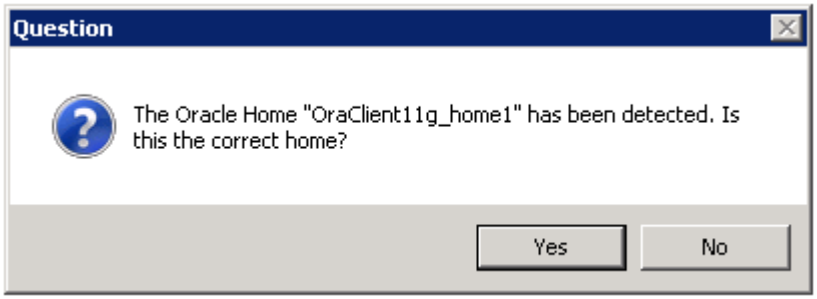
14. Select the database to be used as the default instance from the list provided. You will be able to add additional instances from within the application once it is installed.



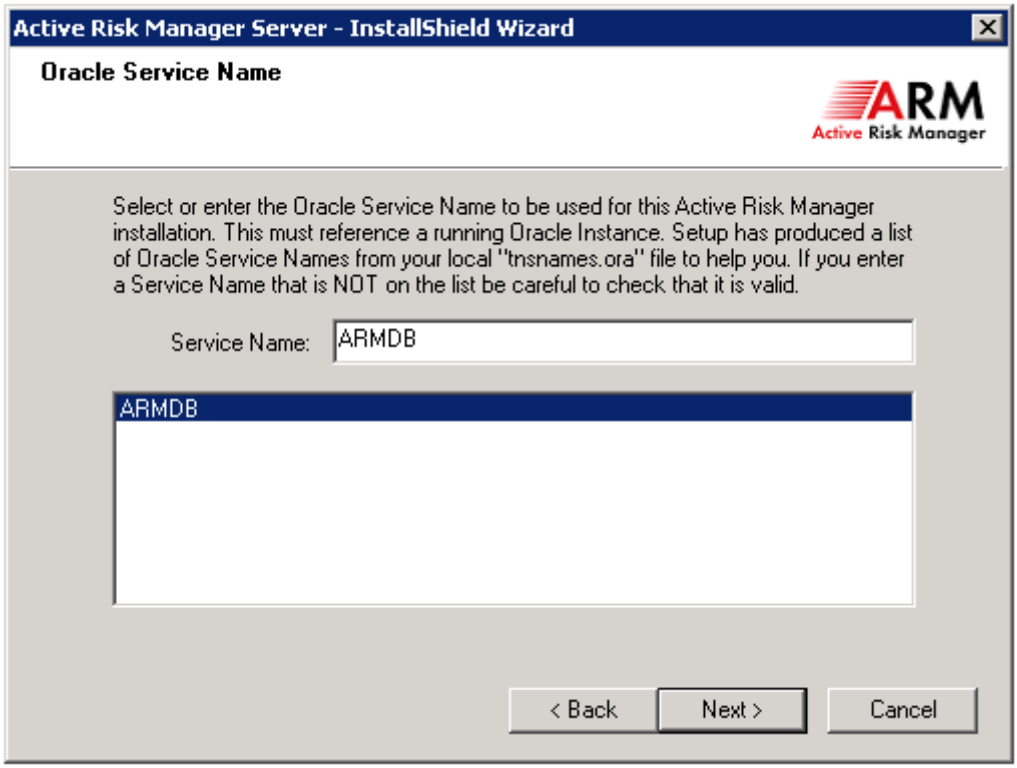
15. For Oracle installs select the Oracle option below, if SQL go to step 10



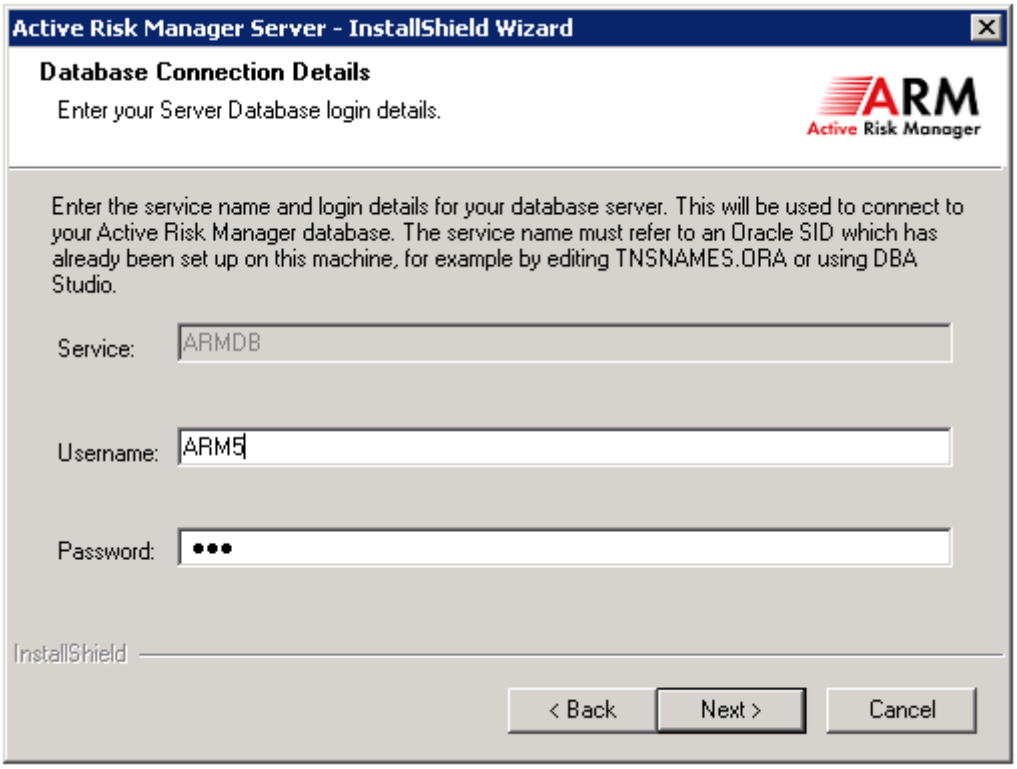
16. A pop up will appear asking you to confirm which Oracle Home to use. If the first one listed is not the one that you wish to use then choose No and then next in the list will be displayed.



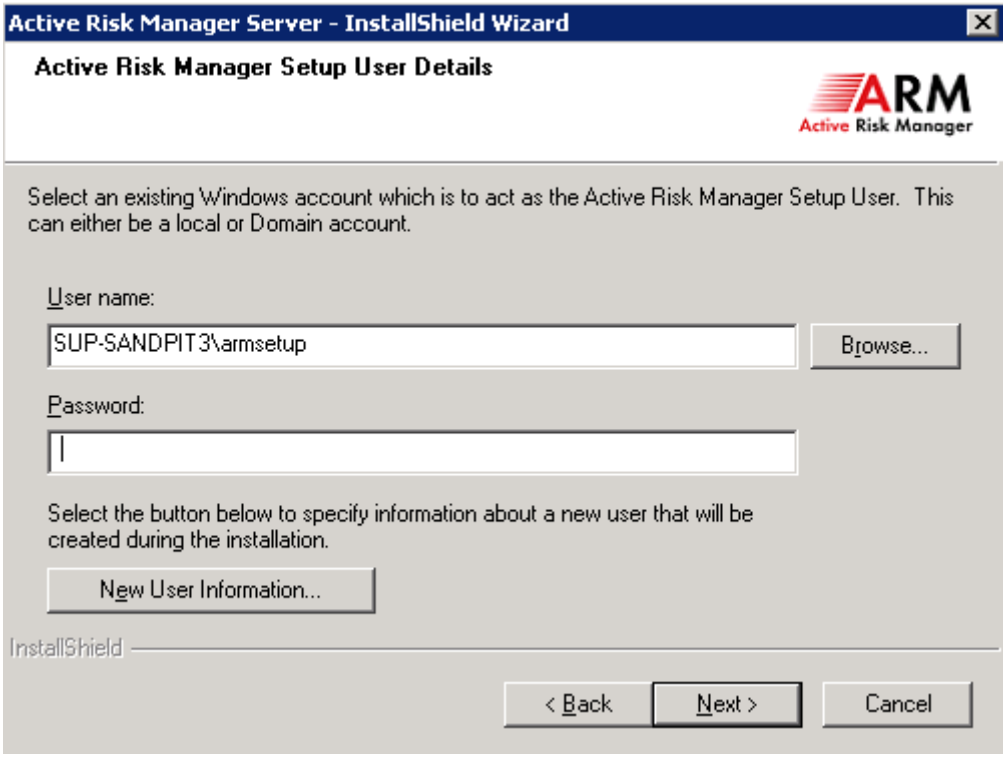
17. The list of Oracle Service Names configured in TNSNAMES.ORA for the home selected will be displayed. Highlight the identifier that references the database to be used for the ARM schema.



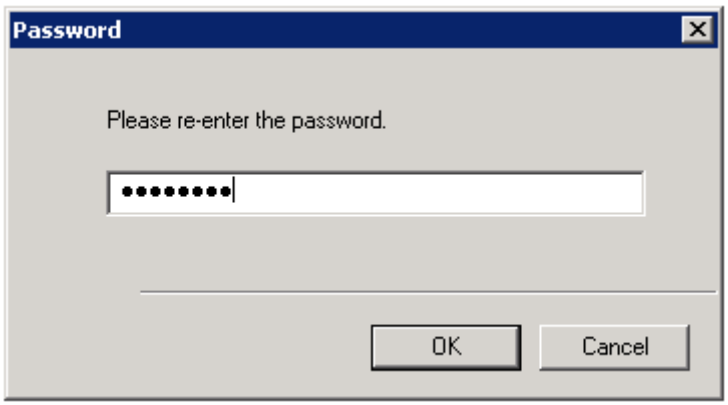
18. Enter the username and password for the ARM database schema. (Ensure that the username is entered in UPPERCASE)



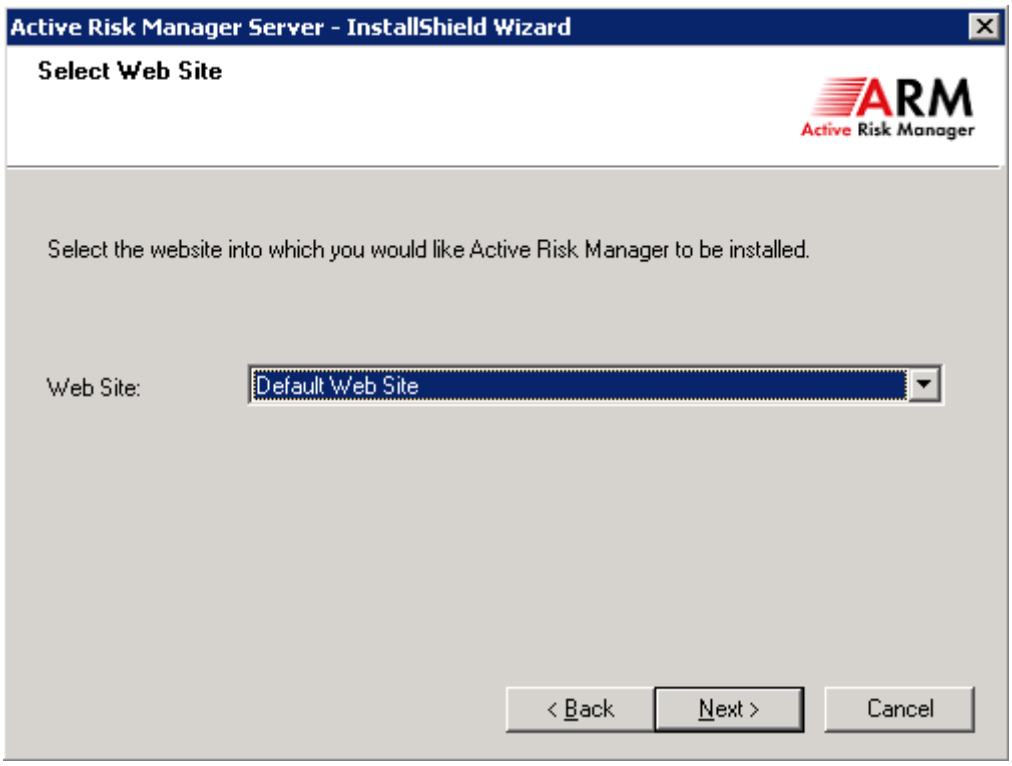
19. Enter the domain\user and password for the ARM service account. This will also be the super admin user for configuring additional instances and mail server settings and initially adding new users. This account must be in the local administrators group.



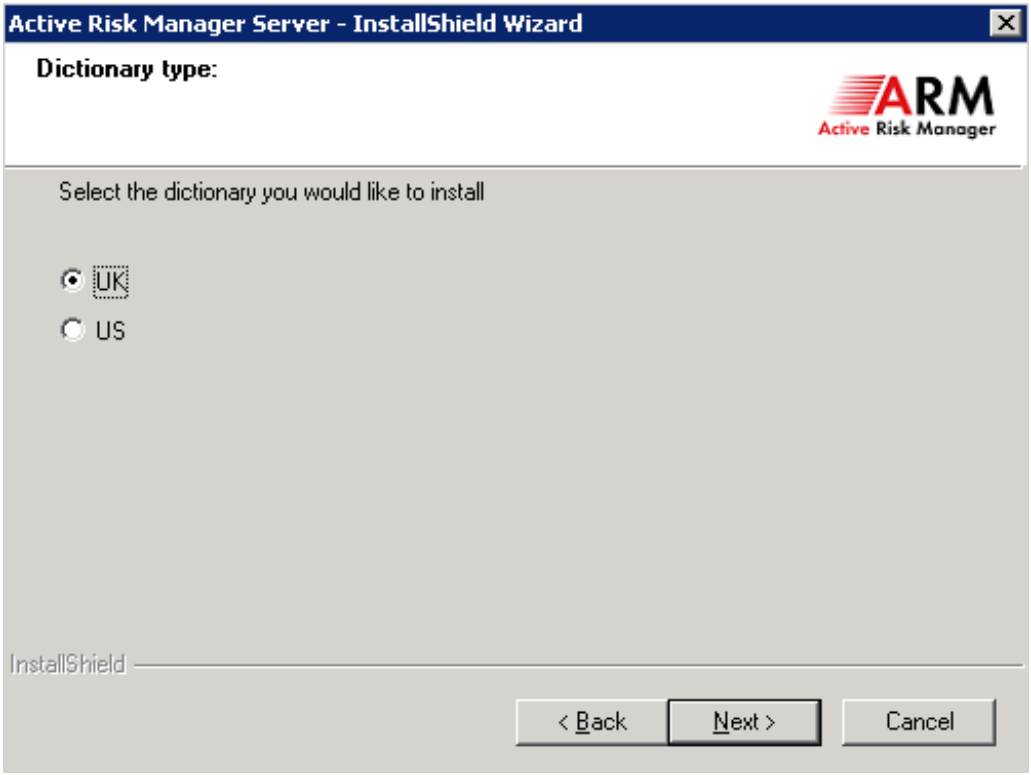
20. Confirm the password entered in the previous step.



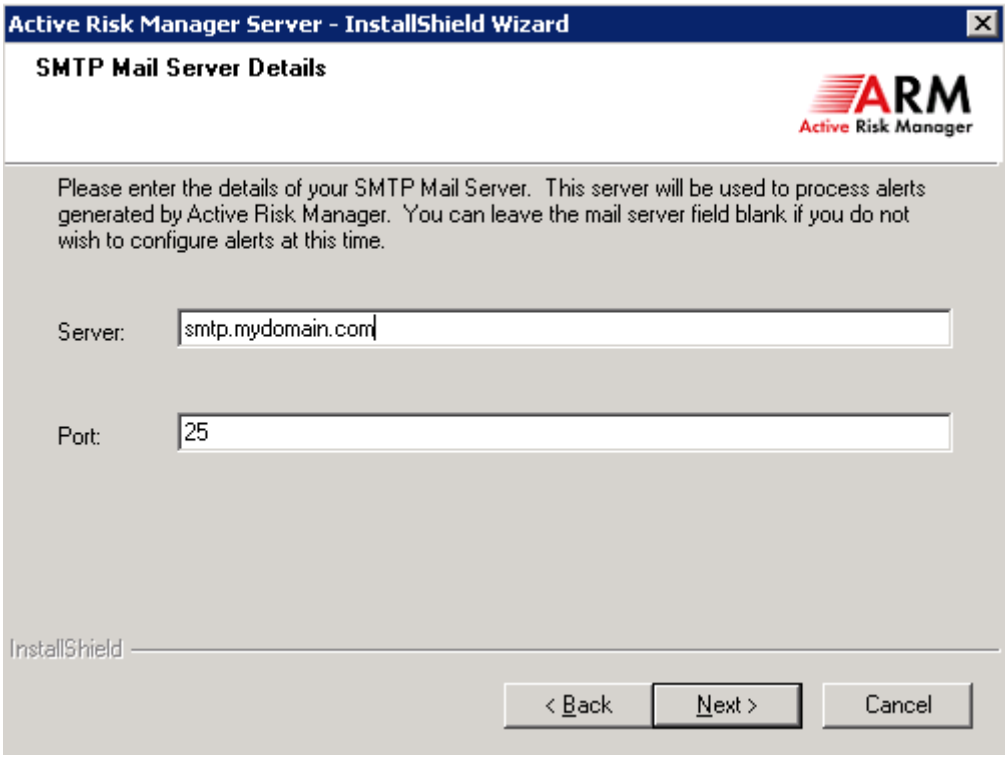
21. Select the IIS website that you wish the ARM application to be created in. Websites must be configured through IIS beforehand if you do not wish to use the default.

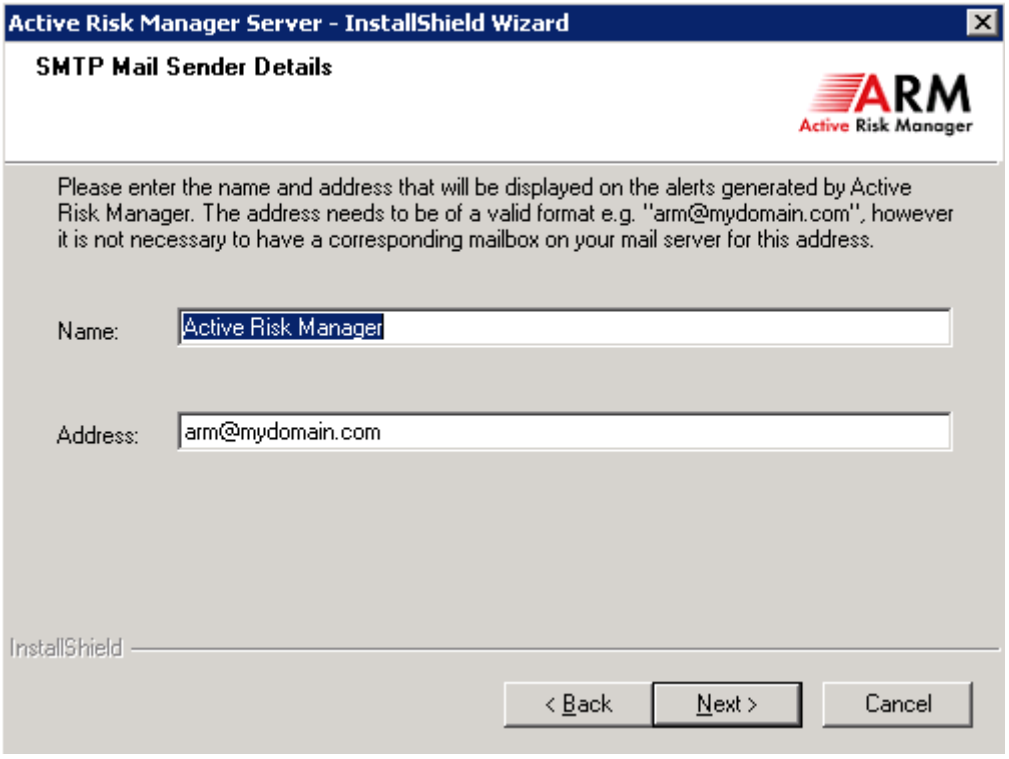


22. Select the appropriate dictionary type.

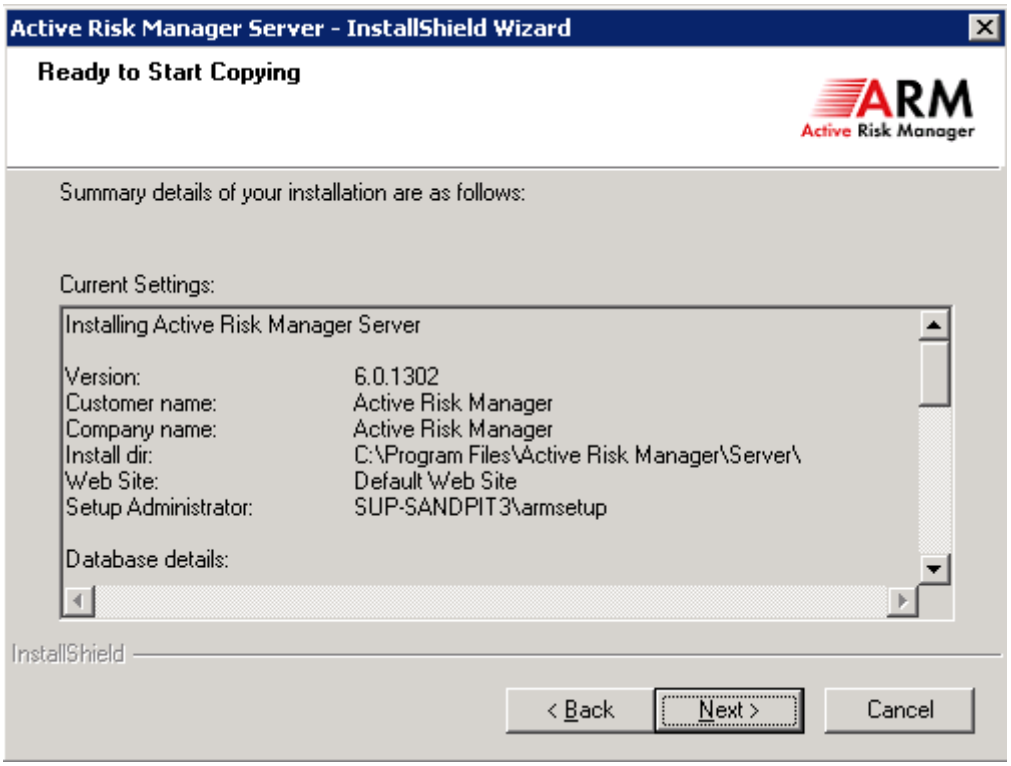


23. If you want to use the ARM email alerts functionality enter the smtp mail server details. If not initially require these can be left blank and configured at a later date.

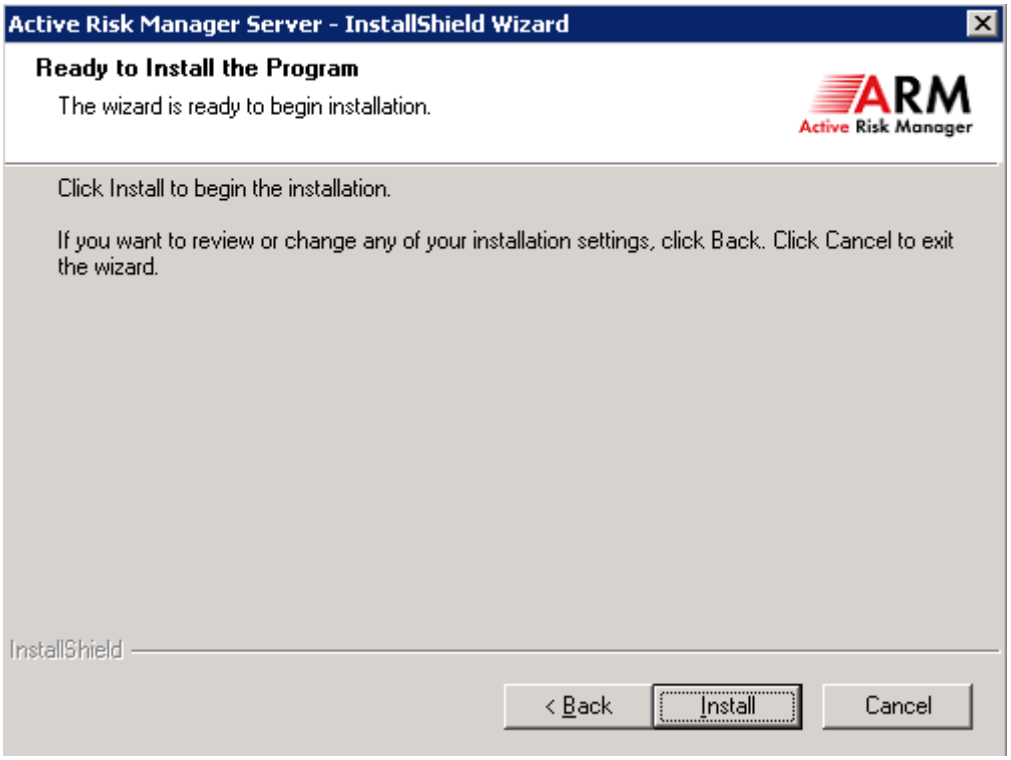




24. Review the installation details.

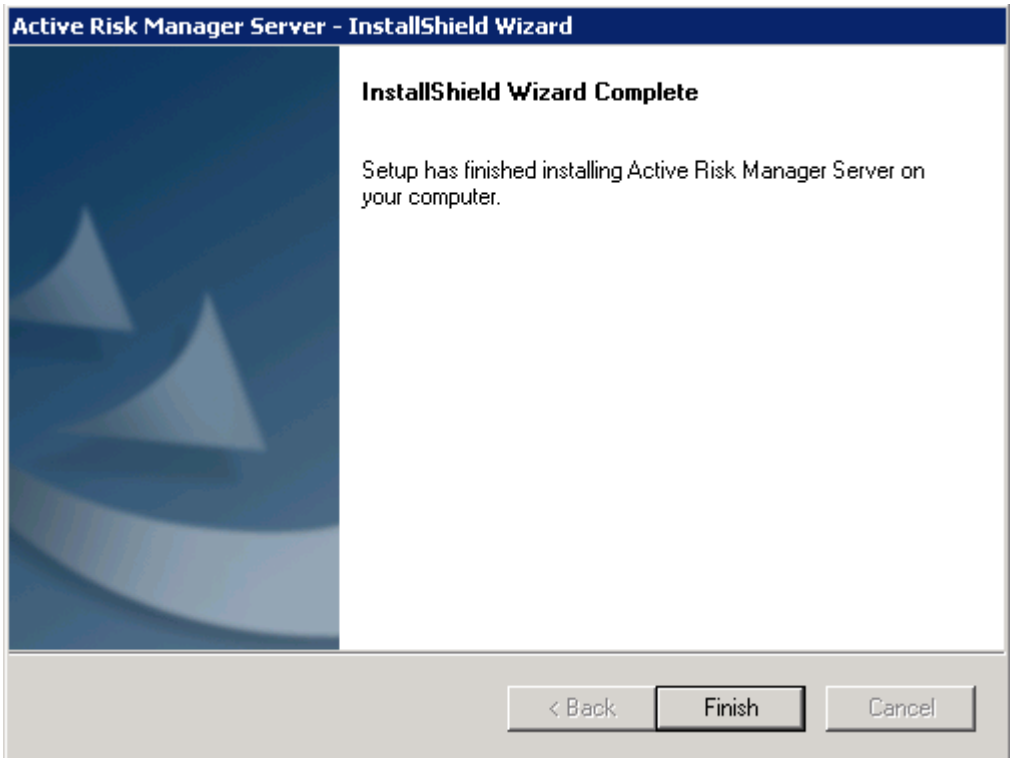


25. Click the Install button to begin the installation process.



26. Oracle installations may have the message below displayed. This is simply to inform you that the SQLNET.ORA file had to be updated to be compatible with ARM.

27. Once complete you will find a dialog as below.



4 Upgrade from Previous Release

You need to consider the following before upgrading to ARM 6:

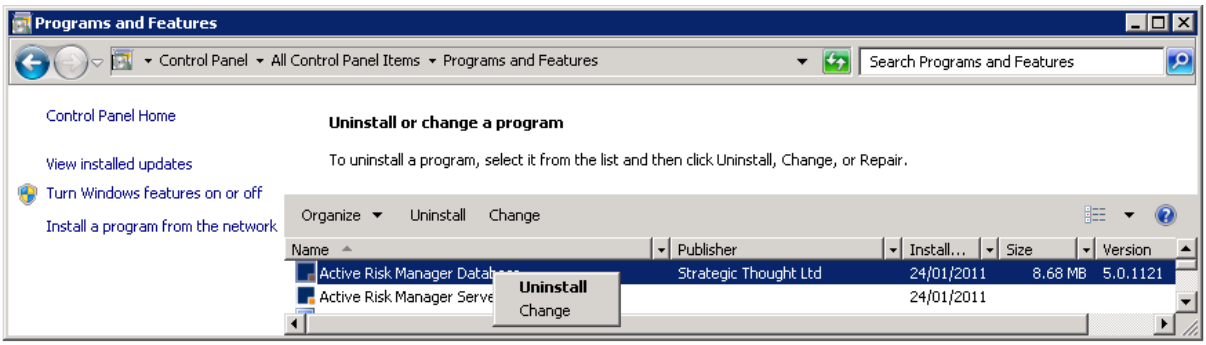
- ARM Filters from releases prior to ARM 5 are not automatically upgraded. These can be migrated after upgrade by going into ARM->Setup and then under the Maintenance tab clicking Migrate Filters to launch Filter Migration Dialog. Filters present in ARM 5 onwards will be automatically migrated.
- Crystal Reports is ***NOT*** supported with ARM 6.
- Ensure that you review the Support Matrix spreadsheet which contains the supported integration applications and their versions that work with ARM 6. This is provided in the Docs folder on the ARM 6 media.
- If there are firewalls in the environment into which you are deploying ARM, make sure you read and understand section 14 of this document – "Firewall Considerations"
- Make sure that the person who performs the installation has system administrator privileges to the ARM server and the DB environment.
- Make sure you have an ARM licence for the ARM server before proceeding with the application server upgrade.

4.1 Database Upgrade

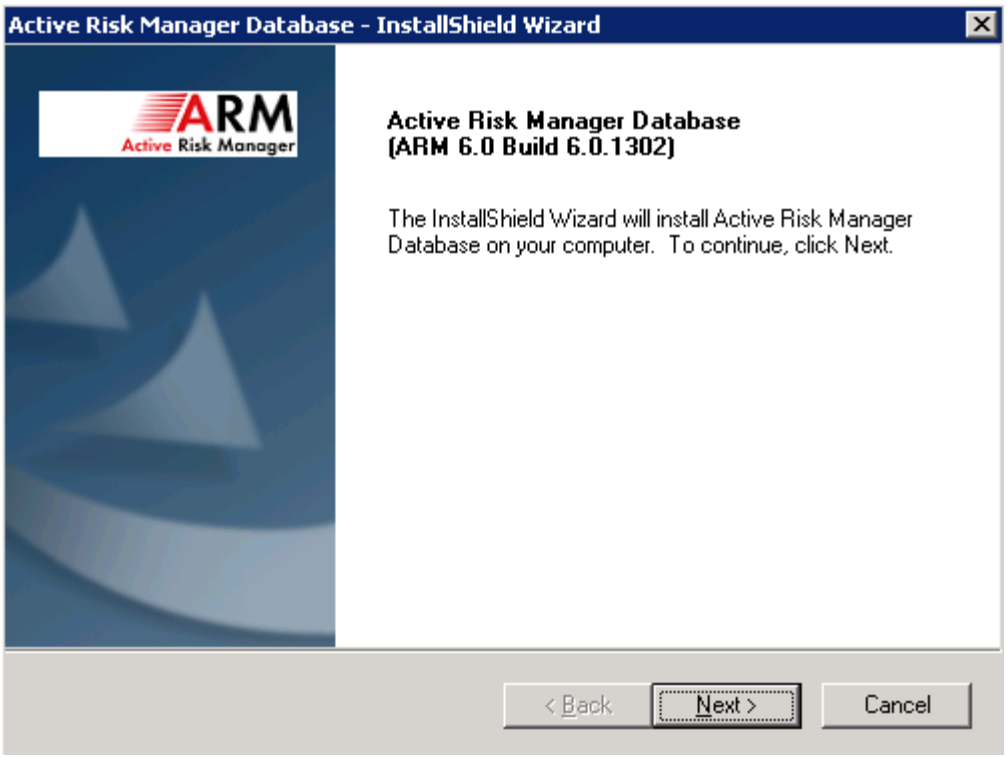
Please Note: The following steps assume that your database installation wizard is being executed from the ARM application server. Always take a full backup of your database or schema before upgrading.

1. Uninstall Active Risk Manager Database from Add/Remove Programs.

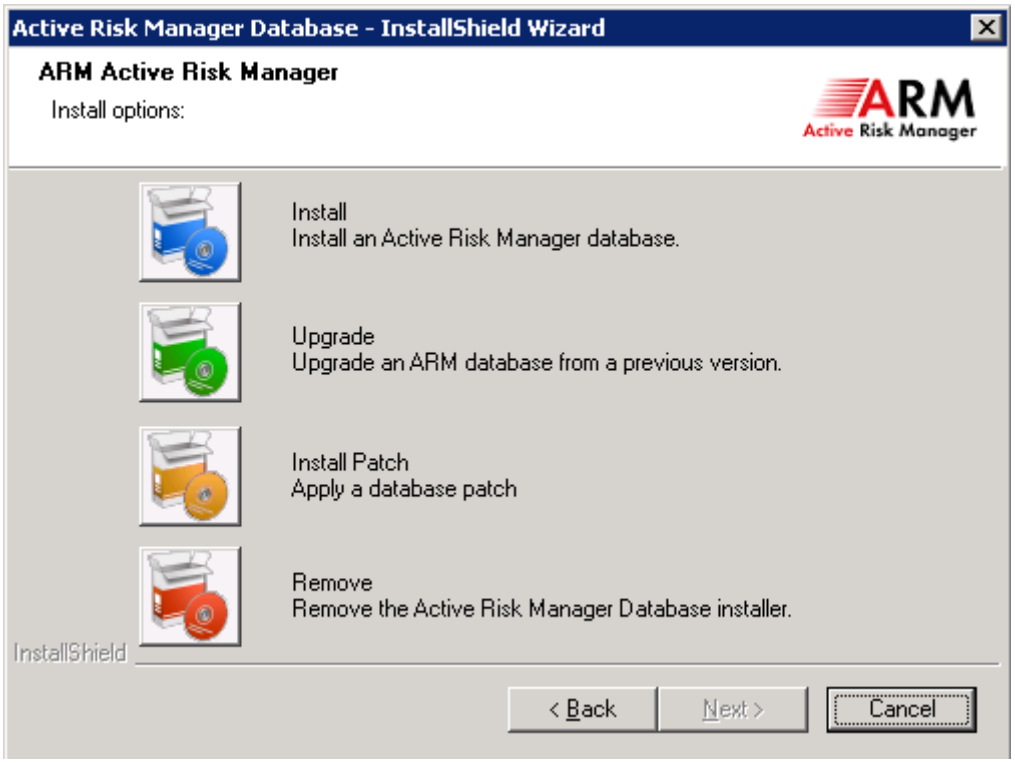
   Note that the database component in Add/Remove Programs is not the ARM database itself but the install wizard used for creating new/upgraded databases.



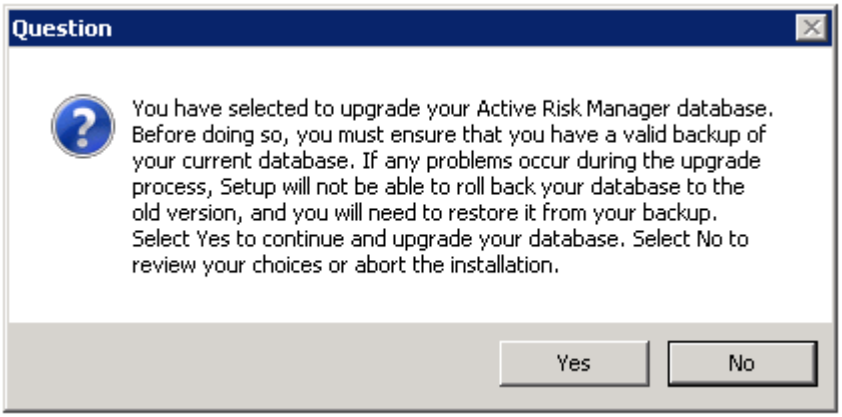
2. Run the Setup.exe from the database folder of the ARM 6 Installation media. Ensure you right click and select "Run as administrator" if applicable.



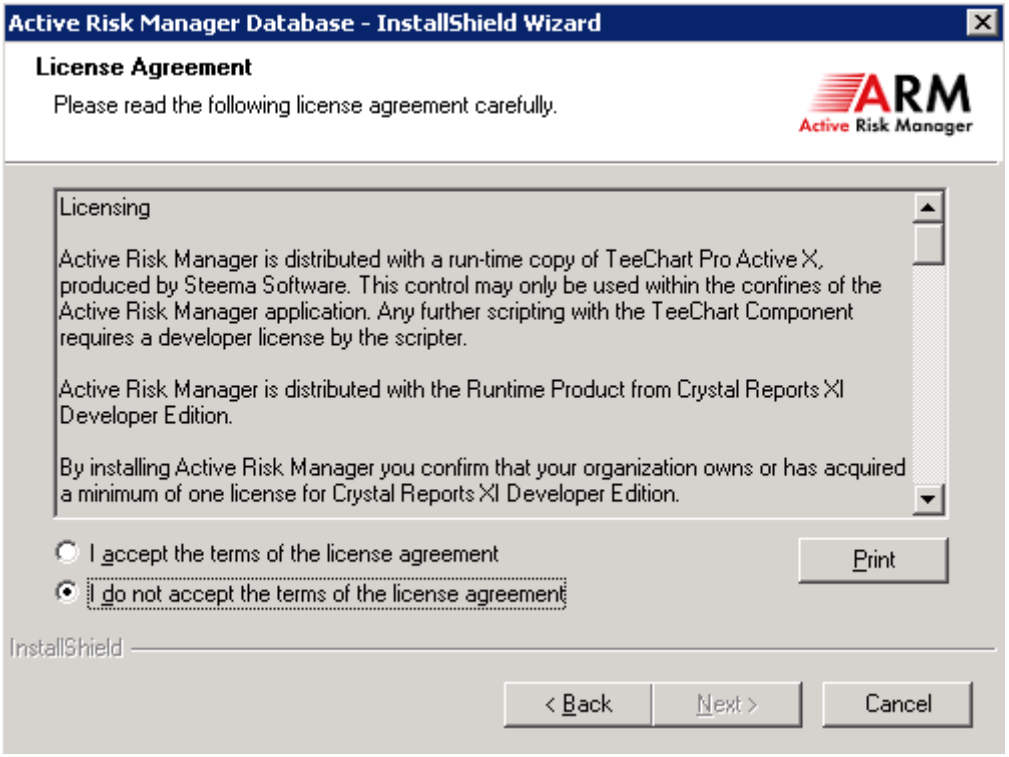
3. Choose the Upgrade option.



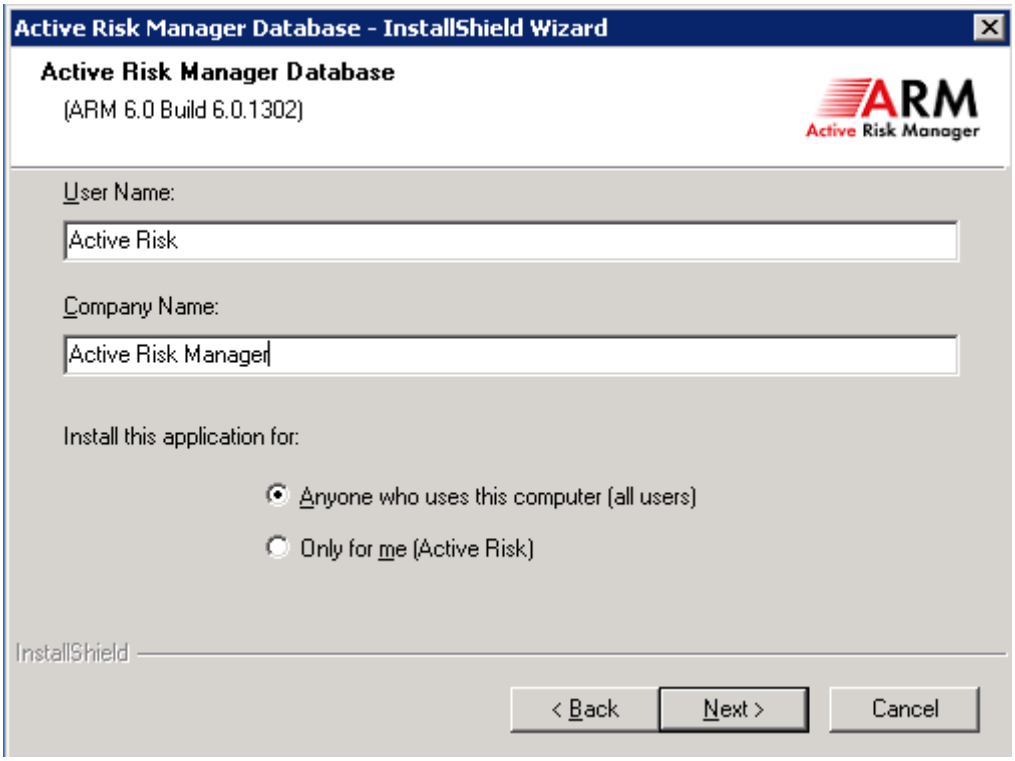
4. Confirm that you've taken all the relevant backups before beginning the upgrade.



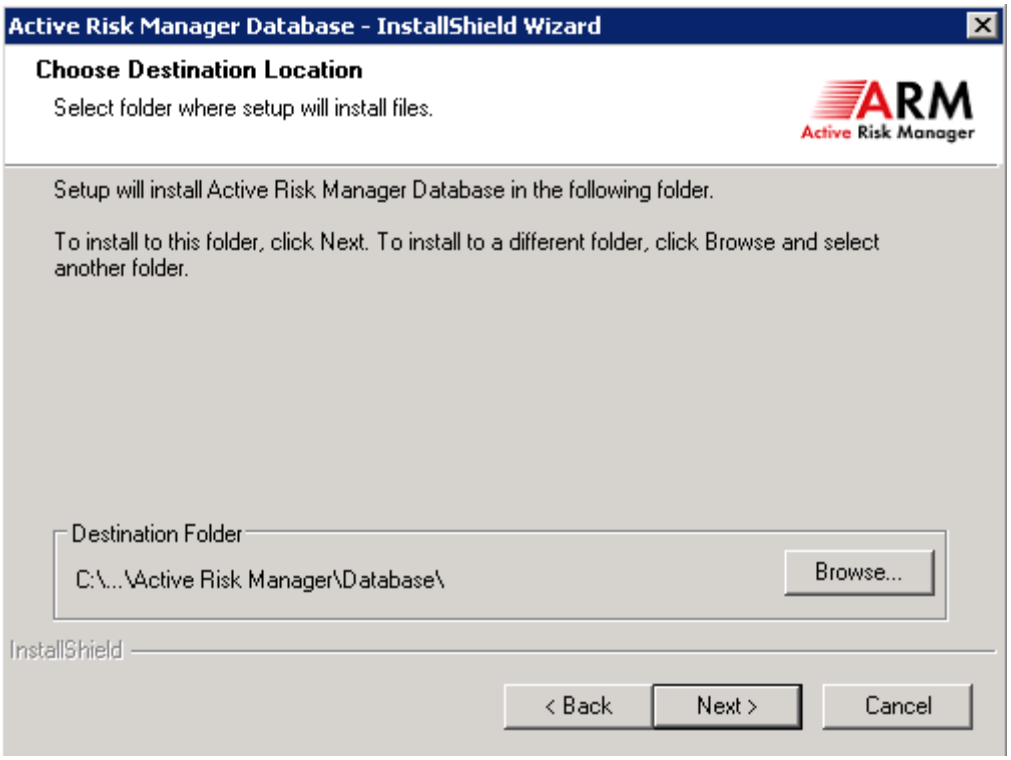
5. Read and accept the licence agreement.



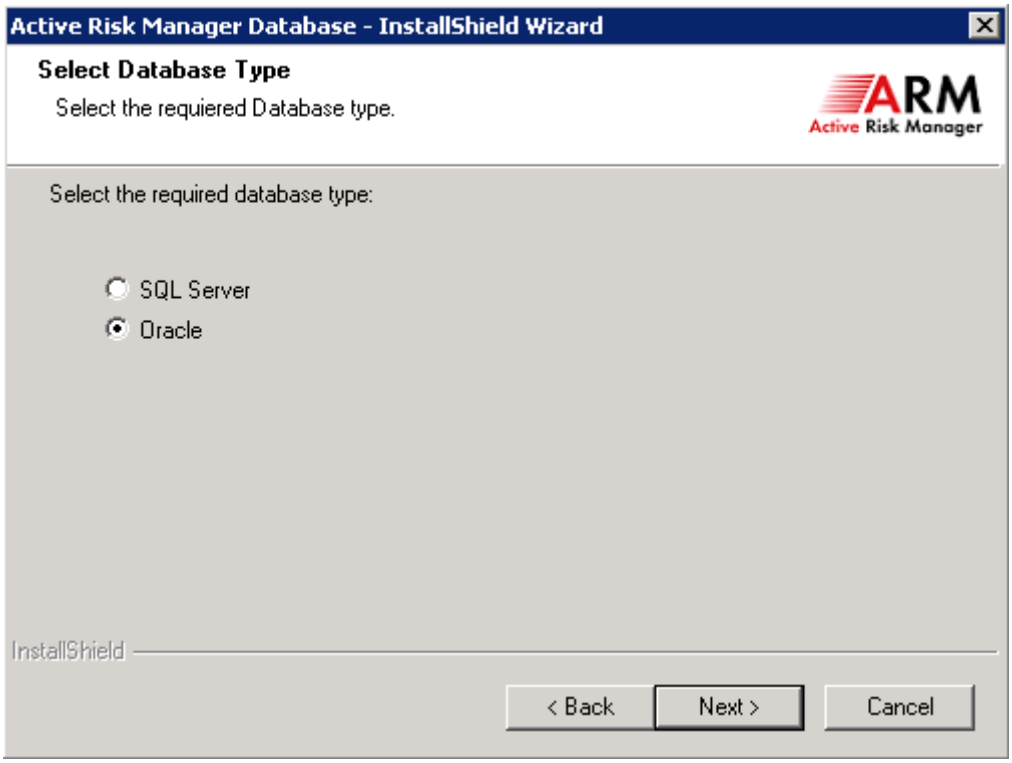
6. Type your User Name and Company Name in to the correct fields. Select who you want the database creation application to be available to.



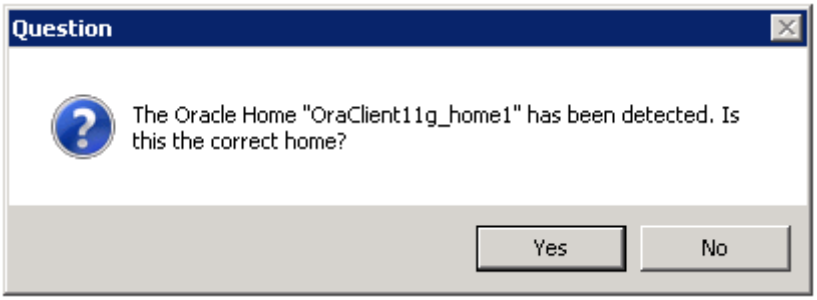
7. Set the location for the SQL scripts for upgrading and creating new databases.



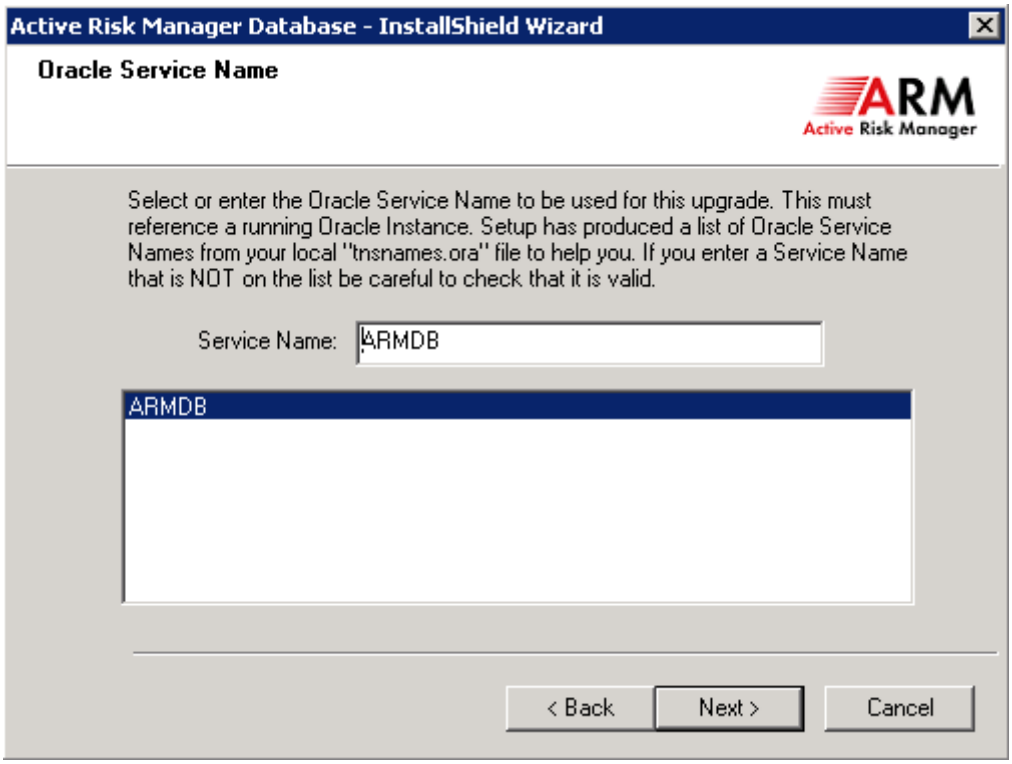
For SQL Server databases select SQL Server and go to step 11
For Oracle database select Oracle option and follow the steps below



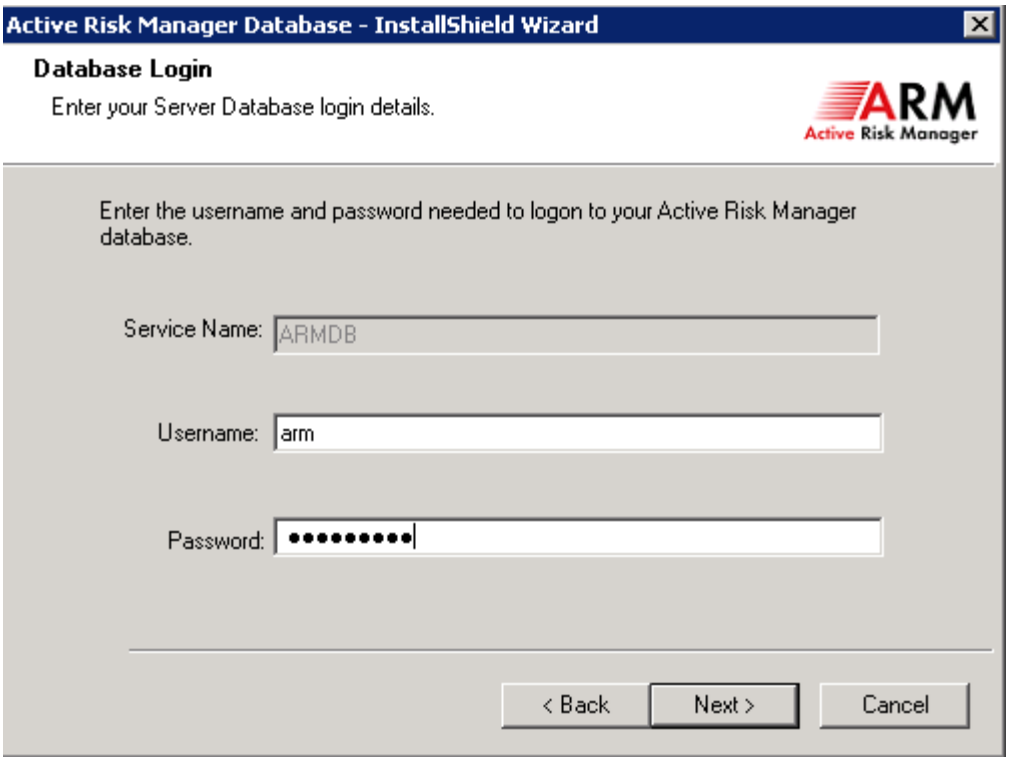
8. A pop up will appear asking you to confirm which Oracle Home to use. If the first one listed is not the one that you wish to use then choose No and then next in the list will be displayed.



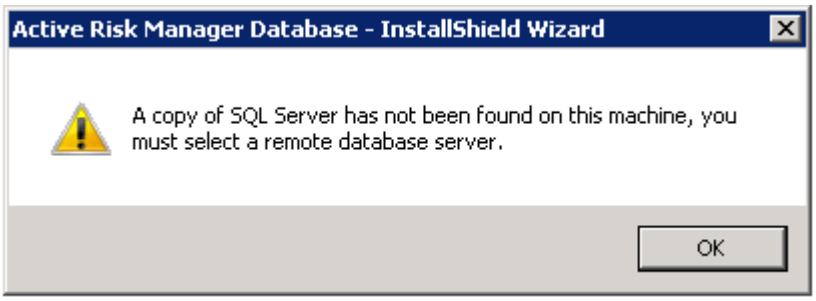
9. The list of Oracle Service Names configured in TNSNAMES.ORA for the home selected will be displayed. Highlight the identifier that references the database to be used for the ARM schema.



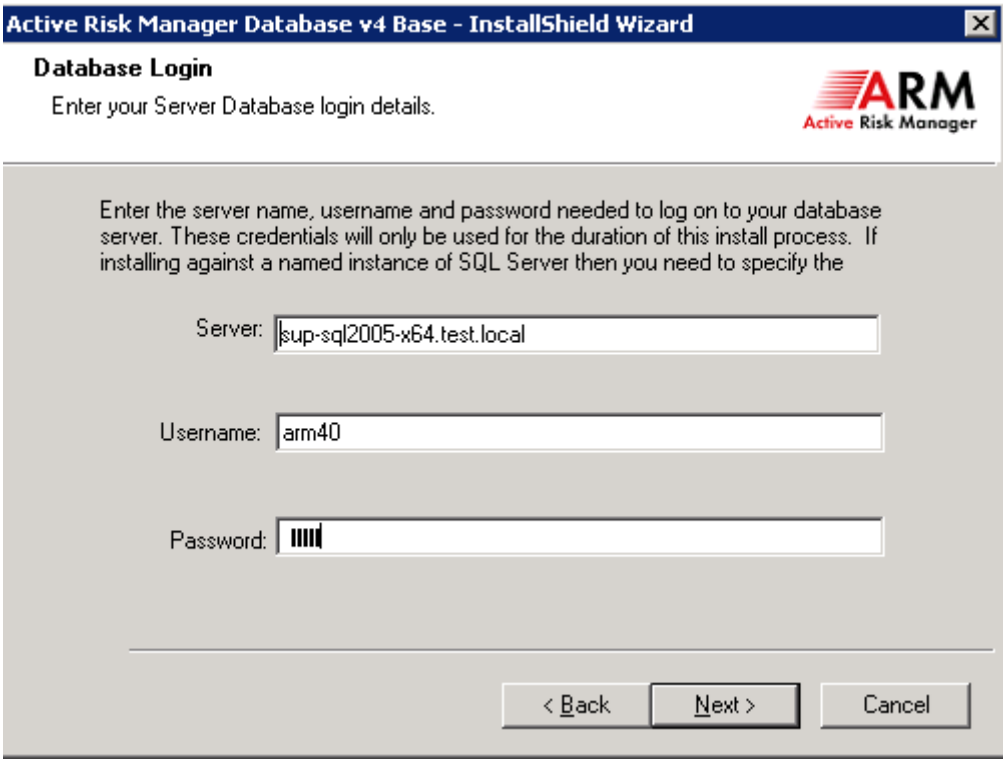
10. Enter the username and password for the schema that you want to upgrade. (Ensure that the username is entered in UPPERCASE)



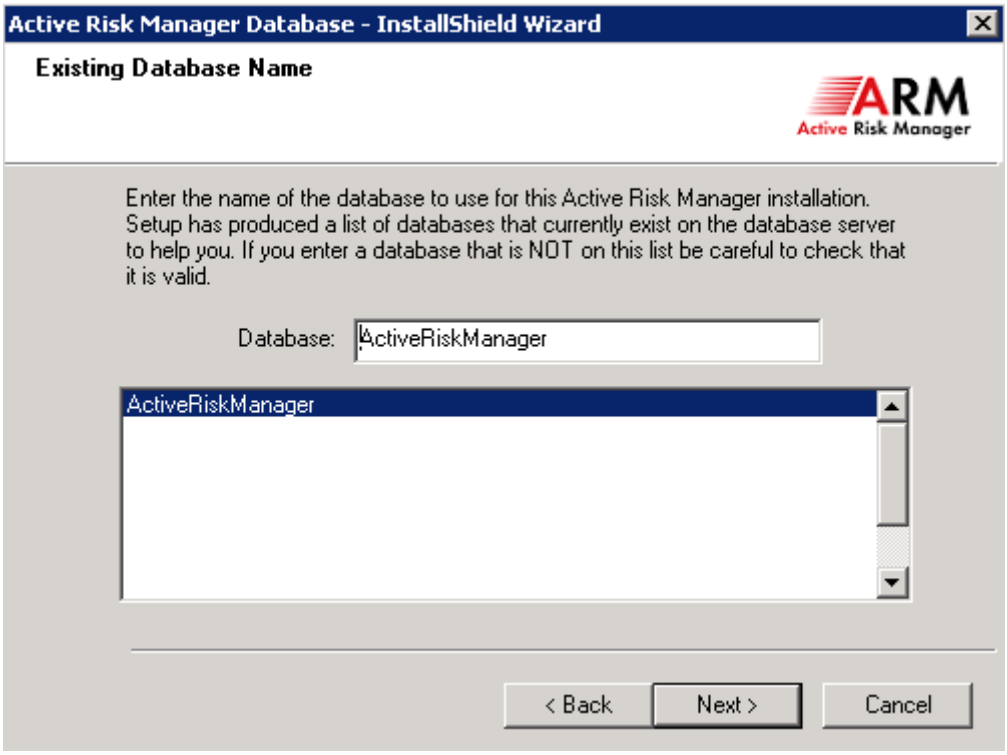
11. You may receive a warning as below, click OK to continue further.



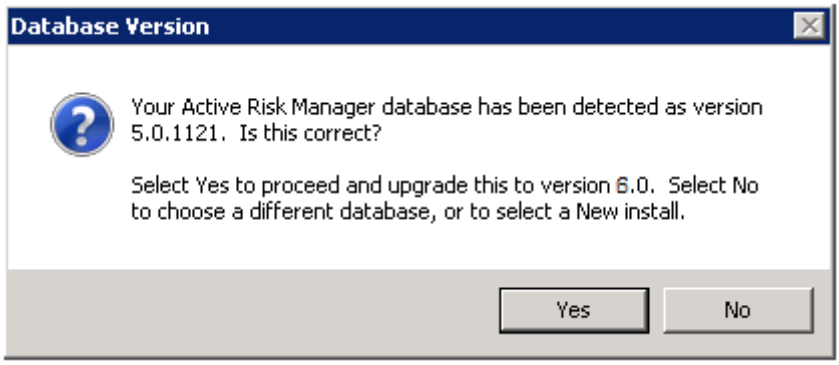
12. For SQL Server database upgrades enter the hostname or IP address of the database server and user login details. This user must be either a Database Owner for the ARM Database or should have **sysadmin** role at instance level.



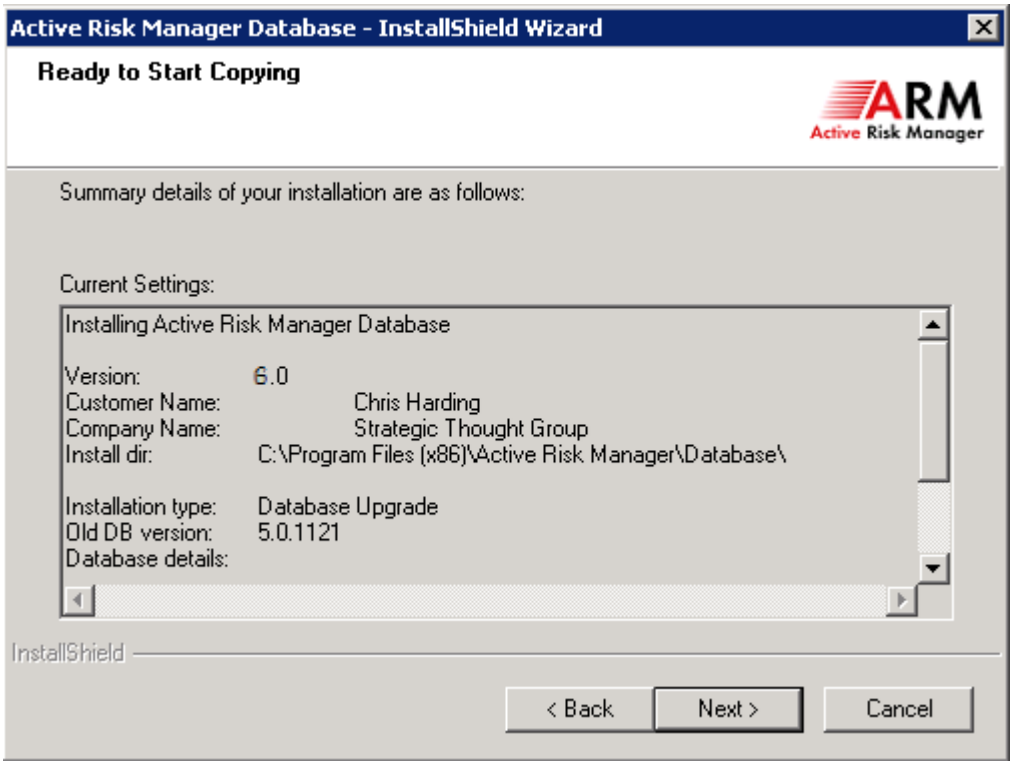
13. Select the database to upgrade from the list.



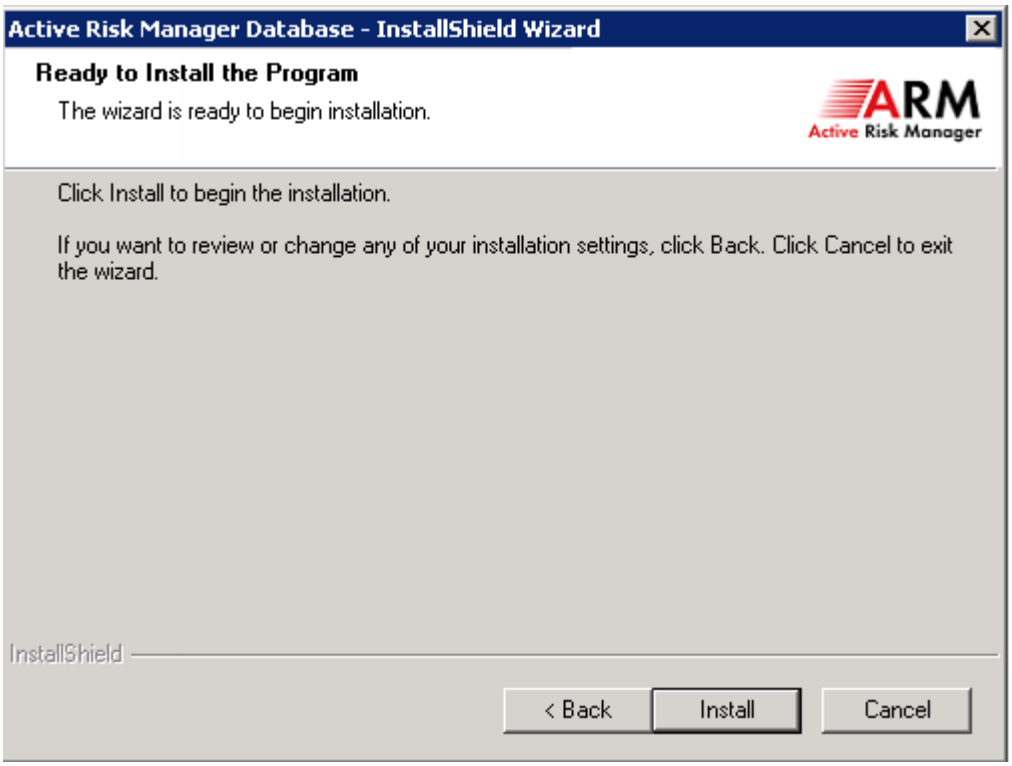
14. Confirm that you are happy to proceed with the upgrade of the chosen database; it is not possible to reverse these changes without restoring your backup. The version numbers mentioned here may be different than your chosen database.



15. Press Next to confirm the options.



16. Press Install to begin the upgrade



17. For Oracle databases, we recommend that you review and implement the suggestions mentioned at the end of this document. Under Section 13 as **Oracle Database Performance Recommendations** after you have finished upgrading your Oracle ARM database.

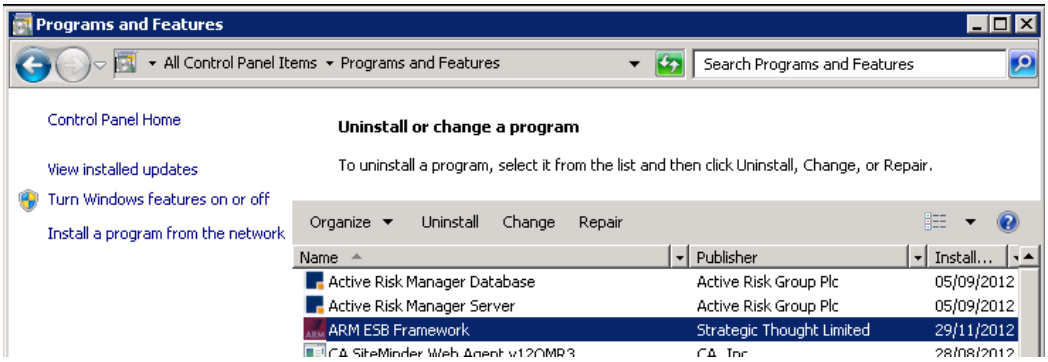
4.2 Application Server Upgrade

There can be various scenarios for an ARM upgrade and it depends on actual installation as which components were originally installed; the following section covers most of the generally installed components that could be considered:

1. From ARM 6 onwards it is now possible to upgrade the ARM Application Server component rather than uninstall/reinstall. However, if you wish to uninstall ARM and then perform a full installation then ensure you remove all of the separate ARM components first before the ARM Application Server.
2. Crystal Reports is ***NOT*** supported in ARM 6. During the upgrade process the Custom Crystal Reports folder will be removed. We therefore recommend that you backup any custom Crystal Reports you have created to prevent them being lost. These are located here:
   `\Program Files\Active Risk Manager\Server\Web\Reports\Custom\`
3. Please backup any Custom SSRS ARM Reports from your SSRS server under the “Custom” folder. If you click on edit for each of the reports you can save the .rdl file locally to your drive. Make sure you perform this task for each instance configured on the SSRS server for ARM.
4. Export/Back up the ARM registry keys containing all your database connection settings from the following location.

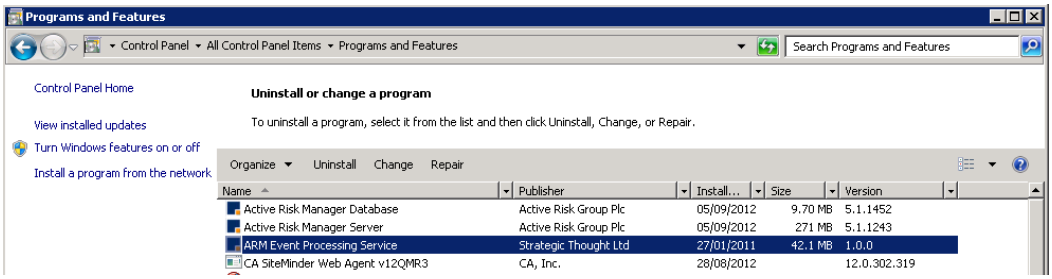
`HKEY_LOCAL_MACHINE\SOFTWARE\Strategic Thought Ltd\Active Risk Manager Server`

5. Backup a copy of the web.config file located at:
   `\Program Files\Active Risk Manager\Server\Web\web.config`
6. ARM ESB Framework Uninstallation [If Installed]
   - Please note that ESB is decommissioned in ARM 6 and therefore this is just an uninstall operation. You are not required to install it again.
   - On the ARM Application Server, go to Control Panel > Program and Features > Uninstall Program
   - Locate ARM ESB Framework application

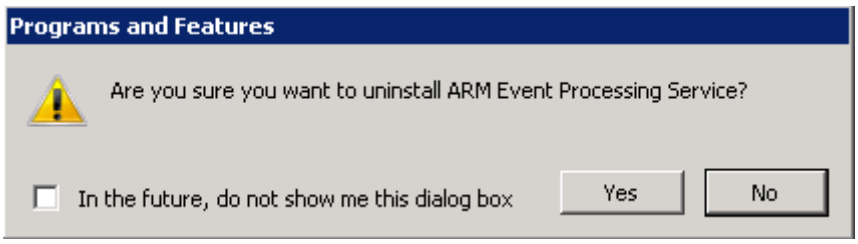


   - Click Uninstall located on the control panel window.
   - The ESB Framework will be uninstalled from Application Server.

7. ARM Event Processing Services [If Installed]
   - On the ARM Application Server, go to Control Panel > Program and Features > Uninstall Program
   - Locate ARM Event Processing Services

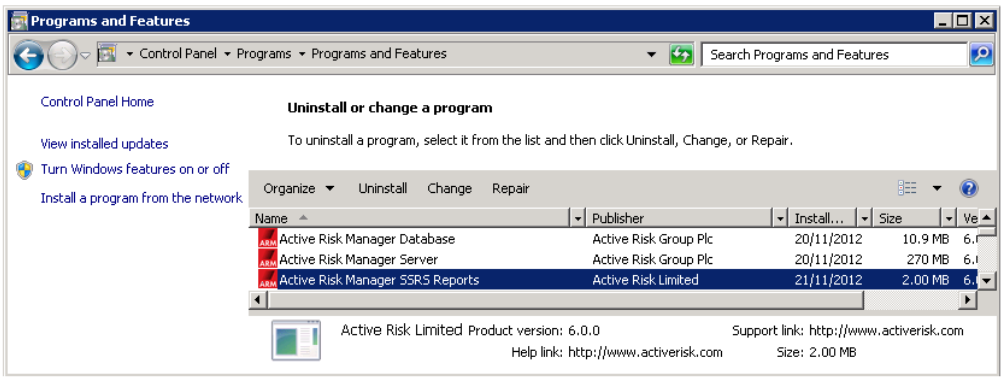


   - Click Uninstall
   - Click Yes on the next dialog box as shown below.



   - The ARM Event Processing Services will be uninstalled from the Application Server.

8. Uninstall the Active Risk Manager SSRS Reports program [Report Assembly], from Add/Remove Programs. Please note that this is located on SSRS Server.



9. Please make sure Database has been upgraded successfully as per section 4.1 and next step is to upgrade ARM Application Server.
10. ARM Application Server upgrade is performed using the same installer as we use for new installation. Please follow the instructions provided in section 3.2 before continuing further.
11. Reinstall the ARM Event Processing Services.
    - Follow the instructions provided in section 9.
12. Reinstall the ARM Reports Assembly
    - Follow the instructions provided in section 7.5.1
13. Redeploy the Standard Reports on Report Server
    - Follow the instructions provided in section 7.6 and 7.7
14. Upgrade any SharePoint installations of the ARM App Framework to version 4.
    - Instructions are included in the ARM App Framework documentation.
    - Please Note that installer expects previous version of installer to be in original location from where it was installed originally.

5 Multi Currency and Multi Language Support

Multi Currency

ARM 6 introduces support for multiple currency data in a single instance. If the business requirement is to use a different currency per Business Area in ARM then there are several implementation options that may be considered, therefore we would recommend that you contact Active Risk support to discuss the best fit implementation option for your organisation.

Impact categories may now be selected as Cost categories allowing a defined currency to be attributed to them (rather than a symbol simply used for units). The ARM 6 upgrade script will select the system “Cost” impact category as “Is Cost” as part of the upgrade script. Any Additional cost impact categories that may be defined in your system will require the “Is Cost” check box to be ticked by the ARM Administrator.

This setting can be found in Tools-> Admin->Configuration->Scoring->Categories.

Multi Language

ARM 6 introduces support for multiple languages. The ARM interface can be viewed in a different language which can be configured on a user by user basis. Activating Multi language support requires a change in configuration files, please contact ARM support for assistance.

6 Non ActiveX Charts

All ARM charts now default to NON Active X except for the Risk Exposure Reduction Chart which requires Active X. The Risk Exposure Reduction Chart is scheduled for migration to NON Active X in a future service pack.

7 Reporting

7.1 Introduction

MS Reporting Services is the default reporting solution for ARM 6 Release. This is a comprehensive, server-based solution that enables the creation, management and delivery of both traditional paper-oriented reports and interactive Web-based reports.

Reports are published to a Reports Server running Microsoft SQL Server Reporting Services and data retrieval and report processing occur on the reporting server.

Please refer to the Reporting Services guide for further details on the ARM Reporting Services module.

7.2 Microsoft Reporting Services

Active Risk Manager supports the use of purpose specific custom reports that are not part of standard report pack. Custom reports are usually created in SQL Server Business Intelligence Development Studio and can then be published through Reporting Services.

Please Note: Customer developed reports are not covered under your support agreement. There is currently no documentation available to assist in the development of custom reports for use with ARM, however training can be provided if required. Please contact your account manager for further details.

Microsoft SQL Server 2008 R2 SP1 Reporting Services is a component of SQL Server and is available on the SQL Server release media. ARM 6 reporting requires SQL Server 2008 R2 SP1 Reporting Services.

Please note that MSDE, MS SQL Express and MS SQL Server Evaluation Edition are not supported database platforms. SQL Server 2000 Reporting Services is not supported.

Reporting Services may be installed on one of the following servers:

- ARM Application Server
- Dedicated MS Reporting services Server
- ARM Database server

For large scale deployments, it is also possible to implement load balanced Reporting servers.

Reporting Services is configured with connection details to the ARM datasource, ARM databases, and also an internal SQL Server database for Reporting Services. The ARM databases and internal report server database may be implemented on separate database servers.

The internal report server SQL Server database also applies to Oracle ARM databases and requires access to SQL Server Database Services. SQL Server database services may be deployed locally on the Reporting Services server or a database added on an existing shared database server.

Deployment of ARM Reporting is via a Reports Deployment Package which is run from the ARM Application Server and collects report server setup details (e.g. service name, db name, etc.) to configure report data sources, configure ARM instances and reports folder structure and install the ARM reports (RDL files) via the reporting service webservice.

There is also a separate package which must be run on the server with Reporting Services installed. This installs a custom component (ARM custom assembly (dll's) which handles authentication, security, etc. and expose a number of methods to support generating reports at run time).

7.2.1 Reporting Services Licensing

SQL Server Reporting Services and Database Services are both licensed products. If Reporting Services is installed on a dedicated server or on the ARM Application server then a SQL Server license is required for the reporting server. This would be in addition to a SQL Server Database Services licence for the database server used for ARM and the internal MS Reporting Services database. A

single SQL Server licence is required for a server hosting both Reporting Services and Database Services on the same server.

7.2.2 Hardware and Software

ARM 6 supports MS SQL Server Reporting Services (SSRS) 2008 R2 SP1 for use with the standard ARM reports.

.NET Framework 3.5 SP1 is recommended.

For full details on the requirements defined by Microsoft for the SSRS application please refer to

SQL Server 2008 R2 Books Online
http://msdn.microsoft.com/en-us/library/ms143506.aspx

7.2.3 Oracle Data Sources

If your ARM database exists within an Oracle database the Oracle client must be installed on the report server. We recommend the same Oracle version as you use on the ARM server.

The Oracle client directory must be located in the system path and both the Report Server Windows service and Report Server Web service must have permissions to access the files in this directory. A reboot of the server is recommended once the components are installed.

TNS connection to the database containing the ARM database must be configured and confirmed to be working through Enterprise Manager or SQLPLUS.

7.2.4 Report Server Firewall Rules (Inbound)

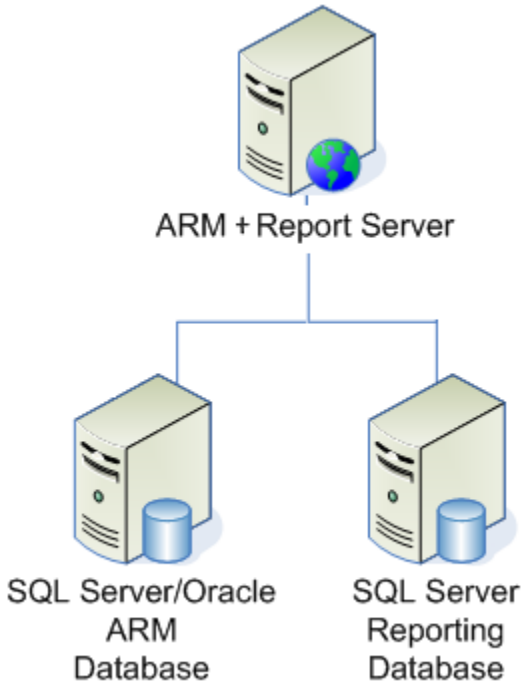
1433 – SQL Traffic (local Report Server database). Report Server database must be listening on standard port 143 for report deployment.

80 – HTTP Traffic

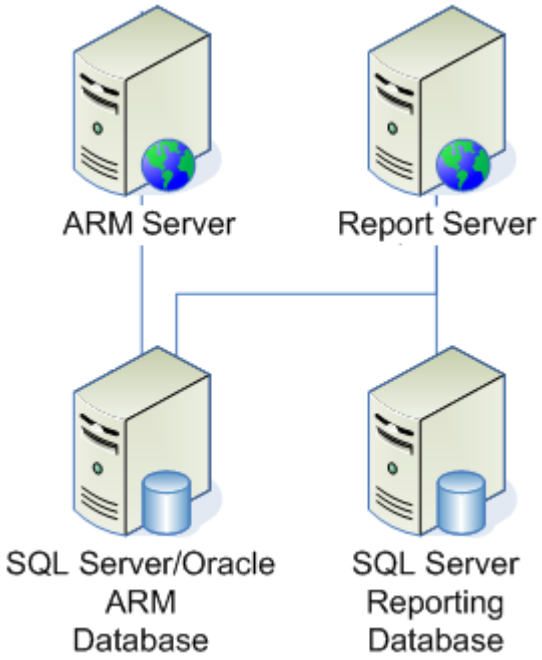
443 – HTTPS Traffic

7.3 Supported Generic Reporting Services Configurations

7.3.1 ARM Application and local Report Server



7.3.2 ARM Application and remote Report Server



7.4 SSRS 2008 R2 SP1 Setup and Configuration

7.4.1 Installation Overview

SSRS 2008 R2 features a redesigned server architecture that removes the dependency on Internet Information Services (IIS). To replace the functionality previously provided by IIS, Reporting Services now includes native support for HTTP.SYS and ASP.NET, URL management for site and virtual directory names. By default only windows integrated authentication is supported in SSRS 2008 R2 SP1, please contact STG Support for solutions on other authentication models.

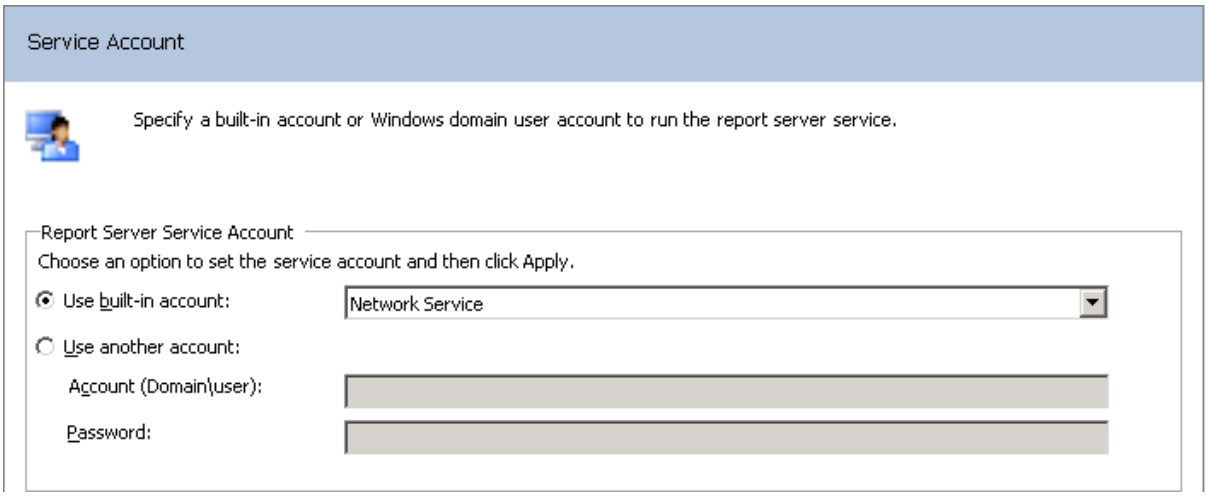
Install the Reporting Services option from your SQL Server 2008 R2 installation media selecting NEWORK SERVICE as the service account and apply SP1 before continuing to the Post Installation Configuration.

If you do not already have a remote or local SQL Server database engine to use with this installation then you should install the Database Engine as well. Full details on the installation process can be found at http://msdn.microsoft.com/en-us/library/ms143219.aspx

7.4.2 Post Installation Configuration

a) Open the Reporting Service Configuration Manager from Start – Programs – SQL Server 2008 R2 – Configuration Tools.

b) **Service Account.** We recommended that you use the NETWORK SERVICE built in local machine account to keep the installation simple and easy to manage. If you wish to use a domain service account please refer to http://msdn.microsoft.com/en-us/library/ms189964.aspx for further details on the considerations required.

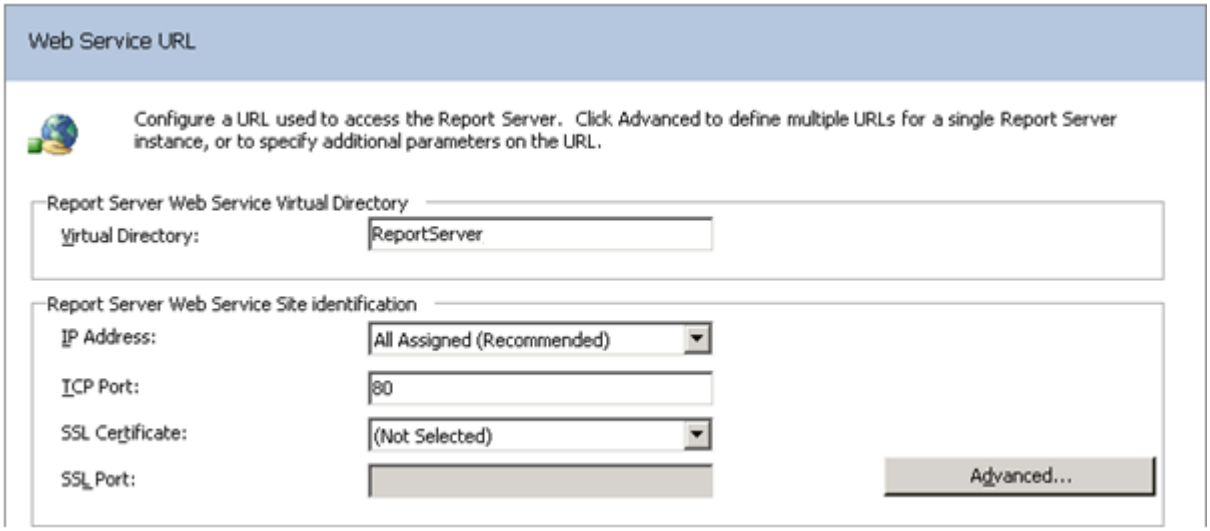


c) **Web Service URL.** Define a virtual directory name and IP/Port bindings for accessing the reporting web services.

Certificates must be imported into the local store under the computer account using the MMC snap-in, http://technet.microsoft.com/en-us/library/dd632619.aspx before they will be displayed in the drop down list.

Please also note the “Interoperability Issues with IIS” section of http://msdn.microsoft.com/en-us/library/ms345223.aspx if you will be using SSRS 2008 and SSL certificates on a server with IIS install.

For named instances of SSRS recommended virtual directory name format is ReportServer_INSTANCENAME

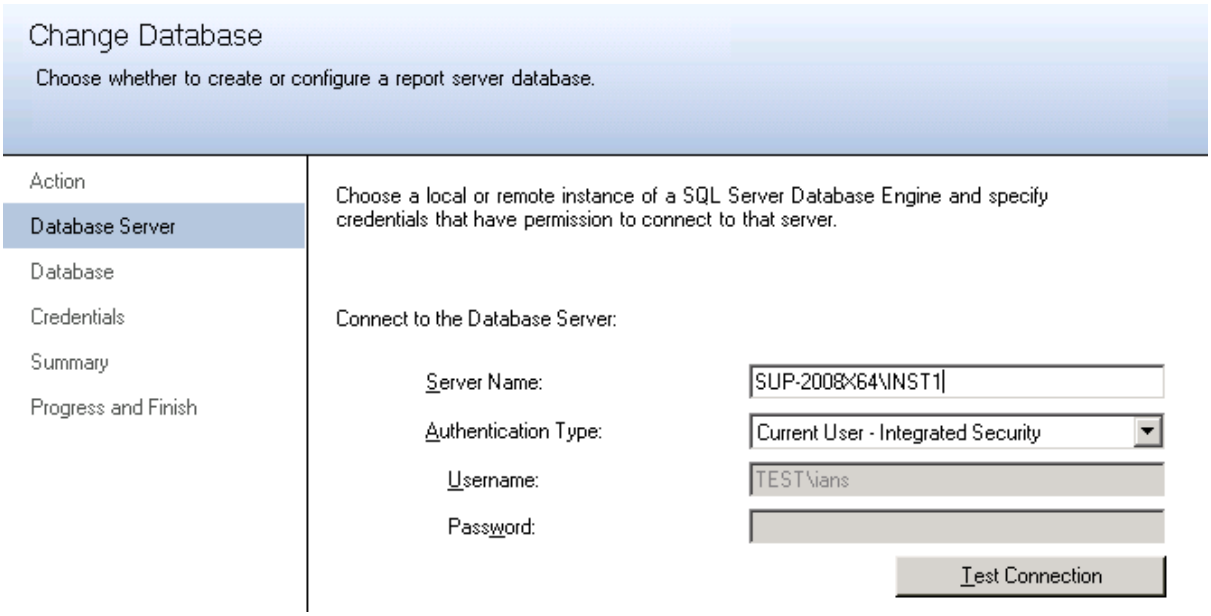


d) Create the Report Server Database.

For full details on the requirements for each of the steps below please see http://msdn.microsoft.com/en-us/library/ms157300.aspx

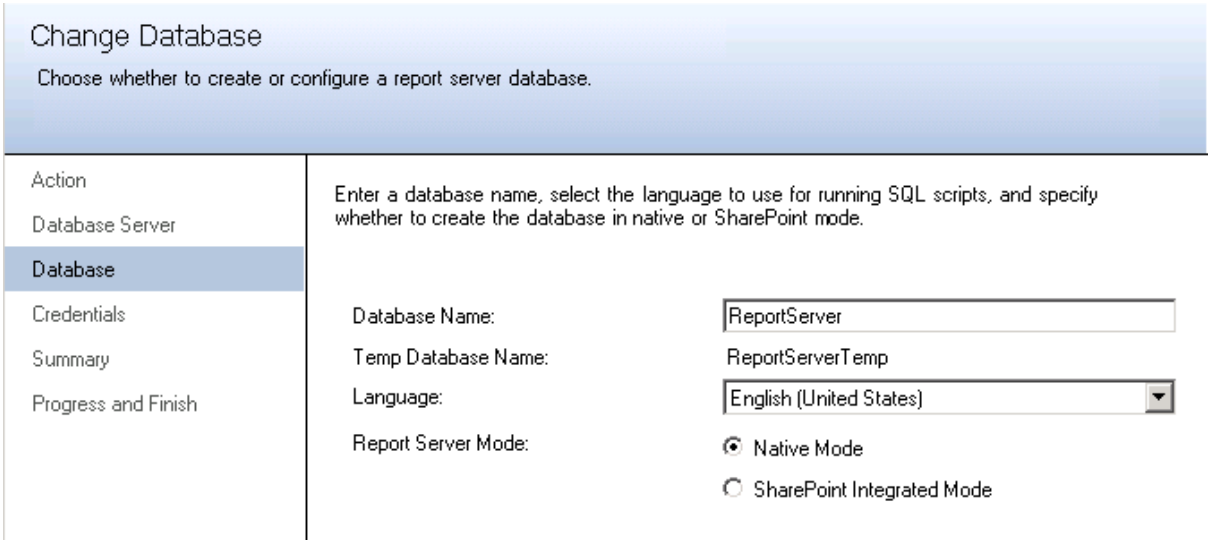
i. Define a SQL Server database for storing the SSRS configuration and uploaded reports. Use the 'Change Database' option and then choose to create a new report server database.

The authentication account used on this page is used for a one-time connection to create the report server database and RSExecRole. The account requires the dbcreator server role as a minimum in the SQL Server database instance.



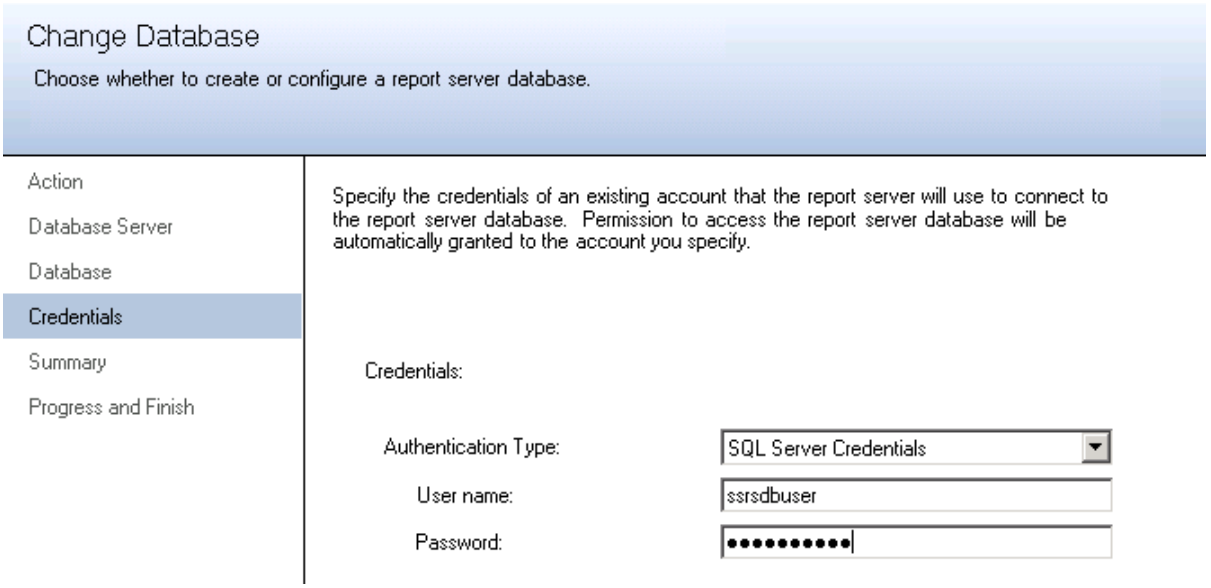
ii. Provide the Database Name and set the Report Server Mode to Native Mode. SharePoint Integrated Mode is not currently supported for use with the ARM standard reports.

For named instances of SSRS recommended database name format is ReportServer$INSTANCENAME

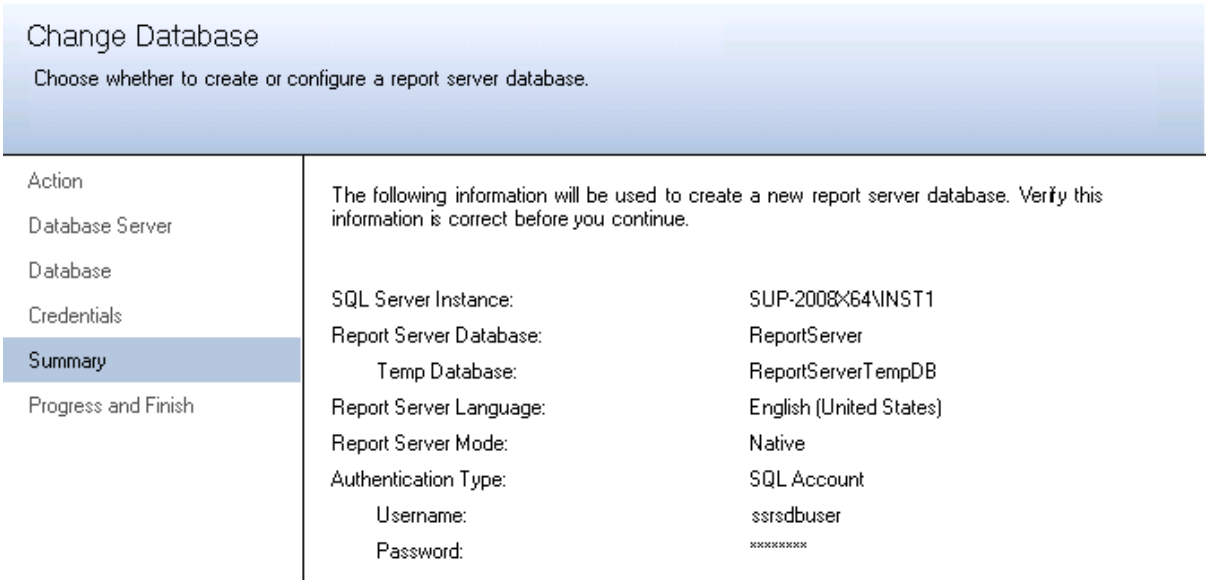


iii. Specify an existing account that will be used for the report server database connection. All the required permissions will be set through this installer.

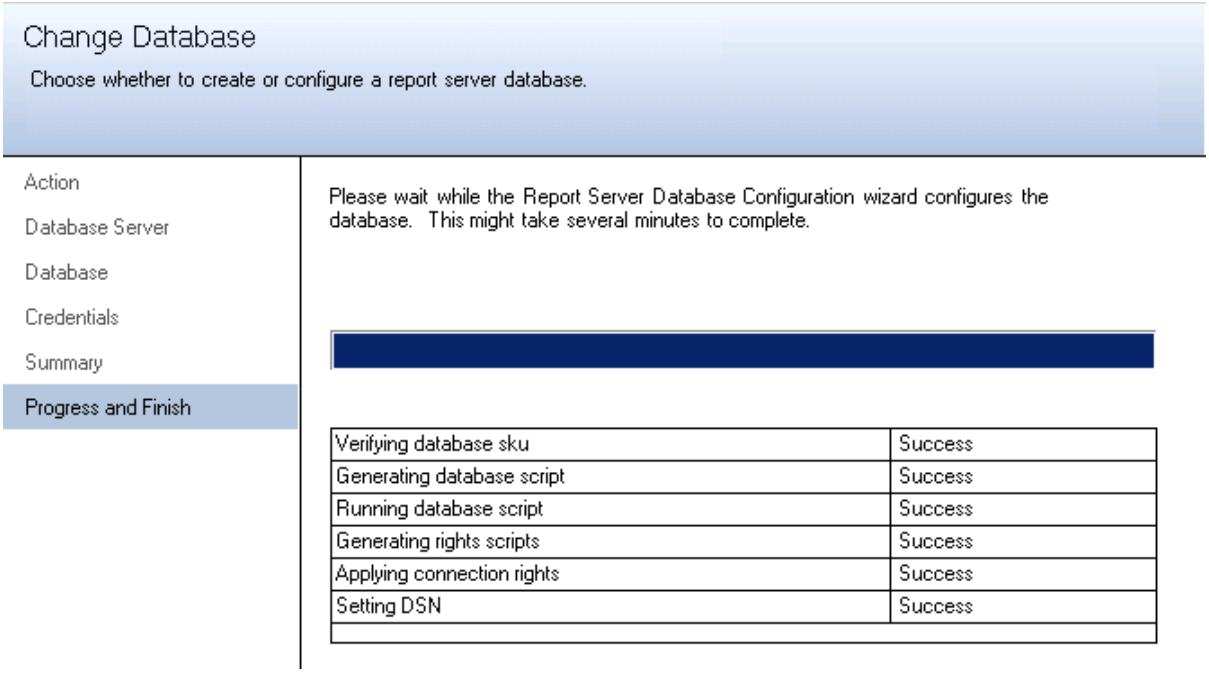
You will need to provide credentials to the Report Deployment Wizard later on so it is recommended that you use a domain or SQL Server database user account at this point. If you choose to use a local machine service account you will need an additional set to credentials later on.



iv. Confirm that the details entered are correct before proceeding.

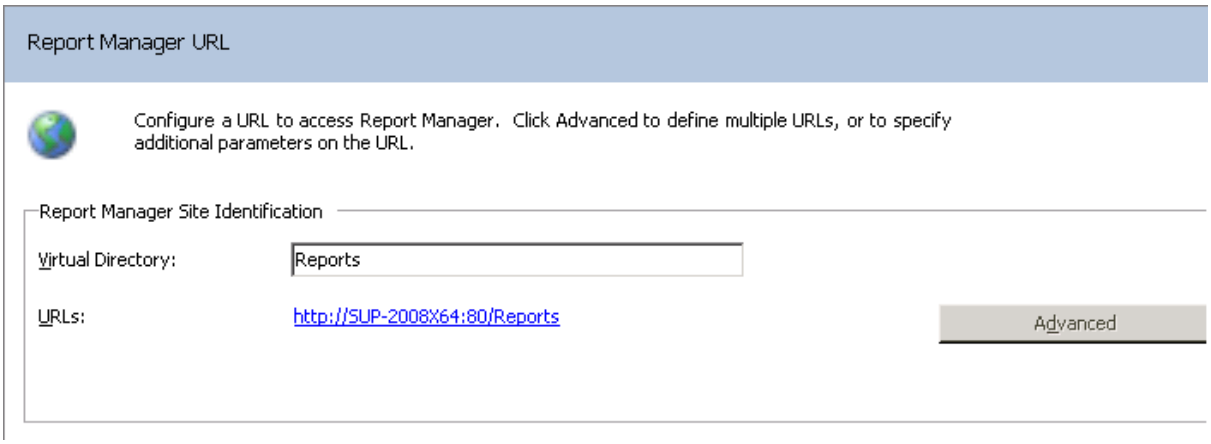


v. The database creation has been successful once you are presented with the screen below. If there are any errors please follow the instructions presented to you or contact STG Support for assistance.



e) **Report Manager URL**. Configure the URL for the Report Manager GUI interface. The virtual directory name defaults to Reports.

For named instances of SSRS recommended virtual directory name format is Reports_INSTANCENAME.



f) Test the URLs that you have defined above for Report Server Web Service and Report Manager e.g. http://localhost/reportserver and http://localhost/reports.

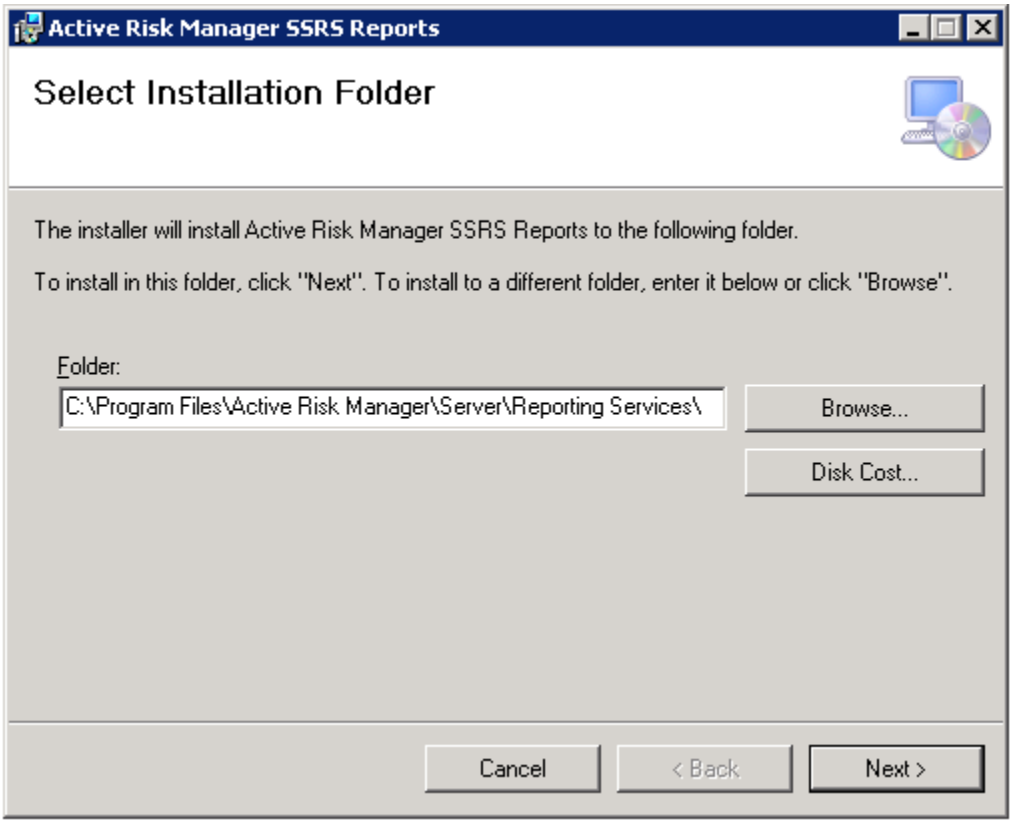
7.5 ARM Report Deployment

7.5.1 Report Assembly Installer.

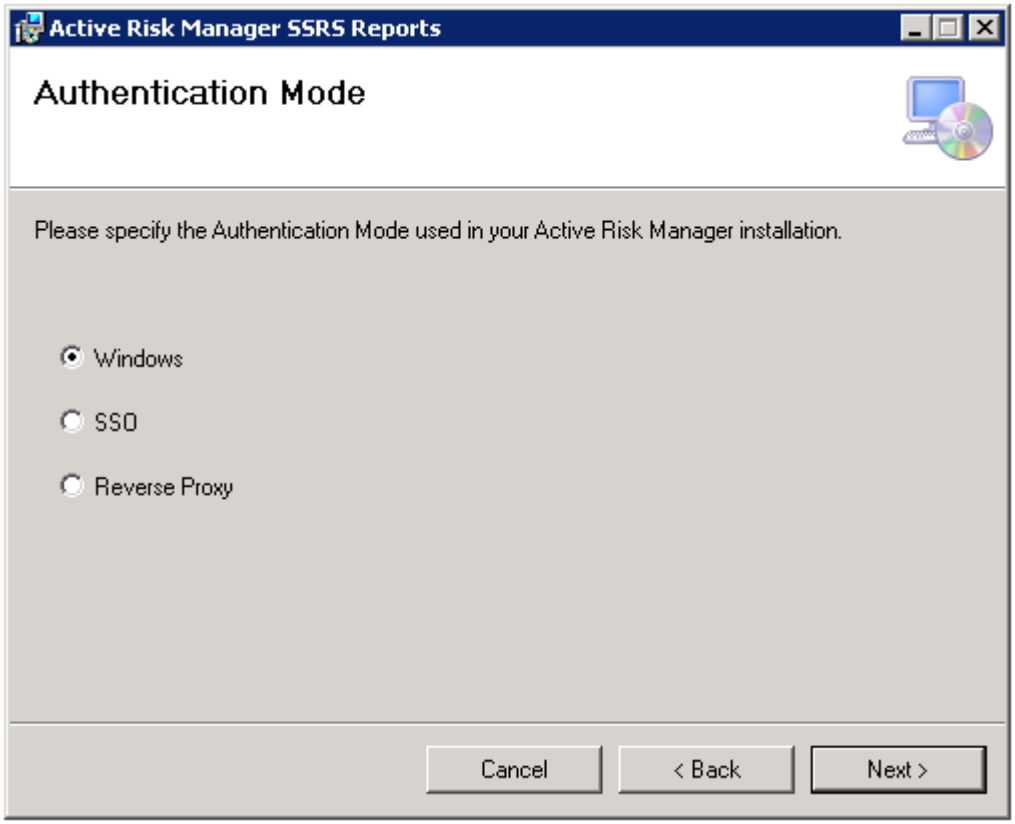
The ARM reports require various custom assembly files to be installed on the **report server** for use with the reports. The wizard will also add additional settings to the report server web.config file for database type and authentication variable.

a) Run the setup.exe from the Report Server directory on the ARM installation media and press Next to start. Ensure you right click and select "Run as administrator" if applicable.

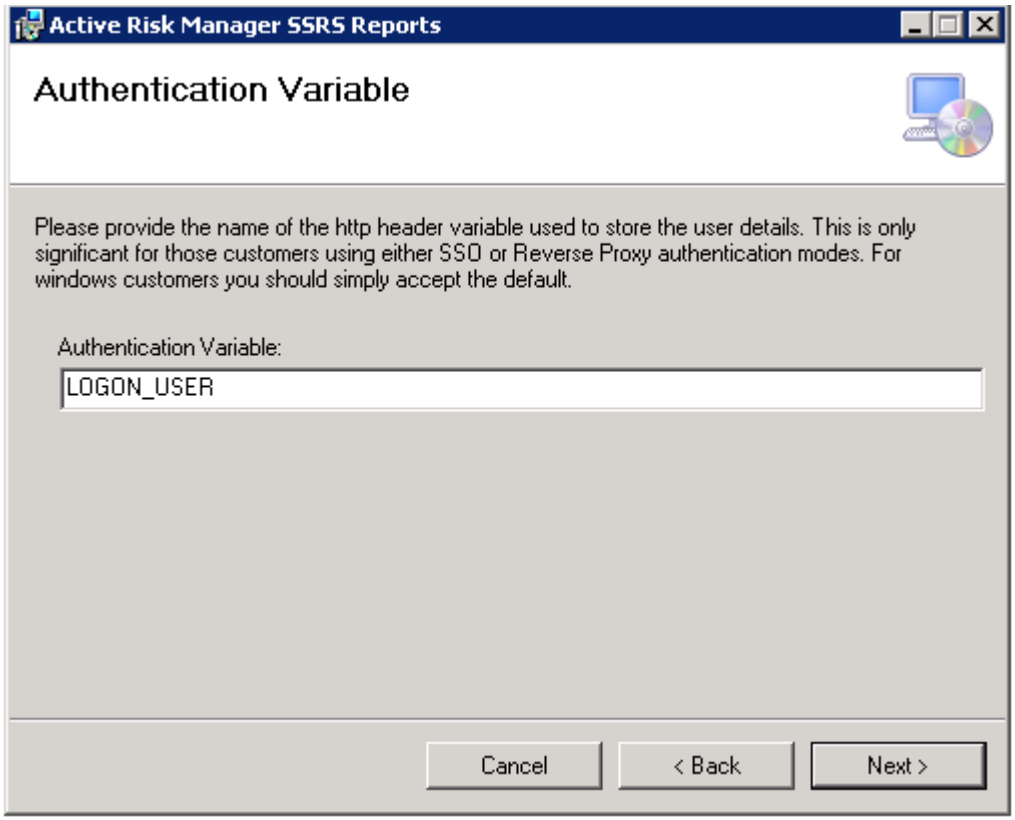
b) Choose the folder that the ARM report assemblies will be installed to. We recommend using the default path.



c) You may be asked to choose the type of ARM database that you will be reporting on. Also choose the authentication type. Unless you are using a reverse proxy or SSO leave as the default “Windows



d) Specify the authentication header. This should only be changed from the default LOGON_USER if using reverse proxy or SSO.



e) Press next and continue until completion.

7.6 ARM Standard Reports Deployment

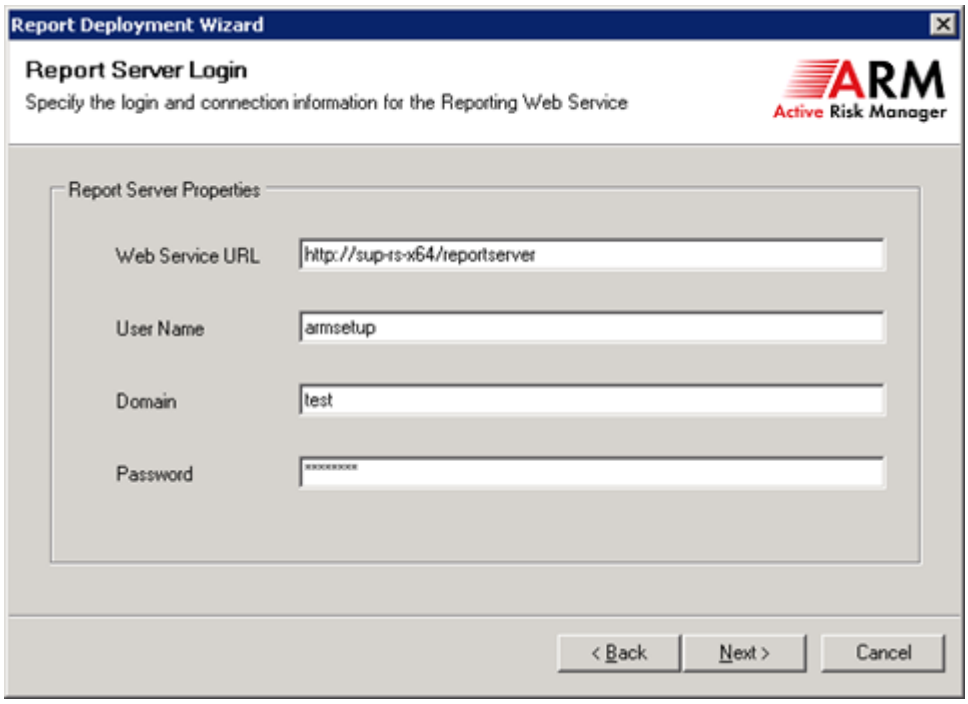
The RDL report definition files reside on the ARM application server. To deploy these reports to the SSRS application follow the steps below.

If upgrading the deployment wizard will remove any existing reports in that instance of SSRS before deploying the ARM 6 reports so there is no need to delete the existing standard reports before upgrading.

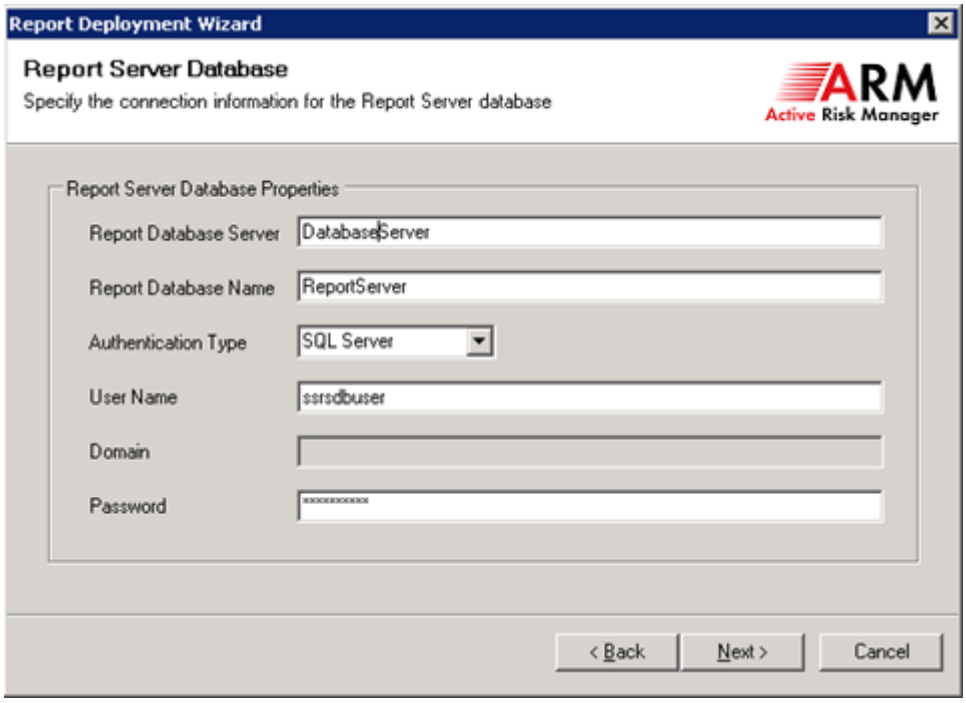
a) Navigate to Program Files\Active Risk Manager\Server\Reporting Services

b) Start the ReportDeploymentWizard.exe and press the Next button. Ensure you right click and select “Run as administrator” if applicable.

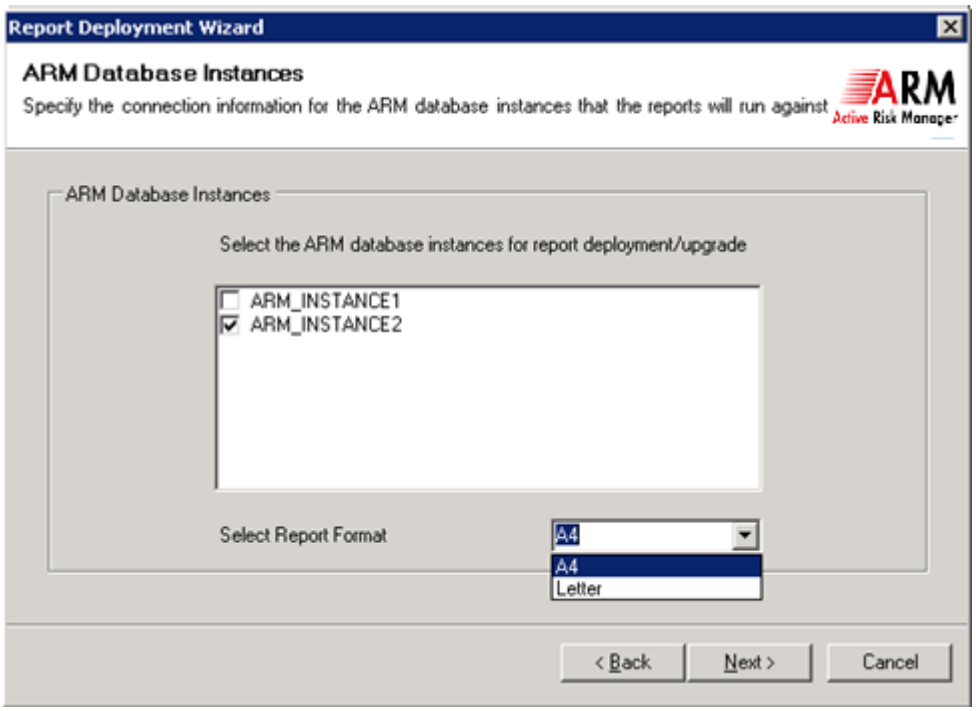
c) Enter Web Service URL for the ReportServer virtual directory configured in the previous section. The authentication account used on this page is used for a one-time connection to create the report server application to upload the reports. This account should have the content manager role within SSRS - local administrator group on the report server has this role by default.



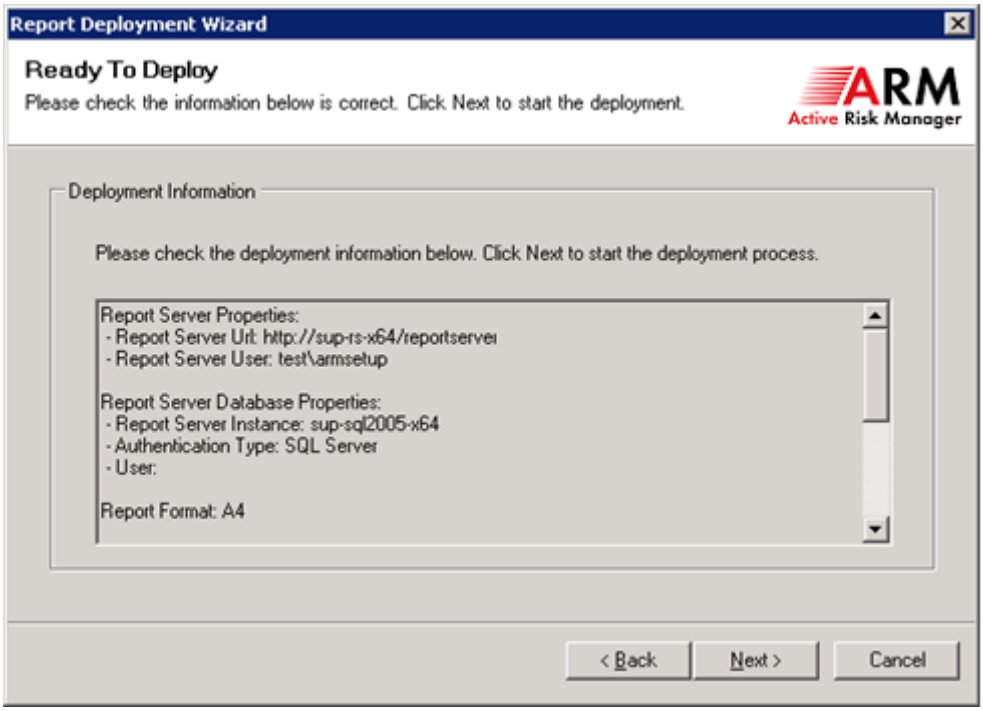
d) Enter the properties for the ReportServer database as defined in the previous section, not the ARM database. The account credentials used here will be stored in a data source in SSRS. Please note that this wizard only supports database connections on the standard SQL Server port 1433.

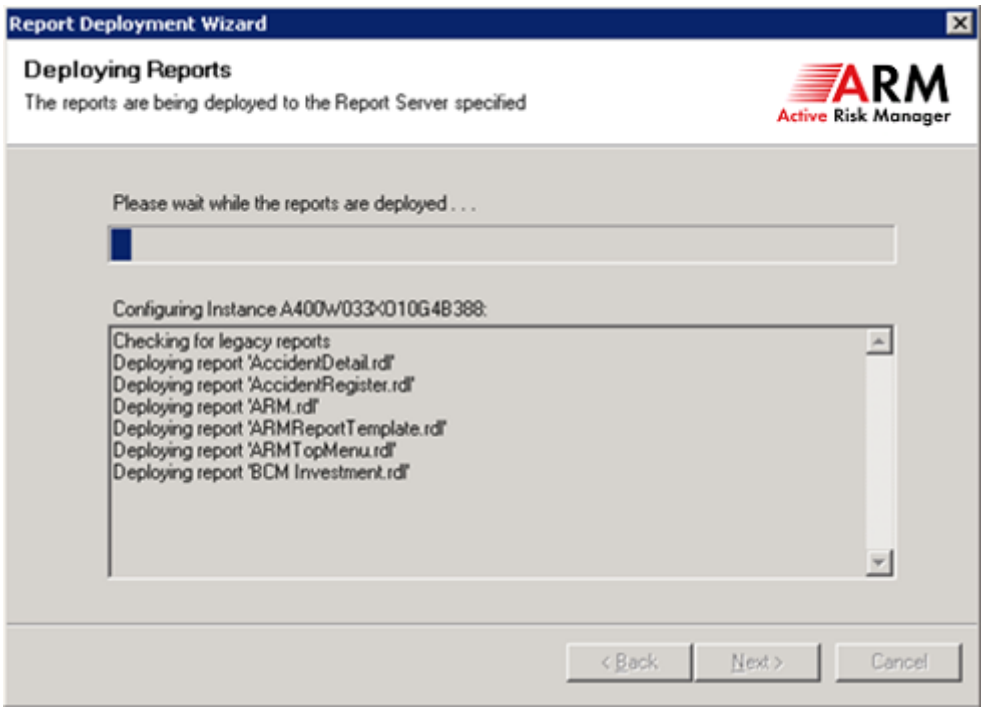


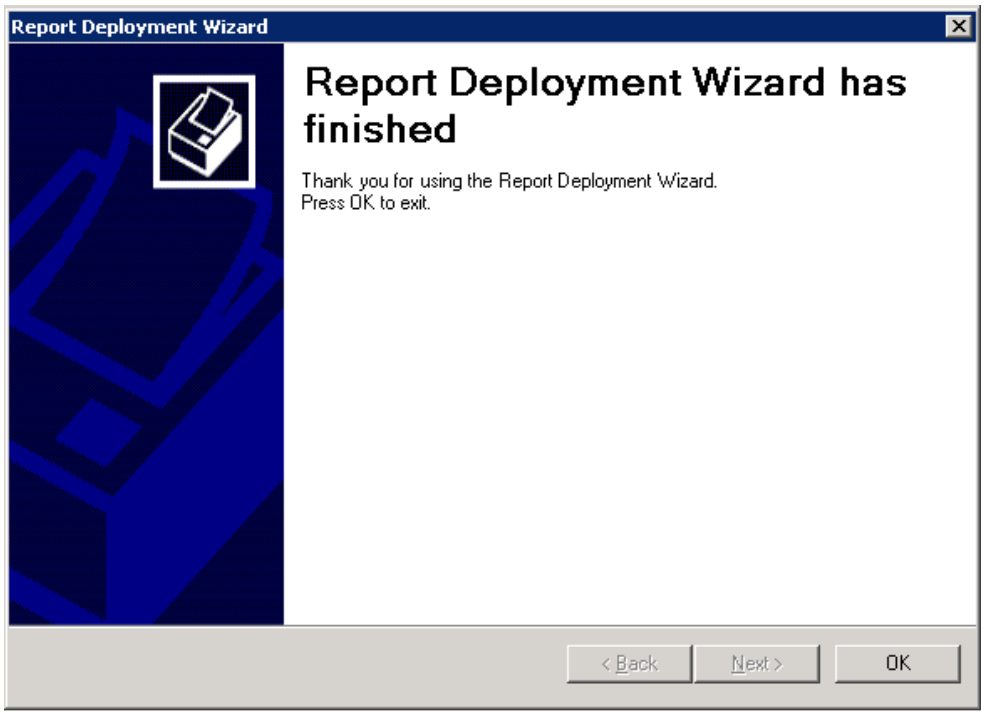
e) Enter the properties for the ReportServer database as defined in the previous section, not the ARM database. The account credentials used here will be stored in a data source in SSRS.



f) Confirm the details entered and press next to continue.







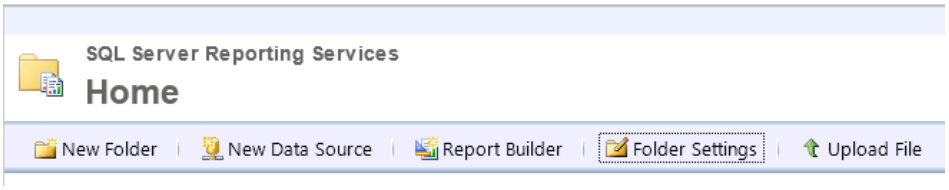
g) If you encounter any errors please retrieve the ReportDeploymentWizard-[Date-Time].log file from

```
Program Files\Active Risk Manager\Server\Reporting Services
```

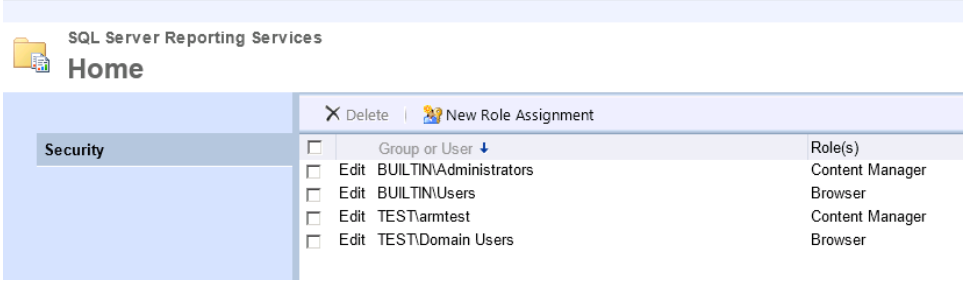
and send it to Active Risk Support.

h) Log into Report Manager

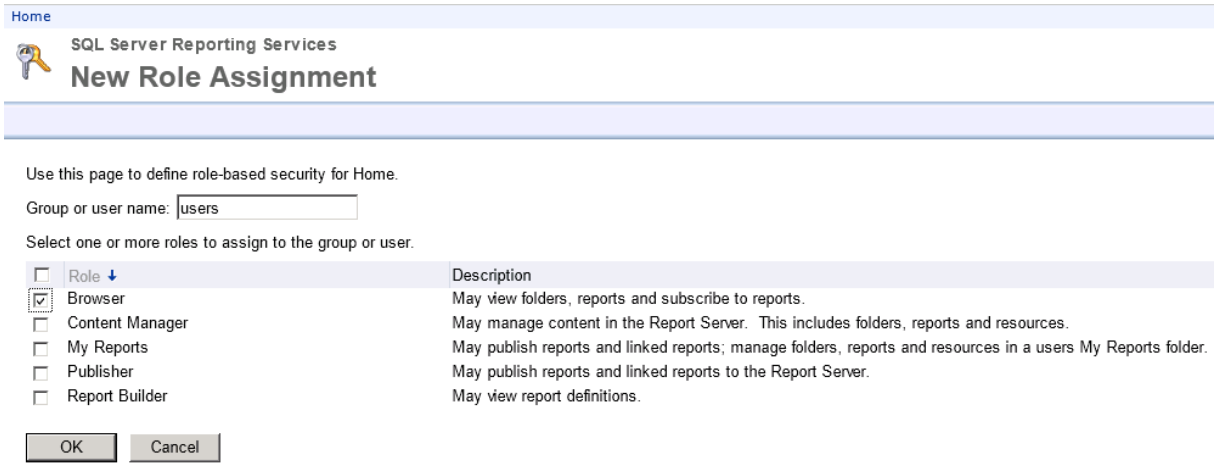
i) Click Home and then go to Folder Settings:



j) Click on New Role Assignment Under Security Tab

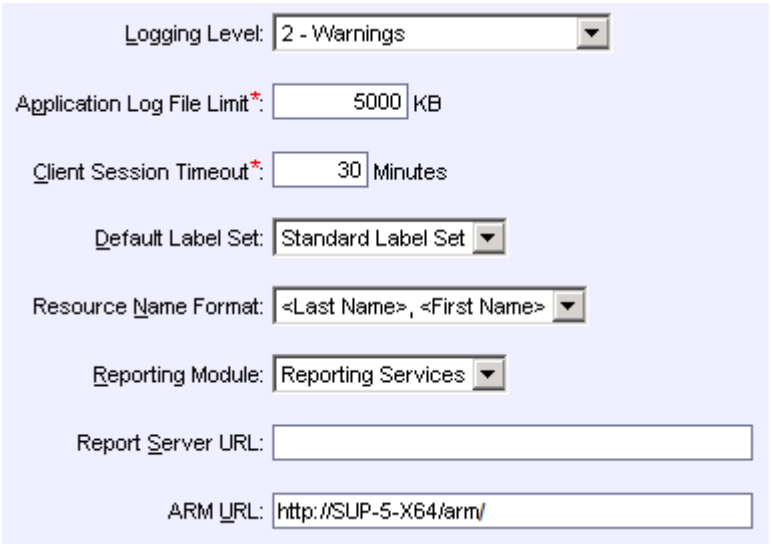


k) Add a new role as Browser for the user or domain/user who should access ARM Reporting Services.

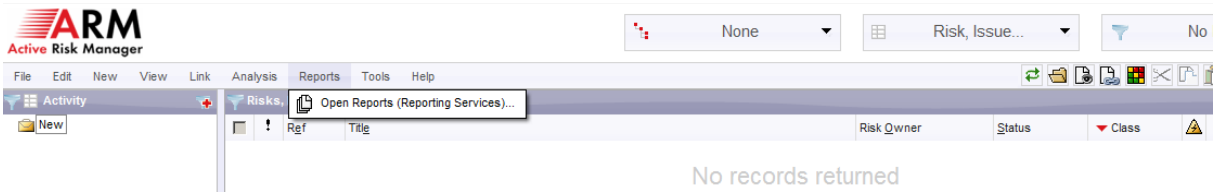


l) Log into ARM application with an ARM Administrator account and set the Report Server URL for each instance from Tools –Admin – on the Preferences Tab - System – Settings button.

Ensure that the ARM URL is correct and has the / at the end.



m) Test the reports by following the link from within ARM under Reports – Open Reports (Reporting Services). Report any problems to Active Risk Support.



7.7 ARM Custom Reports Deployment

For details on how to deploy your custom reports please refer to the documentation provided with the Custom Report originally when delivered as each may have specific requirements or get in touch with Active Risk Support team.

8 ARM Application Framework

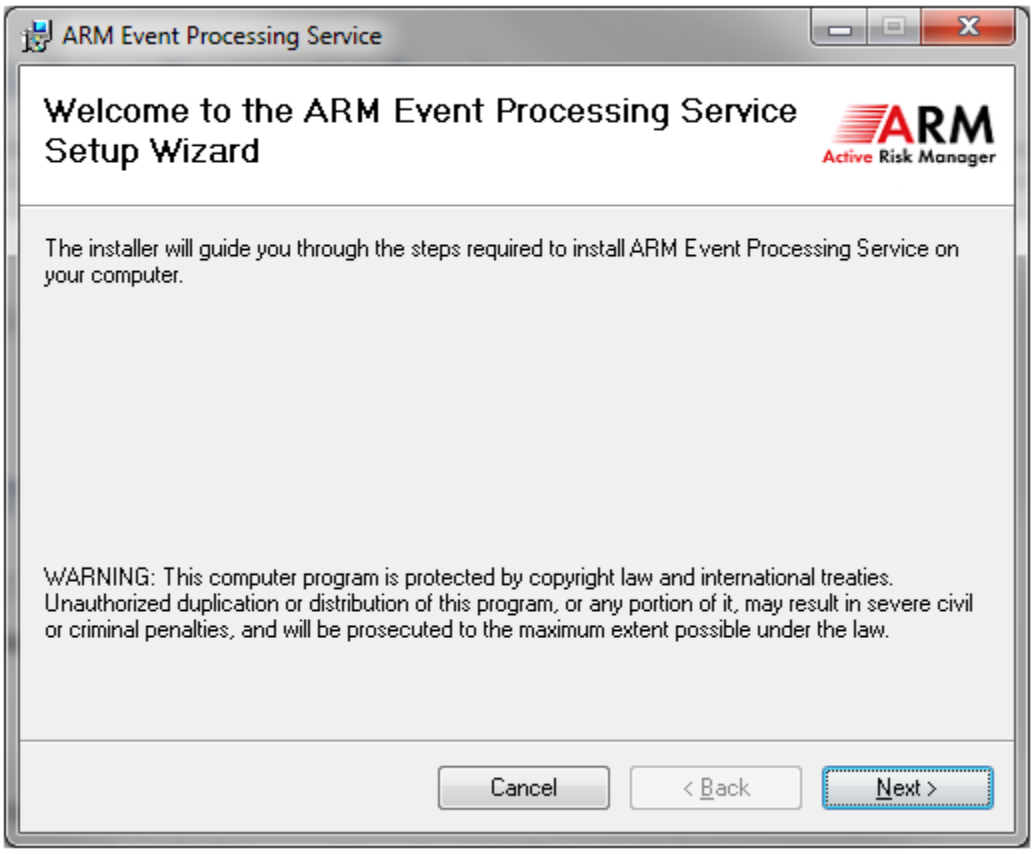
If you would like to access the Installation material for ARM Application Framework Native IIS or Sharepoint solutions, please contact Active Risk Support who will be able to assist you with this.

9 Event Processing Service

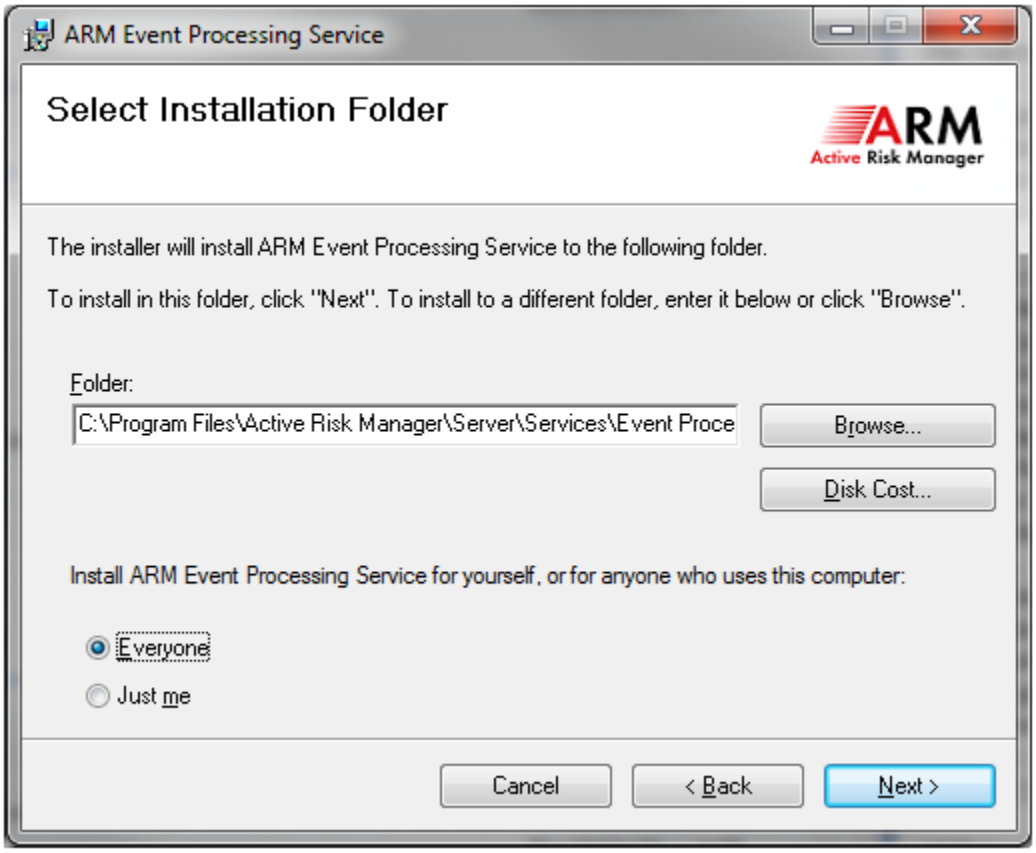
The event processing service is a component designed to publish ARM events to a variety of user customisable event handlers. The service runs on the ARM application server as a Windows service with a set of custom plug-in. The installer shipped with the Active Risk Manager Media will install and configure the Windows service, the deployment of custom event handlers is a separate task.

Installing the Service

On the Active Risk Manager Installation media there is a folder name Events Service, run the file setup.exe to being the installation. Ensure you right click and select "Run as administrator" if applicable.

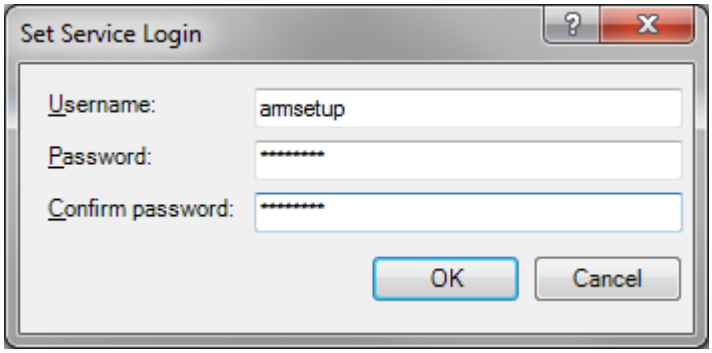


Begin the installation by clicking 'Next'

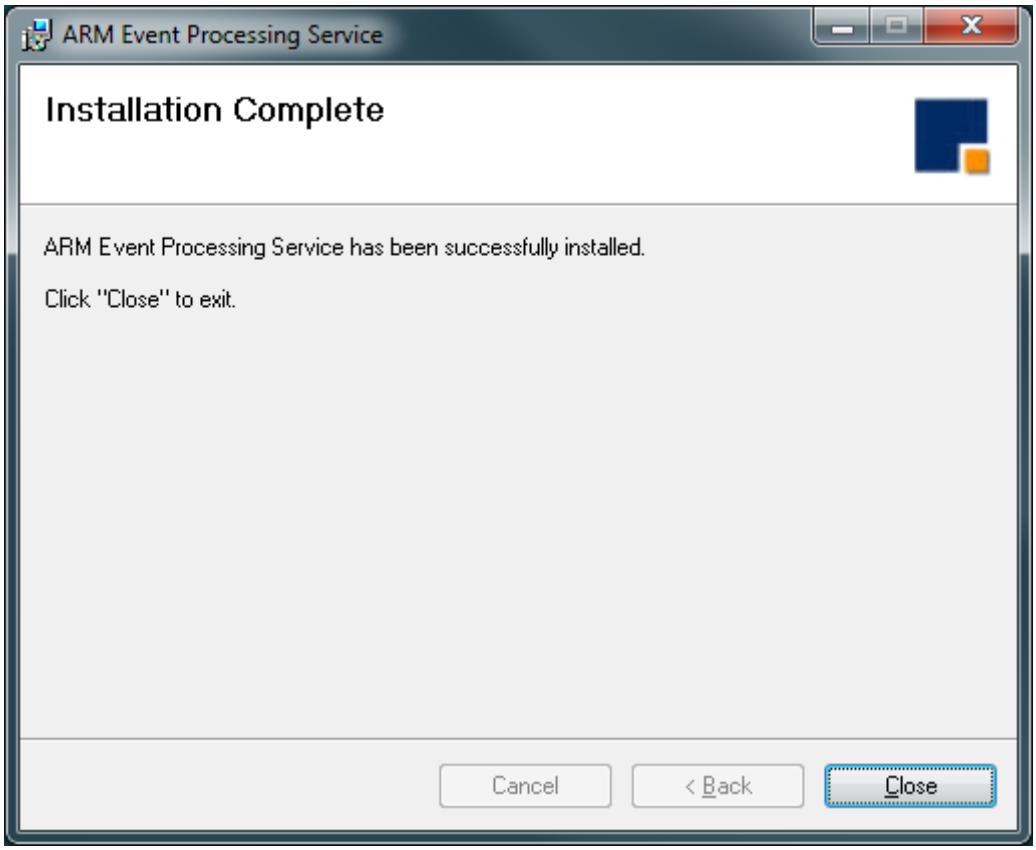


The service should be installed in the Active Risk Manager Installation folder. On a standard install this will be `C:\Program Files\Active Risk Manager\`

During installation you will be prompted to supply a username and password to run the service. We recommend a Domain Account such as ARMSetup, though the service can run under a Local System Account. Whichever account is chosen will need write access to the location the service is installed under to enable logging. If you use a local account remember to prefix the account name with the server name or domain e.g. domain\armsetup or armserver\armsetup



Another consideration is that the service will be running all the custom event handlers in the same process so the ambient credentials of the running user can be accessed. For full details please see the Event Publishing Development Guide in the ARM install media under the Docs directory.



Once the service has been successfully installed it can be started from the services control panel. Found in Control Panel -> Administrative Tools -> Services. Called ARM Event Publishing Service

9.2 Deploying Event Handlers

With the service installed event handler plug-in can be deployed to handle events in different ways. Once a plug-in has been developed it needs to be deployed into the ‘plug-in’ directory of the event handler. Full details and instructions for this procedure can be found in the Event Handler Developer Guide in the ARM install media under the Docs directory.

9.3 Uninstalling

To uninstall it is first necessary to stop the windows service that is running. Then open the add/remove programs tool in the Control Panel and select the option ARM Event Processing Service.

10 Third Party Integration

10.1 Primavera

Supported Product Versions:

- Primavera 8.2 (recommended version)
- Primavera 7.0 SP3 (recommended version)
- Primavera 7.0 SP1
- Primavera 7.0

This functionality is only available if your ARM licence includes the "Primavera" feature.

Please refer to the Primavera Integration/Installation Guide for more information.

10.2 Artemis Views

Please note that Artemis Views is no longer supported. This is due to lack of customer demand.

10.3 IBM DOORS

Supported Product Versions:

- DOORS 9.2 (recommended version)

The appropriate version of DOORS must be installed on the client computer for users who wish to produce the export files from DOORS. Please contact Active Risk Support who will provide the required customisations for DOORS. This will need to be run on each client machine which requires DOORS integration.

Exchange of requirements modules (import and export) between ARM and DOORS requires use of a shared network folder, accessible from both the ARM server and the client computer of the DOORS user. By default this folder is located on the ARM server. The same folder must be accessible from the client computer, using a network path or mapped drive.

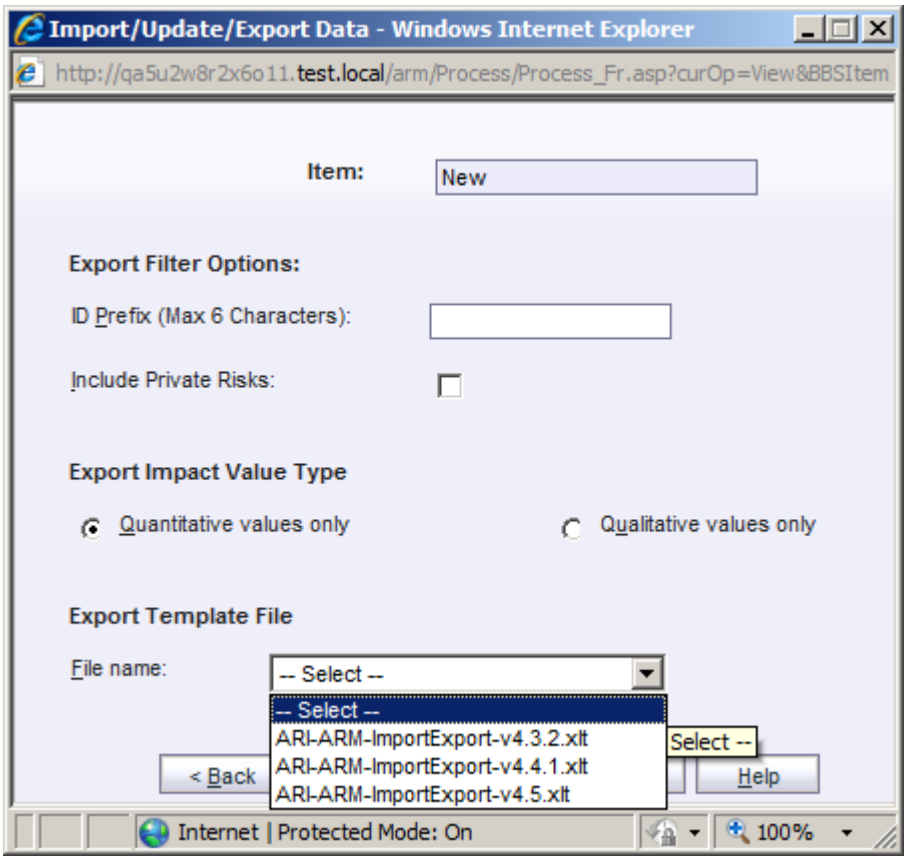
10.4 Microsoft Excel Module

The Import from Excel feature allows Risk, Impact, Plan and Response data to be imported from an Excel spread sheet template supplied with ARM.

The spread sheet template contains validation to ensure the integrity of data imported into ARM. Therefore, text must be typed directly into spread sheet cells or pasted as values only to prevent the spread sheet formatting being overwritten.

Excel files can be imported from any location accessible from the client machine.

This functionality is only available if your ARM licence includes the “Microsoft Excel” feature.



Microsoft Excel Risk, Impact, Plan and Response Integration have been updated for ARM 6 – the supported Excel template version is ARI-ARM-ImportExport-v4.5.xlt. Also supported are ARI-ARM-ImportExport-v4.3.2.xlt (Previously - STL-ARM-ImportExport-v4.3.2.xlt) and ARI - STL-ARM-ImportExport-v4.4.1.xlt – (Previously - STL-ARM-ImportExport-v4.4.1.xlt).

For the Excel versions support see the Support Matrix located in the Docs folder on the ARM media.

It is also possible to import activities in to the activity tree from Microsoft Excel. This functionality requires a different upload template (please request this from STG support) and a Microsoft Component (Office 2007 ODBC Driver) which you will need to download and install on your ARM server from the following site:

http://www.microsoft.com/downloads/details.aspx?FamilyID=7554F536-8C28-4598-9B72-EF94E038C891&displaylang=en

11 Reverse Proxy with LDAP and SSO Configuration

11.1 ARM Application configuration

a) Modify the ARM registry settings so that they reflect the changed authentication mode.

HKEY_LOCAL_MACHINE\SOFTWARE\Strategic Thought Ltd\Active Risk Manager Server

AuthenticationMode = '3'
AuthenticationVariable = 'HTTP_AUTHORIZATION'
SetupDomainName = 'EXTERNAL'

Authentication Mode 1 is for standard Windows Integrated Authentication, mode 2 is for third party SSO authentication, mode 3 is for Reverse Proxy with LDAP.

AuthenticationVariable should be set to the header that contains the username once authentication has been successful. For Reverse Proxy with LDAP this standard is HTTP_AUTHORIZATION. SSO products have their own specific or user defined values.

SetupDomainName should always be set to EXTERNAL if you are not using Windows Integrated Authentication.

b) When adding users to ARM application enter the domain value as EXTERNAL.

The following steps For Reverse Proxy with LDAP Only:

c) On the ARM virtual directory in IIS set the Authentication Mode to Anonymous Access for Reverse Proxy with LDAP.

d) Add ProxyPass and ProxyPassReverse directives for ARM, arm and ReportServer virtual directories as required.

e) Edit the ARM web.config file located at \Program Files\Active Risk Manager\Server\Web\web.config and modify the following values accordingly.

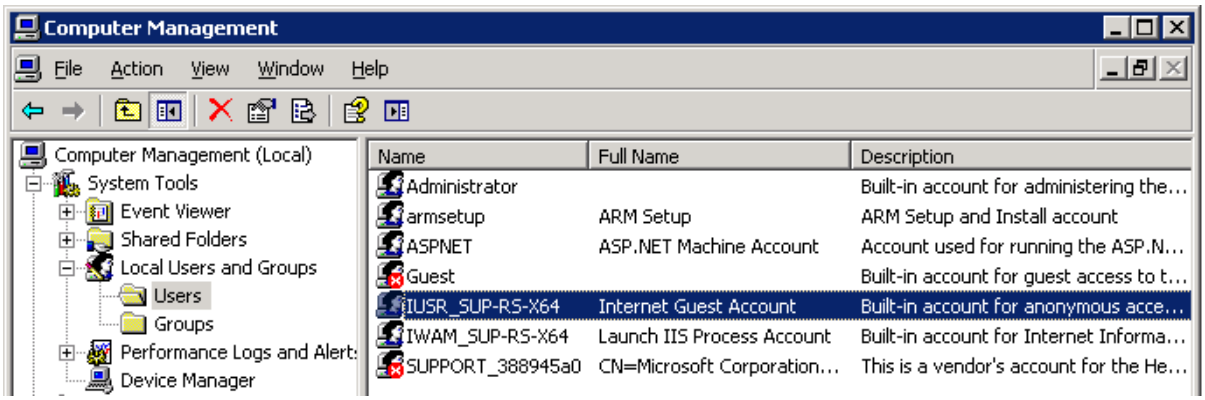
```
<add key="ReverseProxyHostName" value="<hostname>"/>
<add key="ReverseProxyPort" value="<port number>"/>
<add key="ReverseProxyScheme" value="<http/https>"/>
```

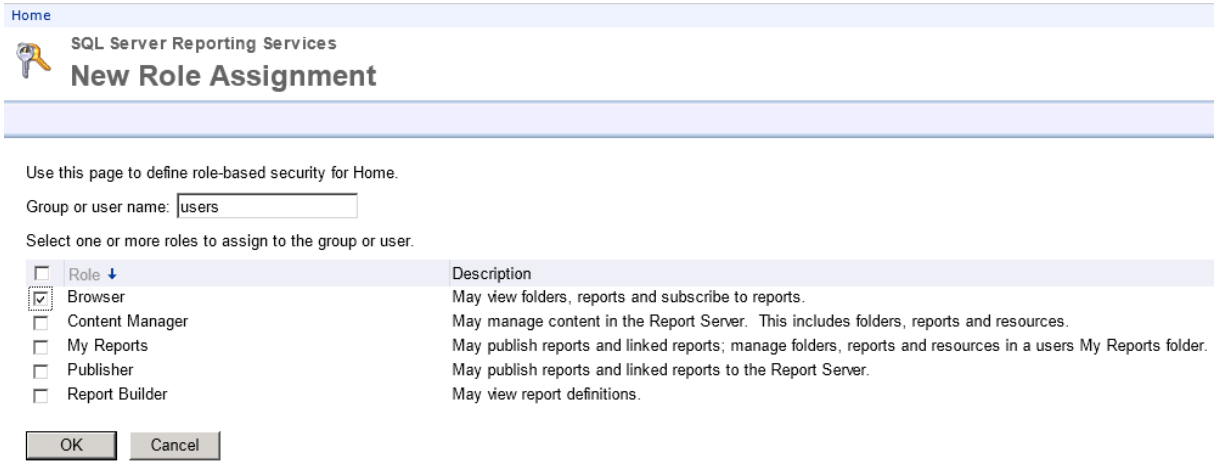
f) ReverseProxyHostName value should be the same as that used by end users to access ARM whether that is FQDN or simply a hostname.
g) ReverseProxyPort need only be defined if a non standard port for the given scheme is used i.e. HTTP/80 or HTTPS/443.
h) ReverseProxyScheme can only take one of two values, either http or https.

11.2 SSRS configuration

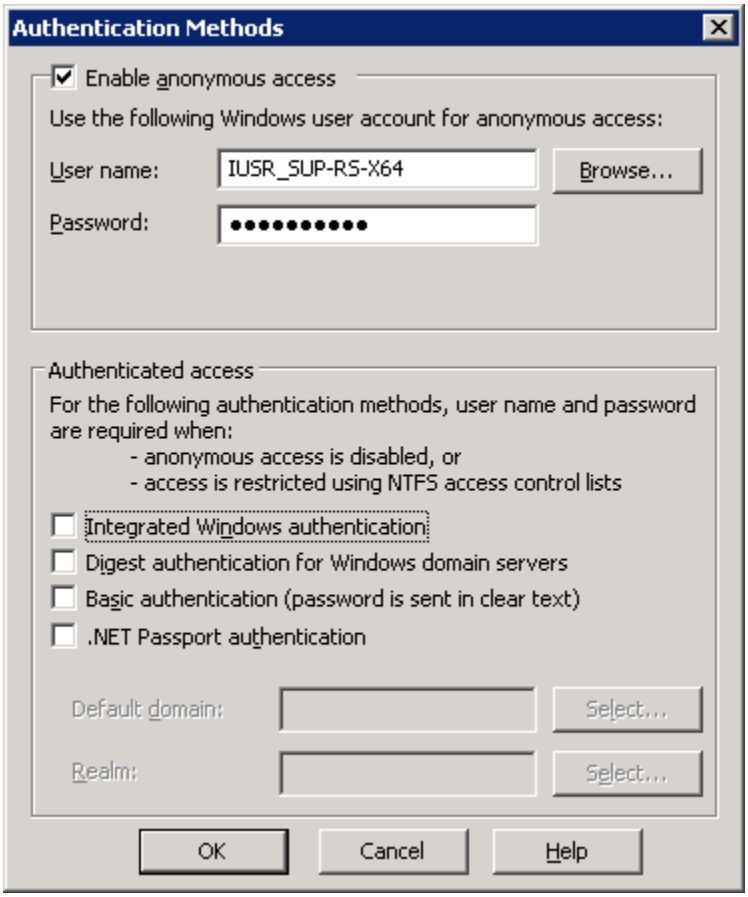
This configuration should only be done once the reports have been uploaded in the usual way.

a) Grant the anonymous internet user account the browser role through the Report Manager interface. This should be in the format [SERVER NAME]\IUSR_[SERVER NAME]





b) On the ReportServer virtual directory in IIS set the authentication method to Anonymous Access if you are using Reverse Proxy with LDAP. Disable Integrated Windows Authentication.



For SSO you should follow the software specific guidelines for enabling the SSO authentication.

c) To upload new custom reports and/or updated standard reports using the deployment wizard, temporarily enable Integrated Windows Authentication and disable Anonymous Access for the duration of the work.

12 Post Installation Configuration

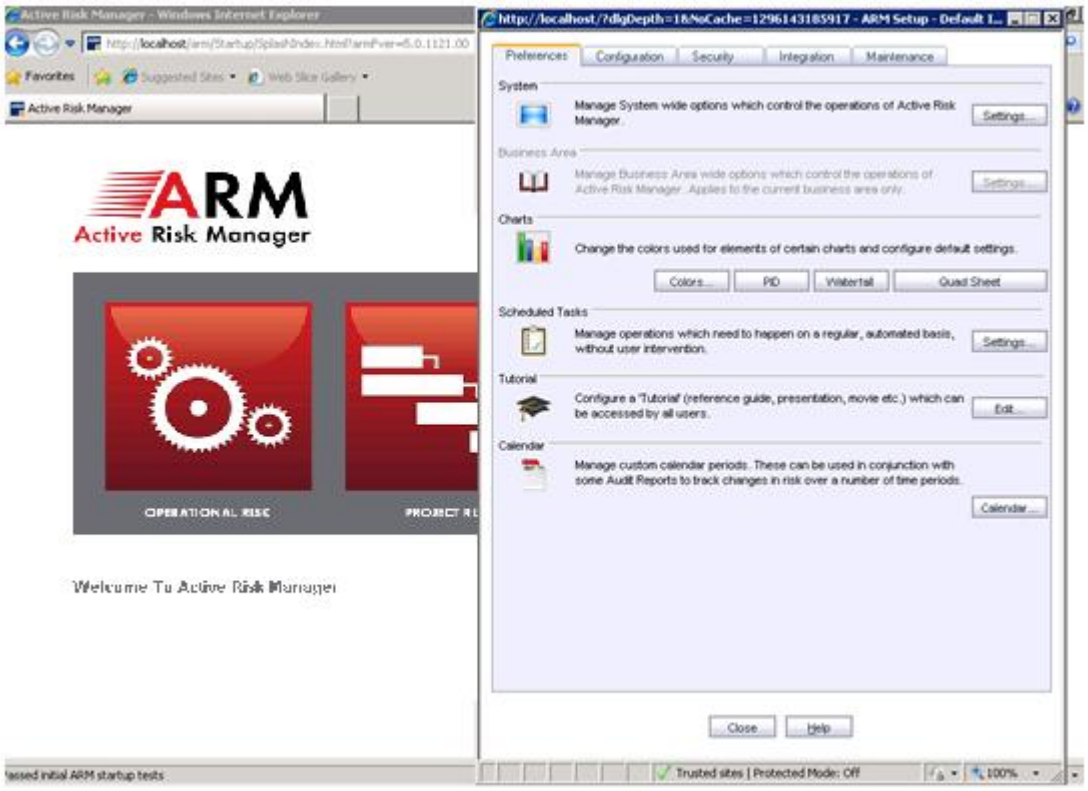
12.1 Basic Application Test

a) Change your Internet Explorer settings to force your browser will prompt you for login credentials.

b) Tools – Internet Options – Security Settings – Local Intranet – Custom Level – User Authentication (Logon) – Prompt for username and password.

c) Open Internet Explorer on the application server and browse to http://localhost/arm. When prompted for credentials enter the details of the service account configured in the installer (armsetup).

d) Press the Setup button. If this dialog opens without generating errors then all major parts of the application are working well.



e) Go to the Security tab, and click on the Users button to add users. Add a user to the group labelled 'New Folder Admins' initially. Domain and username should match those used to log onto your client machine.

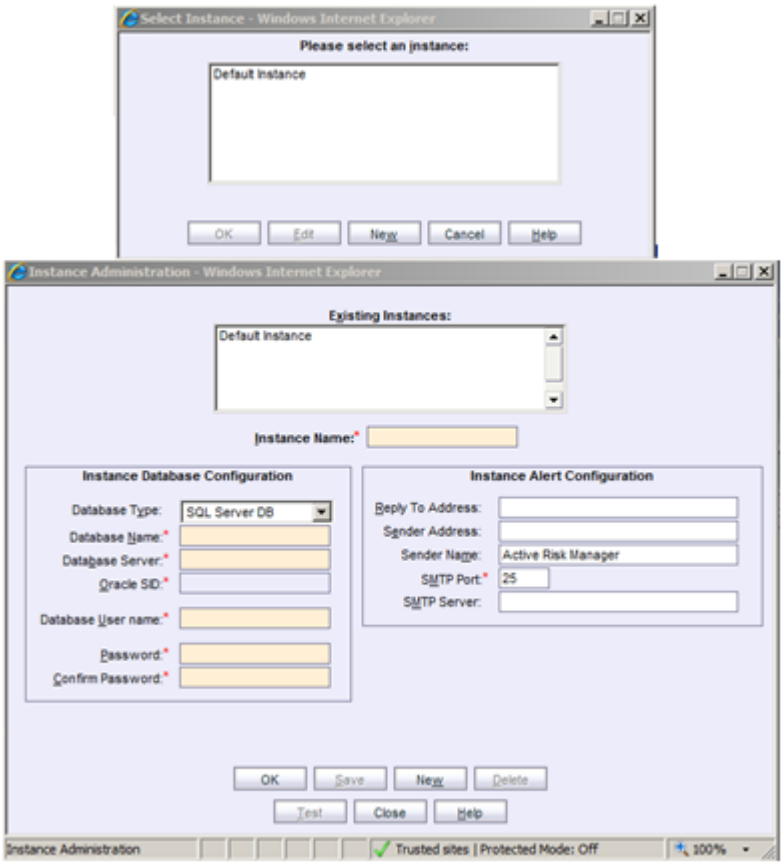
f) From a client machine logged on with the account referenced in the previous step, open Internet Explorer and browse to http://servername/arm

12.2 Add Additional Instances

a) While logged in with the service account (armsetup) click on the ‘Change Instance’ link in the bottom left hand corner.

b) Click on the new button to Add new instances or Edit to modify the existing configuration.

c) Once saved, use the Test button to confirm the database connection settings applied



12.3 Configure SMTP Settings for ARM Alerts

a) From the Edit option on the Change Instance dialog you will be able to configure the SMTP setting to be used with ARM Alerts.

b) You will need to restart the ARM Alert Service from services.msc before the changes to be picked up.

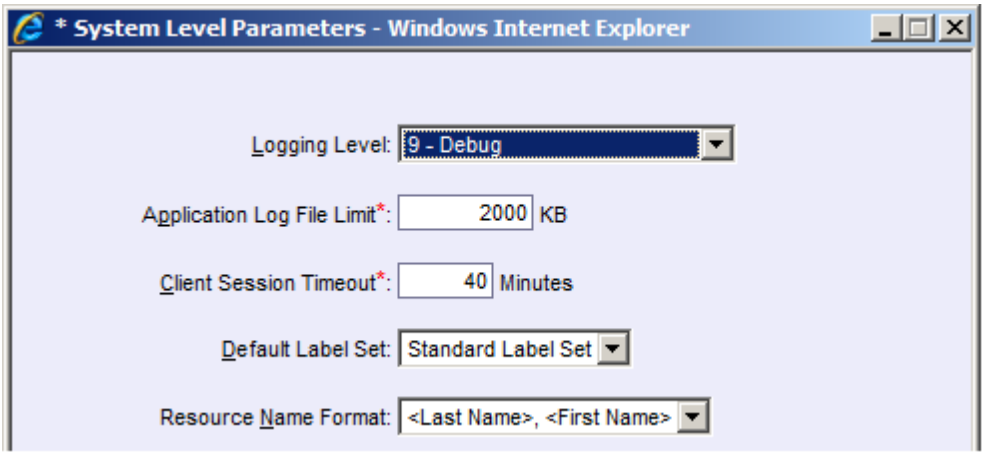
c) \Program Files\Active Risk Manager\Server\Tools\Alerts\EmailTest.exe can be used to test the SMTP connection and send a test email.

12.4 Application Log Files

a) The application log file can be accessed from the Maintenance tab or directly from the application server file system. There is one per database instance.

\Program Files\Active Risk Manager\Server\Logs\ARMApplicationLog_1.txt
\Program Files\Active Risk Manager\Server\Logs\ARMApplicationLog_2.txt

b) The log level can be changed from 1 Errors Only, 2 Warnings, 9 Debug etc. from the Preferences tab, System Settings button. If there are any application errors you will normally be asked to capture the error in Debug log level before sending to STG Support.



c) Beware that log level 9 Debug generates large log files which could consume all of the available disk space in days/weeks depending on system usage. It is advisable to keep the log level on '1 Error Only' until problems occur.

12.5 Client Side Configuration

a) The following settings will need to be applied to the Internet Explore security zone for the ARM application. See http://support.microsoft.com/kb/174360 for full details on each of the zones.

Script Active X controls marked safe for scripting - ENABLE
Download signed Active X controls – PROMPT
Run Active X controls and Plug-ins - ENABLE
Active scripting Enable – ENABLE
Allow cookies that are stored on your computer - ENABLE
Allow per session cookies – ENABLE

b) For client machines that do not have permission to install ActiveX controls an MSI installer is provided on the ARM installation media under the \Support\ActiveX folder. This can be used manually on each machine on distributed through GPO.

c) The ARM application should not be access through a proxy server. You will need to add exclusion rules to your client side proxy settings to bypass the proxy server.

13 Oracle Database Performance Recommendations

a) Execute the dbms_utility package to re-compile all schema objects, for example

```
EXEC DBMS_UTILITY.COMPILE_SCHEMA('ARM_SCHEMA')
```

Generate optimizer statistics weekly and especially after a restore from backup to test environment etc, for example

```
DBMS_STATS.GATHER_SCHEMA_STATS(ownname=> 'ARM_SCHEMA , cascade=>
TRUE);
```

b) There are other recommendations available for optimised performance of Oracle however we would recommend consulting your DBA to validate that it is desirable and will bring improvements:

- Allocate minimum 3 GB memory to SGA
- Change cursor_sharing parameter to FORCE
- Enable default database maintenance jobs.
- Change db_file_multiblock_read_count=128
- Change optimizer_mode to FIRST_ROWS

14 MSDTC Configuration Specifics

MSDTC is an acronym for Microsoft Distributed Transaction Coordinator which is a transaction manager program that permits client applications to include several different sources of data into one transaction. MSDTC then coordinates committing the transaction across all of the servers that are listed in the transaction. MSDTC needs to be installed, enabled, and running on both ARM and SQL Database servers for ARM to work.

14.1 Server Ports used by MSDTC:

Operating System	MSDTC sending out transaction messages on port	MSDTC response messages return on a dynamically assigned port in range
Windows 2008 R2	135	49152 to 65535

14.2 DTC Communication

Out of various setup specific requirements DTC requires following to be able to communicate between servers:

- being able to resolve names by DNS or NetBios (from both sides)
- being able to communicate through port 135 (RPC Endpoint Mapper port for handshake)
- being able to dynamically assign at least one port for communication (by default in the 1024 – 65535 range)
- RPC & DTC must exist on all participants

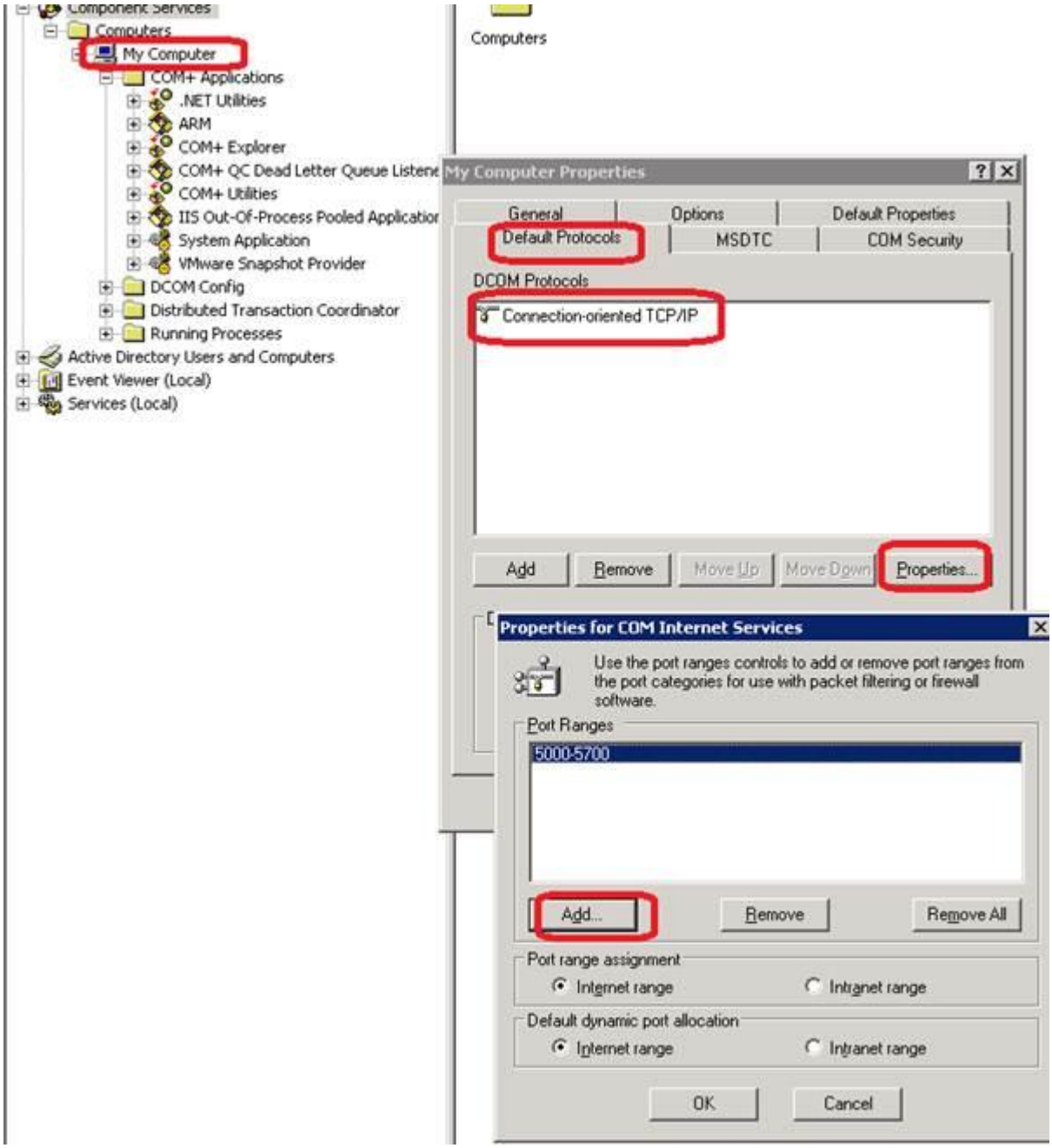
If there is a firewall between ARM and DB server, the MSDTC transactions could get blocked.

14.3 Firewall Considerations

To avoid any firewall issues, it may be required to open some specific port ranges on Firewall to be used for MSDTC. At least 200 ports should be opened on the Firewall (otherwise it may cause port exhaustion). Once firewall ports are opened for MSDTC, the ARM server needs to be updated to use only these ports for MSDTC transactions.

Follow these steps to allow customer ports for MSDTC.

Log on the ARM application server
Open Adminstrative Tools – Component Services
Expand Component Services – Computers – My Computer
Right click on My Computer and select Properties
Click on Default Protocols
Select “Connection-oriented TCP/IP” and then click on properties button
Click on add button
Add the port range



Please contact support@activerisk.com for your requirement if you would like to discuss MSDTC configuration.