PowerScribe® 360 Reporting

Upgrade Manual

PN 889679 *September 28, 2018*

PN 889679

Printed in U. S. A. September 28, 2018

Trademarks

Nuance®, the Nuance logo, Dictaphone®, Dragon® NaturallySpeaking®, PowerScribe®, RadPort™, and RadWhere™ are trademarks or registered trademarks of Nuance Communications, Inc. or its affiliates in the United States and/or other countries. All other trademarks referenced herein are trademarks or registered trademarks of their respective owners.

Copyright Notice

This manual is copyrighted and all rights are reserved by Nuance Communications, Inc. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of Dictaphone Healthcare Solutions, Nuance Communications, Inc., 1 Wayside Rd., Burlington, MA 01803.

Copyright © 2018 Nuance Communications, Inc. All rights reserved.

Disclaimer

This document is provided "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Nuance shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including, without limitation, damages resulting from use of OR RELIANCE ON the INFORMATION presented, loss of profits or revenues or costs of replacement goods, even if informed in advance of the possibility of such damages.

Every effort has been made to ensure the accuracy of the information presented. However, Nuance assumes no responsibility for the accuracy of the information. Product information is subject to change without notice. Changes, if any, will be incorporated in new editions of this publication. Nuance may make improvements and/or changes in the products and/or the programs described in this publication at any time without notice. Mention of non-Nuance products or services is for information purposes only and constitutes neither an endorsement nor a recommendation.

Table of Contents

Table of Contents iv

Best Practices 1-1
Notations 1-2

Pre-Upgrade Checklist 2-1

Preliminary Steps 2-2
Run Upgrade Scripts 2-2
Backup the System Data 2-2
Upgrading a System Which Uses “AlwaysOn SQL” 2-4
Verify Access to IPs and Ports 2-8
Apply All Firmware and Microsoft Updates 2-8
V4.0.1 (SP1) Upgrade - Microsoft SQL Server Management Studio Requirement 2-8
Migrated Database to a New Server 2-10

Upgrade Process 2-11
Software Download 2-11
Client Admin Cleanup 2-11
Run Upgrade Tool 2-12
Run Database Upgrade 2-18
Completing the Upgrade - Installing Your New Version 2-28
Client Administration Configuration Tool 2-38
Update Clinical Guidance Rules 2-44
If site will FAX out of PS360
Downgrade PDF version on Application Server 2-45
Apply Post Installation Hot Fixes 2-46
Enable UAC 2-46

Mobile Server 2-47
Enable UAC 2-47

Speech Server (SUS) 2-48
Verify Dragon Version 2-48
Upgrade Dragon SDK Medical Software on SUS 2-48
Verify SUS Version 2-49
Uninstall Applications 2-49
Upgrade Microsoft SQL Server Express 2-51
Install the SUS Software 2-56
Enable UAC 2-64

PowerXpress 2-66

Enable UAC 2-66

Upgrade Add-On Products / Modules 2-67
Hot Spare 2-67
Upgrade ModLink 2-67
Upgrade ModLink Web Forms 2-67
Upgrade mPower 2-68

Appendix 1 - Troubleshooting . . . . . .Appendix 1-1
Password Conversion Issues . . . . . .Appendix 1-1
Login Issues . . . . . .Appendix 1-2

Appendix 2 - Microsoft Windows Configuration Guidelines . . . Appendix 2-1

Appendix 3 - Microsoft SQL Server Installation Guidelines . . . Appendix 3-1

Manual Revision History History-1

Best Practices

- Nuance recommends following Microsoft best practices as outlined in

  Microsoft TechNet General Security Advice and Best Practices

- ***PowerScribe 360 Reporting*** stores data containing Protected Health Information (PHI) in the product databases as well as in various locations throughout the file system. Nuance recommends encrypting ***PowerScribe 360 Reporting*** at the operating system and/or storage system levels to ensure that PHI is encrypted consistent with the customer's data encryption policies.
- ***PowerScribe 360 Reporting*** is compatible with several currently supported versions of Microsoft Windows Server operating systems, Nuance recommends using the latest compatible version listed in the ***PowerScribe 360 Reporting*** System Specifications, currently ***Windows Server 2016***.
- ***PowerScribe 360 Reporting*** is compatible with several currently supported versions of Microsoft SQL Server, Nuance recommends using the latest compatible version listed in the ***PowerScribe 360 Reporting*** System Specifications, currently ***SQL Server 2016***.
- Nuance recommend that all ***PowerScribe 360 Reporting*** network communication be secured and encrypted using Hypertext Transfer Protocol Secure (HTTPS). Nuance also recommends that the customer obtain a certificate from a trusted Certificate Authority consistent with the customer security policies.
- Nuance fully supports all third-party hardware and software updates related to critical security fixes immediately upon release. Nuance recommends that customers apply third party updates consistent with their internal security policies.
- ***PowerScribe 360 Reporting*** supports Lightweight Directory Access Protocol (LDAP). Nuance recommends the use of LDAP for end-user authentication to ***PowerScribe 360 Reporting*** to ensure consistency with the customer's authentication and password management policies.
- During the ***PowerScribe 360 Reporting*** installation process several system level users and associated passwords need to be created. Nuance recommends that the Customer's site administer provides the system level passwords consistent with the customer's internal password policies. Nuance recommends the use of strong/complex passwords consistent with the customer's password management policies.
- Nuance recommends that any Passwords created during ***PowerScribe 360 Reporting*** installation and configuration only be communicated over secure encrypted channels and/or stored in secure encrypted locations.
- Nuance recommends that customers protect ***PowerScribe 360 Reporting*** from viruses, malware, data loss, etc. consistent with their internal policies. To prevent performance degradation Nuance recommends excluding ***PowerScribe 360 Reporting*** processes from antivirus (AV), data loss prevention (DLP), or similar applications to prevent interference with application operations resulting in latency and or file manipulation. Process exclusion will protect application

performance while allowing AV, DLP, etc. to monitor file operations initiated by other processes. Specific locations and file types are available for AV applications that do not allow process exclusion, see Article 6870: *Files and Folders Acted Upon by the PS360 Client and Servers* for details.

- Nuance does not recommend exposing network services to untrusted networks unless otherwise advised by Nuance documentation or Support.

Notations

This section defines notations that may appear throughout the document.

Best Practice	This **Best Practice** icon indicates the recommended Nuance procedure to follow when installing or configuring the Nuance PowerScribe 360 application. For example: • PowerScribe 360 Reporting supports Lightweight Directory Access Protocol (LDAP). Nuance recommends the use of LDAP for end-user PS360 access. • During the PowerScribe 360 Reporting installation process several system level users and passwords need to be created. The Customer's site administer should provide system level passwords consistent with the customer's internal password policies. Passwords should only be communicated over secure encrypted channels and/or stored in secure encrypted locations. • Microsoft General Security Advice and Best Practices. • Client workstations rebooting recommendations. • Nuance Anti-Virus recommendations. • Nuance recommends the use of LDAP for end-user PS360 access.
 IMPORTANT	The **IMPORTANT** icon indicates to the reader's attention to important information you don't want them to miss.
	The **NOTE** icon provides auxiliary information or further explanation to the adjacent paragraph(s).
	This **STOP** icon is an indication that a necessary requirement is to be met before you proceed to the next step.

Pre-Upgrade Checklist

Step	Task	Information
Pre Install		
	Review Upgrade Questionnaire	Review for possible conflicts.
	Verify OS Configuration	Appendix 2 - Microsoft Windows Configuration Guidelines
	Verify and upgrade, if necessary, MS SQL to the latest supported version	Appendix 3 - Microsoft SQL Server Installation Guidelines
	Confirm if using PS360 Faxing	See **If site will FAX out of PS360 Downgrade PDF version on Application Server**
	Is there a hot spare?	See Upgrading Systems with Mirrored Hot Spare Configuration (Hot Spares on version 3.0.x and lower) or See Upgrading a System Which Uses “AlwaysOn SQL”
	Run Pre-Upgrade Scripts	Well before the upgrade, you should Run Upgrade Scripts.
Install		
	Upgrade from V1.x	Use Software Installation Manual — 889718
Post Install		
	Is there a Hot Spare?	Hot Spare Installation and Configuration — 889715 Client Hot Spare — 889719
	Perform Checkout	System health checks tool is on the DML: https://private.filesany-where.com/Nuance/fs/v.aspx?v=8972658a9e61b47a9e
	Is LDAP disabled?	If LDAP is disabled, enable LDAP after the upgrade is complete.

Preliminary Steps

If you experience an issue using the tool, revert to the manual uninstall / reinstall process outlined in the standard install manual for your version.

Run Upgrade Scripts

Well before the upgrade date, be sure you run the following SQL scripts against the PRODUCTION database:

1. PS360 AutoText Migration to Version4.sql script.
2. PS360 AutoText Orphaned Removal.txt.
3. Default_Settings_That_Will_Change_In_3_5.SQL.
4. Save the outputs as CSV files, and provide the files to the project manager.

Backup the System Data

System Snapshot

- Have the Client take a system snapshot (VM or otherwise) of the Application and SQL server before starting this process.

Backup the Nuance Data Folder

- Make a backup copy of the x:\Nuance\ directory and sub folders.
- Place the backup(s) in a safe location, preferably in a place other than the server itself.

Upgrading Systems with Mirrored Hot Spare Configuration (Hot Spares on version 3.0.x and lower)

If the site has the Mirrored Hot Spare configuration in use (e.g. SQL mirroring), perform the following:

1. Break the mirror between the production and Hot Spare systems and turn off mirroring.
2. Disable and delete the Hot Spare Windows scheduler jobs used to replicate profiles, waves, and logs on both the production and hot spare systems

3. If not already performed, you will need to upgrade the operating system of the MSSQL server to the Windows Enterprise version by applying the new/proper license keys.
4. If not already performed, you will need to upgrade the MSSQL server application to the Enterprise version by applying the new/proper license keys.

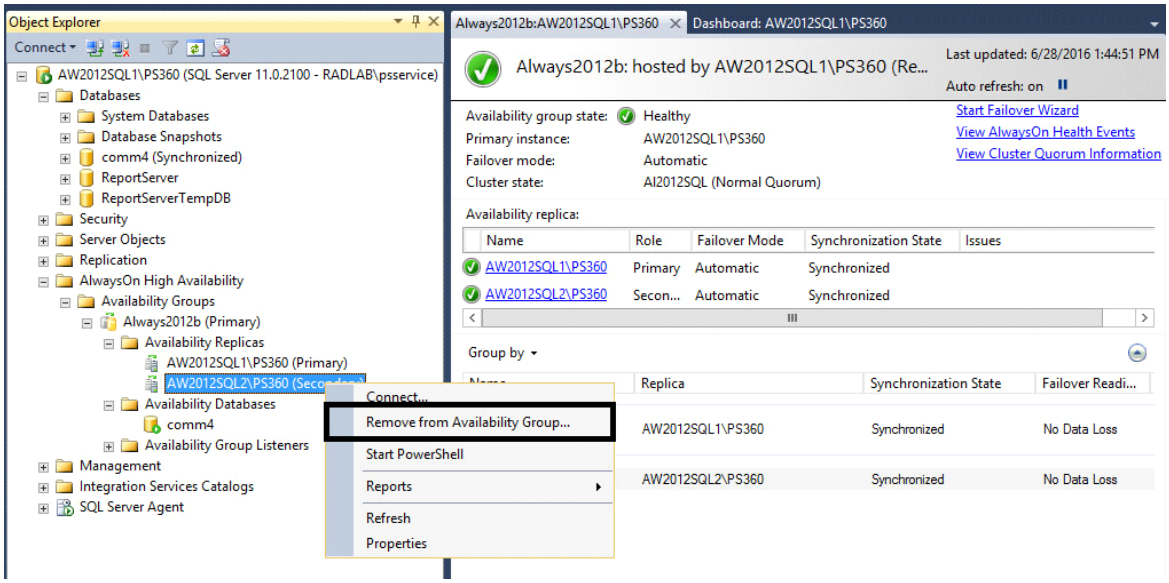
Upgrading a System Which Uses “AlwaysOn SQL”

The following provides the steps for upgrading the PowerScribe 360’s Comm4 database on a system running SQL AlwaysOn High Availability:

1. Stop all Nuance Application Services.
2. Make sure that the site's Primary server is set as the Primary Database server. If not, fail it over to the Primary server.

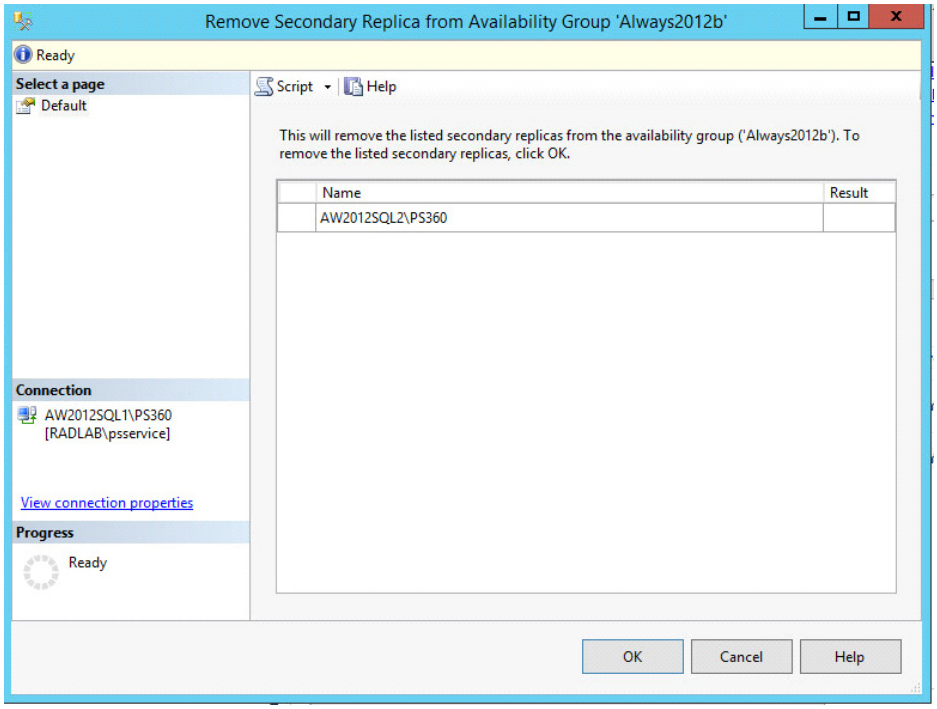
Remove Secondary Replica

1. Log in to the SQL Enterprise Manager to the Primary server.
2. Expand **AlwaysOn High Availability**.
3. Expand **Availability Replicas**.
4. Right-click the Secondary Replica, and select **Remove from Availability Group**.



The Remove Secondary Replica from Availability Group dialog displays.

5. On the Remove Secondary Replica from Availability Group dialog, click **OK** to remove the Secondary Replica.

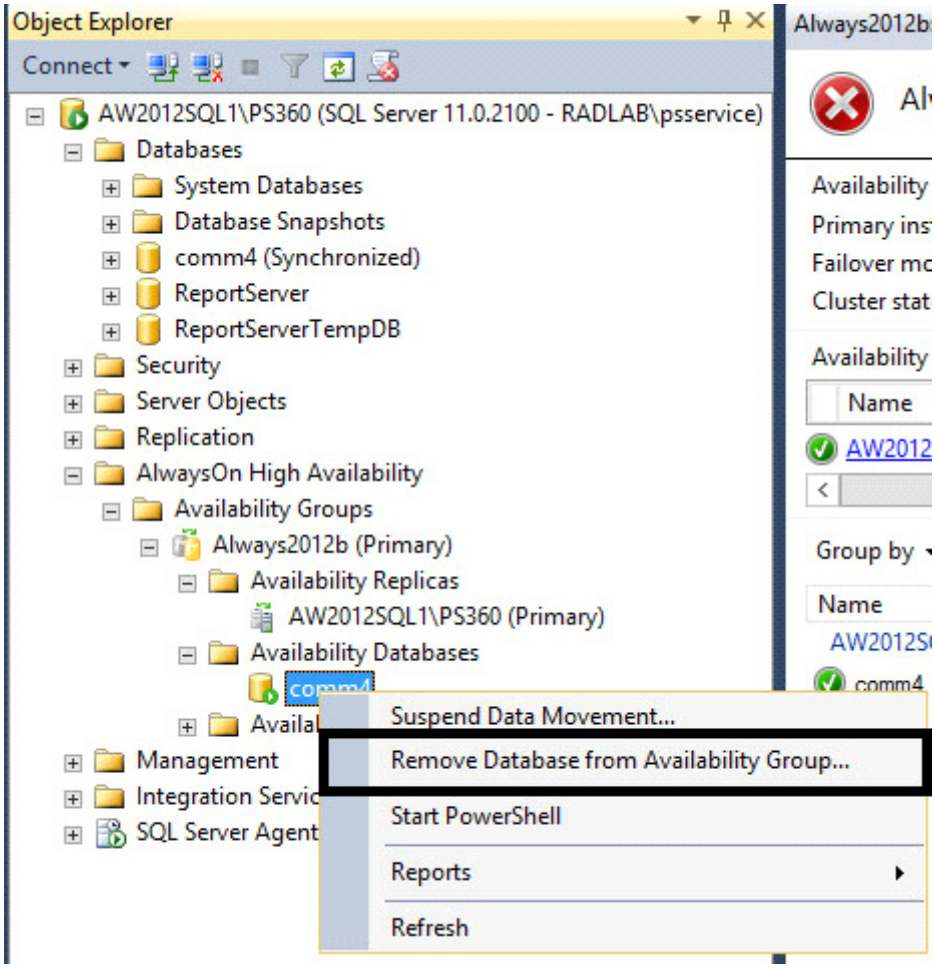


Remove Comm4 Database from Availability Databases

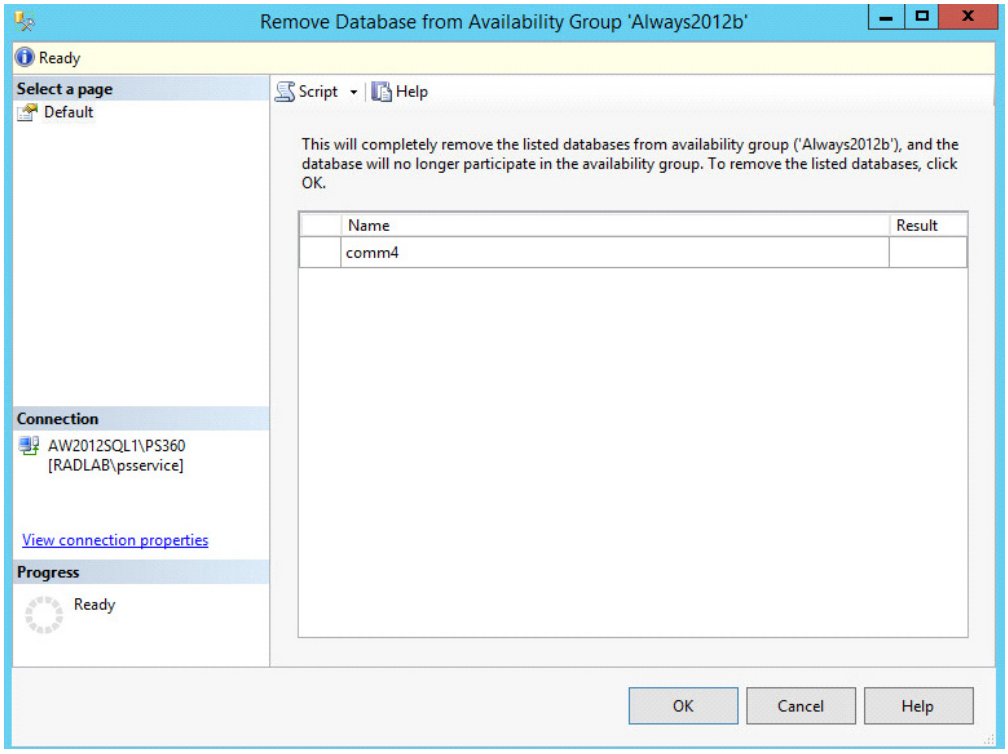
Next follow these steps to remove the Comm4 Database from the Availability Databases before you upgrade it.

1. Expand **AlwaysOn High Availability**.
2. Expand **Availability Databases**.

3. Right-click **Comm4** database, and select **Remove Database from Availability Group**.



The Remove Database from Availability Group dialog displays.



4. On the Remove Database from Availability Group dialog, click **OK** to remove the database.
5. Run DBSetup as you normally would pointing at the Primary SQL server.

Verify Access to IPs and Ports

Allow Internet access to the following IPs and ports. Verify the server has access to at least 2 of these URLs during the Application install. Access to them can be removed after the install is complete. These URLs are only used when running the Client Administration Configuration Tool later in this process.

http://timestamp.globalsign.com/scripts/timestamp.dll

202.176.218.10:80

202.176.218.11:80

202.176.218.12:80

http://timestamp.comodoca.com/authenticode

91.199.212.132:80

http://tsa.starfieldtech.com

173.201.19.11:80

68.178.177.11:80

http://sha256timestamp.ws.symantec.com/sha256/timestamp

If the site does not allow access to the Internet from the application server you will need to download the PS360ClientCabFileSigner tool to allow proper generation of the publication off line (without Internet) so a proper timestamp is applied.

Apply All Firmware and Microsoft Updates

Before beginning, run the Microsoft Updates tool and ensure all current Critical and Important updates are applied to the system. This is to help ensure that IE is at version 11 and that .Net Framework 4.5 is also installed.

Also, if the server was sold by Nuance and is under a maintenance contract, update the HP firmware and applications.

V4.0.1 (SP1) Upgrade - Microsoft SQL Server Management Studio Requirement

IMPORTANT

Service Installation - When installing on a system that has MicrosoftSQL Server Management Studio, install NDP462-DevPack-KB3151934-ENU.exe.

This is necessary because the .NET Framework application will point to the C:\Program Files (x86)\Reference

Assemblies\Microsoft\Framework\.NETFramework folder patch instead of C:\Windows\Microsoft.NET folder path.

If the application does not see the folder path C:\Program Files (x86)\Reference Assemblies\Microsoft\Framework\.NETFramework\v4.6.2, it will revert down to the folder patch.

C:\Program Files (x86)\Reference Assemblies\Microsoft\Framework\.NETFramework\v4.0, hence the Web Service Application will fail, and TLS 1.2 support will not work.

PowerScribe 360 Client - v4.0 required 4.6.1 .NET Framework. For v4.0.1, it requires 4.6.2 .NET Framework.

Migrated Database to a New Server

If you migrated the Database to a New Server, be sure to perform the following:

1. Run PS360User Script.
2. After the restore completes, download and run the “PS360 ps360user User Script.txt“ from the SharePoint SQL script library.

   NOTE: This is not the standard PS360User script that accounts for the SQL Service Broker. You may need to modify the SQL script to reflect the correct password for the PS360User account for the site you are working on.

3. Go to the Comm4 DB and delete, if they exist, the SQL Query Notification items shown below:

4. Run the SQL Service Broker Script.

Upgrade Process

IMPORTANT

If you are upgrading from V 1.x or 2.0.x to version 3.0 or higher, you must first upgrade the DB to version 2.5.

If the version of PowerScribe does not have the Client Admin icon, manually delete the folders.

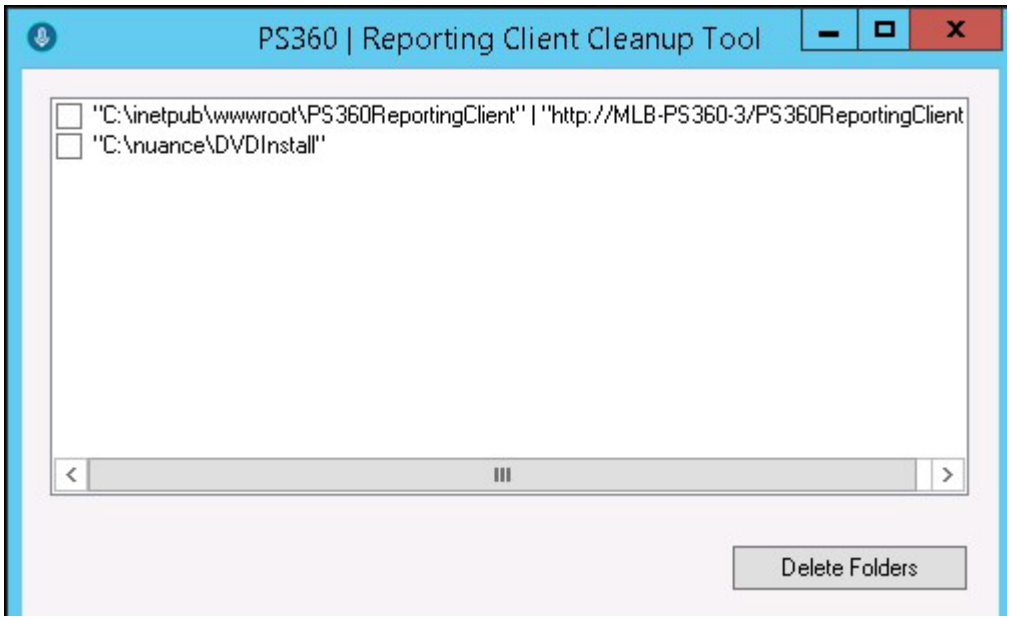
Software Download

1. Create a folder **X:\Software\360_Install\<Version to Upgrade>**.
2. Download the PowerScribe 360 Version software you are upgrading to and place it in the X:\Software\360_Install**<Version to Upgrade>** folder.
3. Right-click each step from the PowerScribe_360_Install Folder and choose **Extract All** to extract each step to the **X:\Software\360_Install\<Version to Upgrade>** folder.

Client Admin Cleanup

1. Double-click the **Cleanup ClientAdmin** icon on the desktop.

   The PS360 Reporting Client Cleanup Tool dialog displays.



2. Check the boxes and click **Delete Folders**. The application closes.

3. If the version of PowerScribe 360 Reporting you are upgrading does not have the Client Admin Cleanup Tool on the desktop, you need to manually delete the folders indicated above.
4. If the Client has a separate Mobile Server or separate Reporting Services server, you will need to repeat this process on those servers.

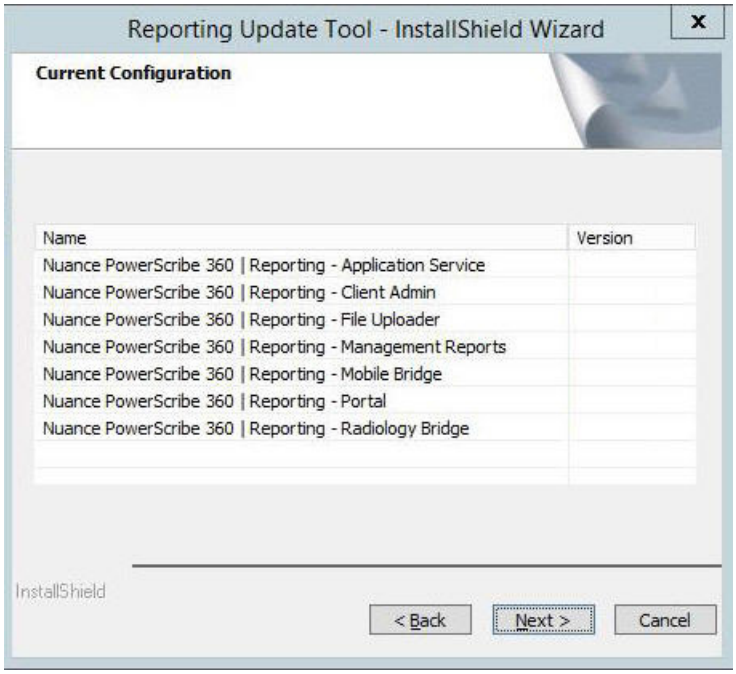
Run Upgrade Tool

Be sure you are using the latest Upgrade Tool.
Use the Upgrade Tool version 2.0.4.0 for PowerScribe 360 Reporting versions up to 3.5.x, and version 4.0.0.14 for PowerScribe 360 Reporting 4.x versions.

1. Right-click the Upgrade Tool exe, and choose **Run as Administrator**.

   The Report Update Tool Welcome dialog displays.

2. Click **Next**. The Installed components and versions display on the Current Configuration dialog.



3. Click **Next**.

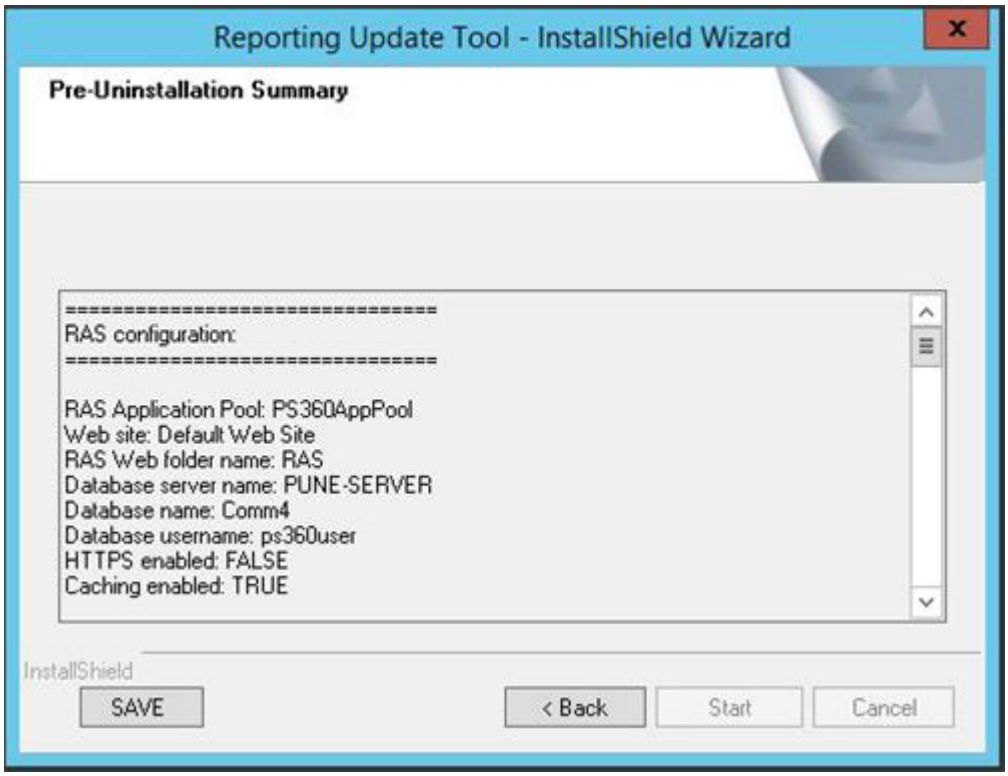
   The dialog boxes for each installed component are displayed along with the configuration information. Do not make changes, this is only for review.

4. The Application Service Dialog displays; click **Next**.
5. The Portal Configuration Dialog displays; click **Next**.
6. The Radiology Bridge Configuration dialog displays; click **Next**.

7. The Mobile Bridge Configuration dialog displays; click **Next**.
8. The File Uploader Configuration dialog displays; click **Next**.
9. Reporting Service Configuration dialog box displays; click **Next**.

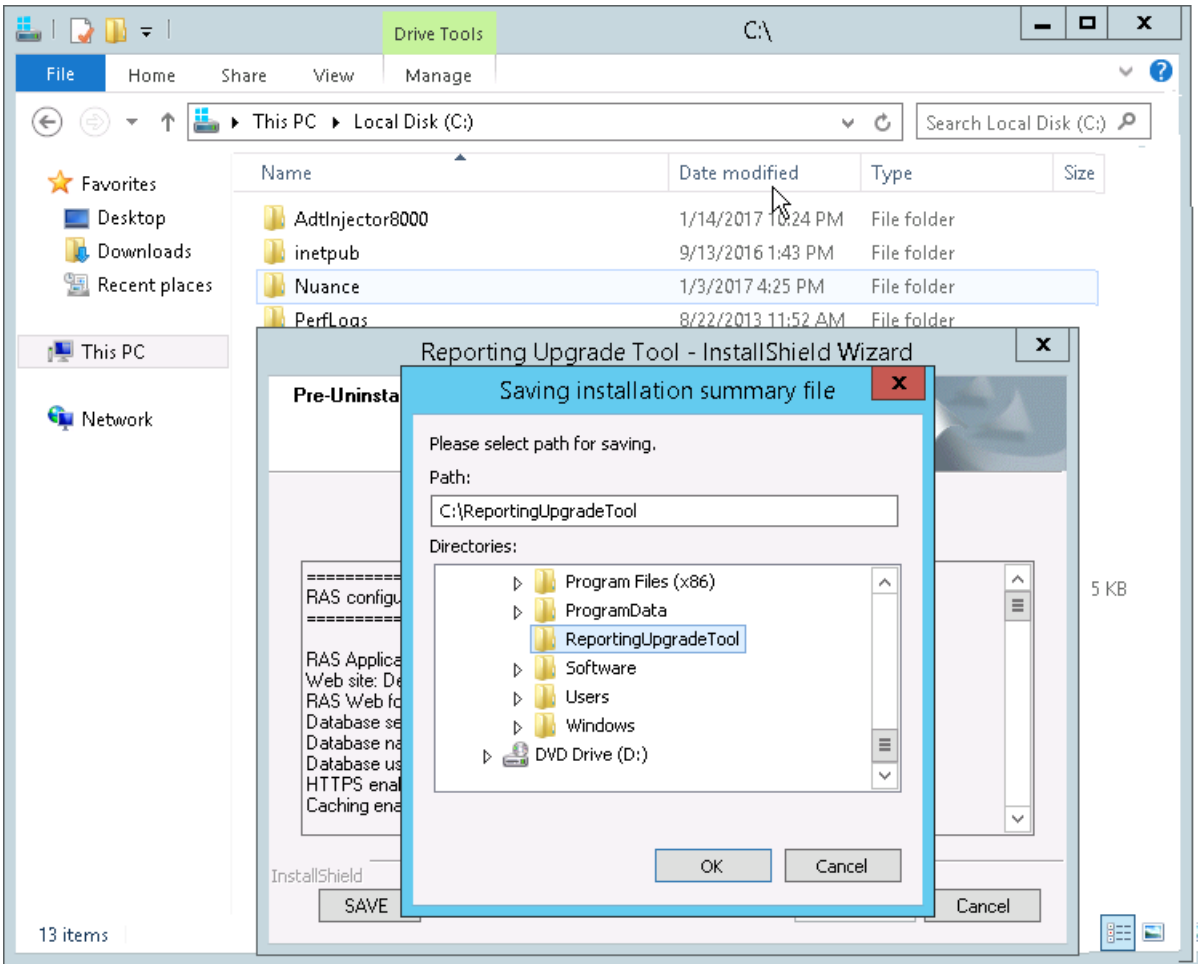
   The Check Reporting Service connection message displays.

10. Client Administration Configuration dialog box displays; click **Next**.
11. Once, all the Configuration dialog boxes for each component are done, the utility displays a dialog providing a Summary of the configuration information of all the present components.

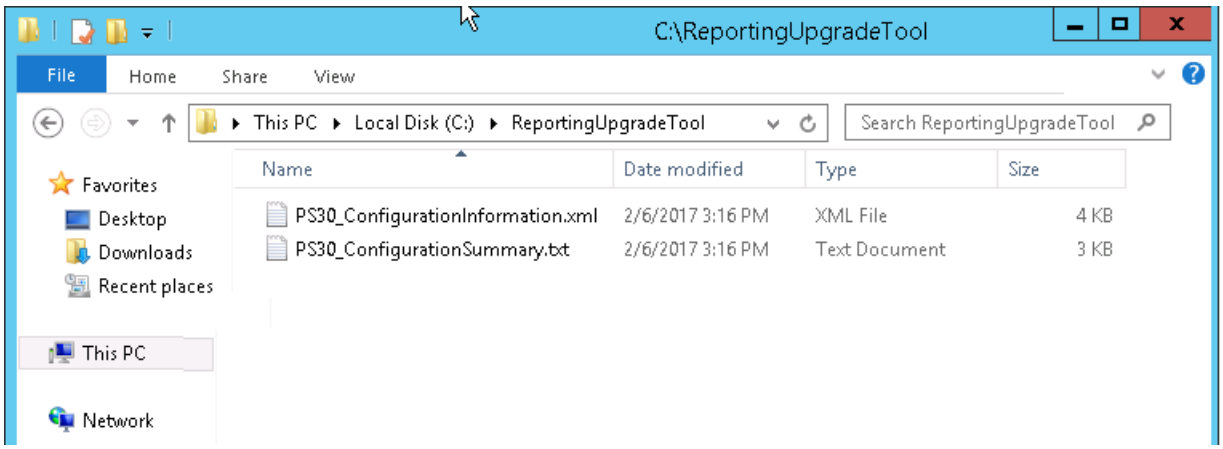


12. Click **SAVE**. This must be done to create the config file for the upgrade.
13. Save file to location where you can easily access it.

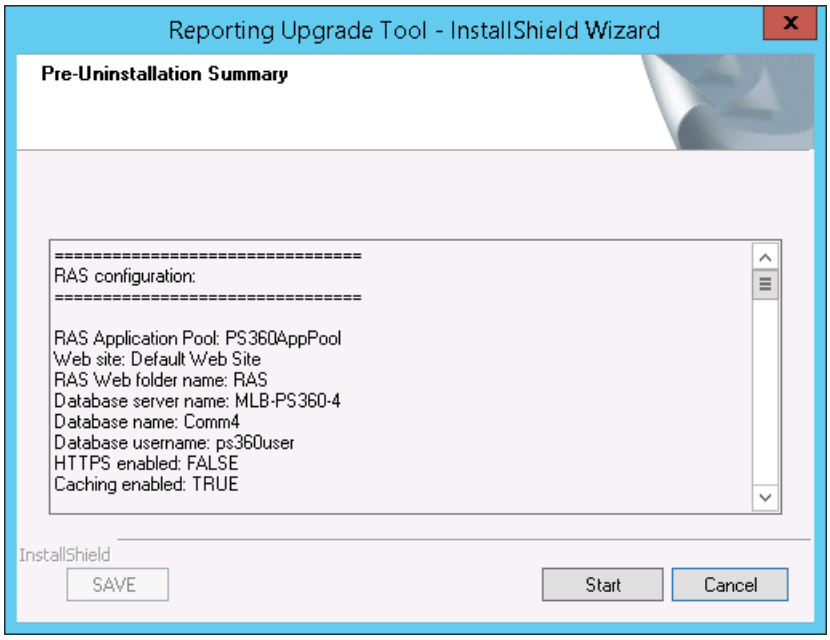
The Saving Installation summary file dialog displays.



14. Click **OK**. This saves the configuration information to the default desired location in two formats.

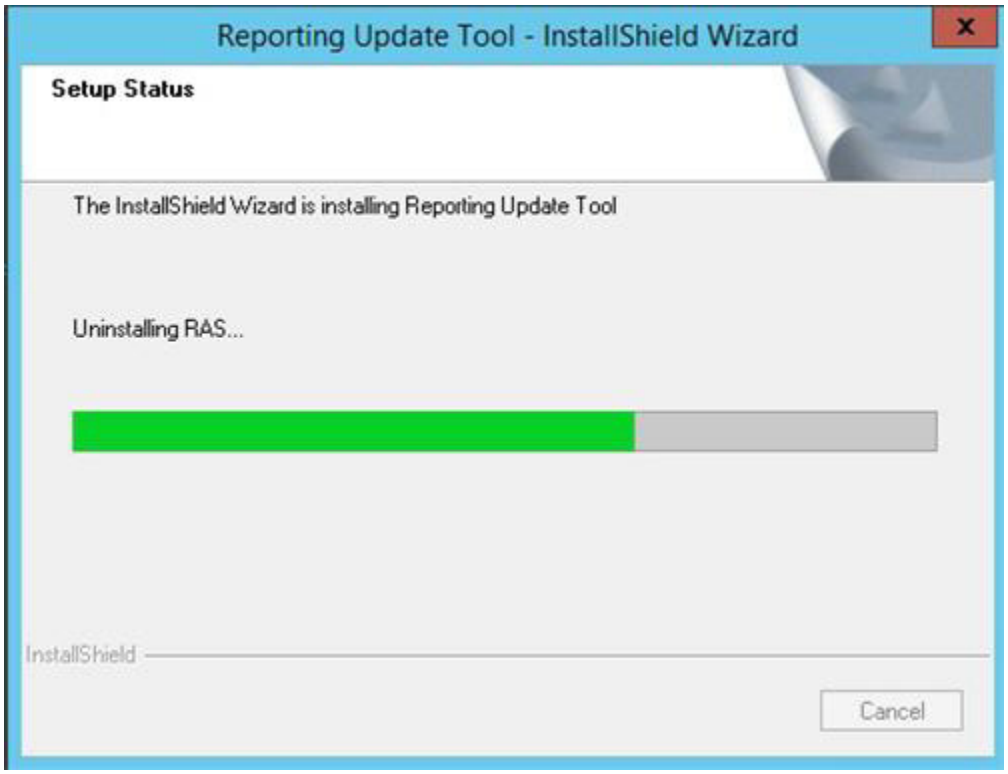


The Pre-Uninstallation Summary dialog now displays the SAVE button disabled, and the Start button enabled.

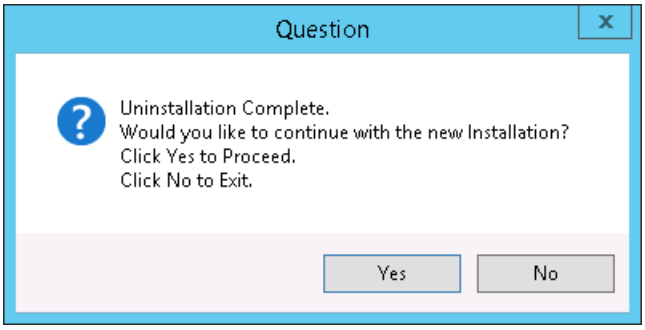


15. Click **Start**.

    The Setup Status dialog displays the uninstall process.

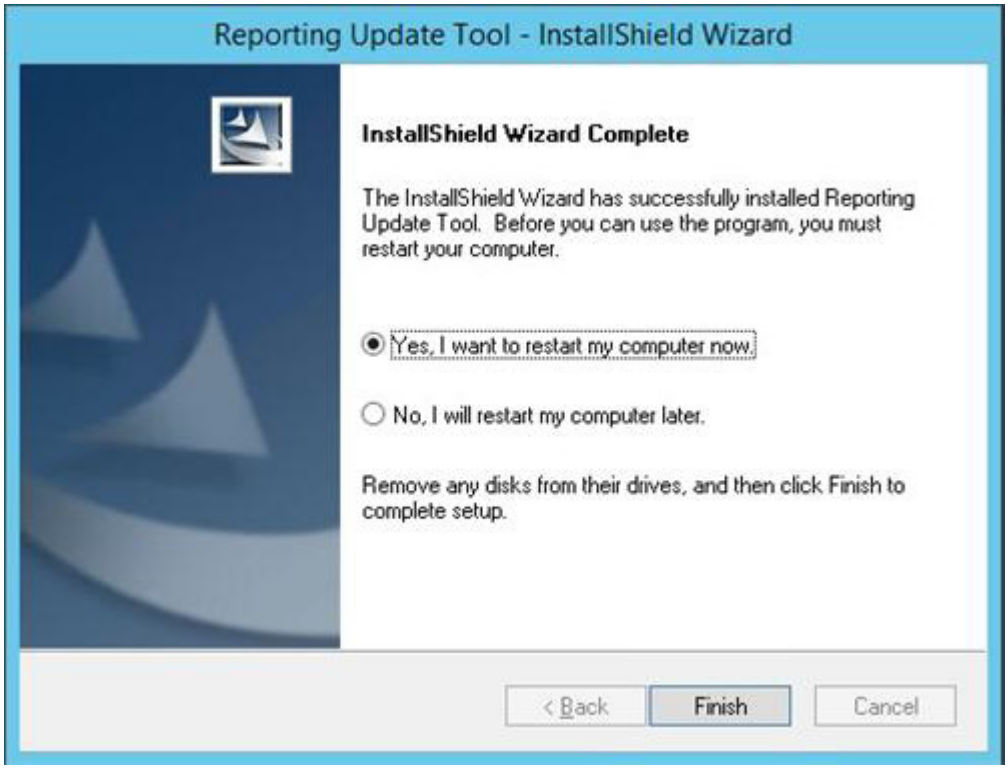


Once, all the components are uninstalled, a popup questions you if you want to continue the installation



16. Make sure you click **No**.

    The InstallShield Wizard Complete dialog displays.



17. Click **Finish** to reboot server.

IMPORTANT

A reboot is required at this point in the process.

Run Database Upgrade

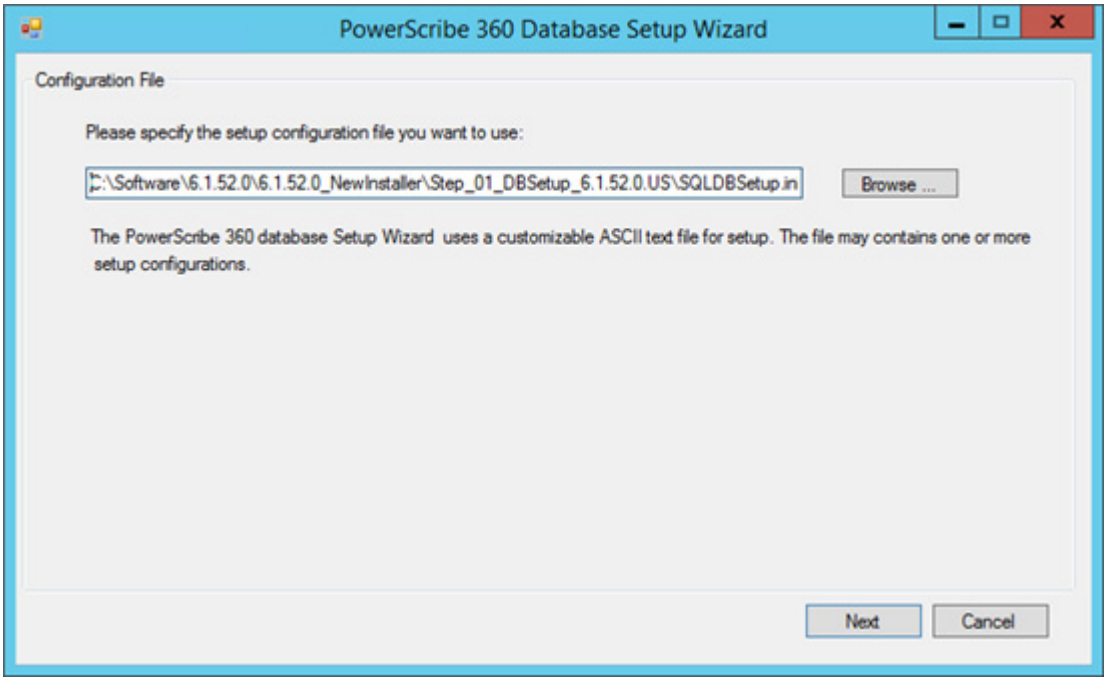
NOTE

For a cluster configuration, update the database only once on the Virtual SQL Server Instance.

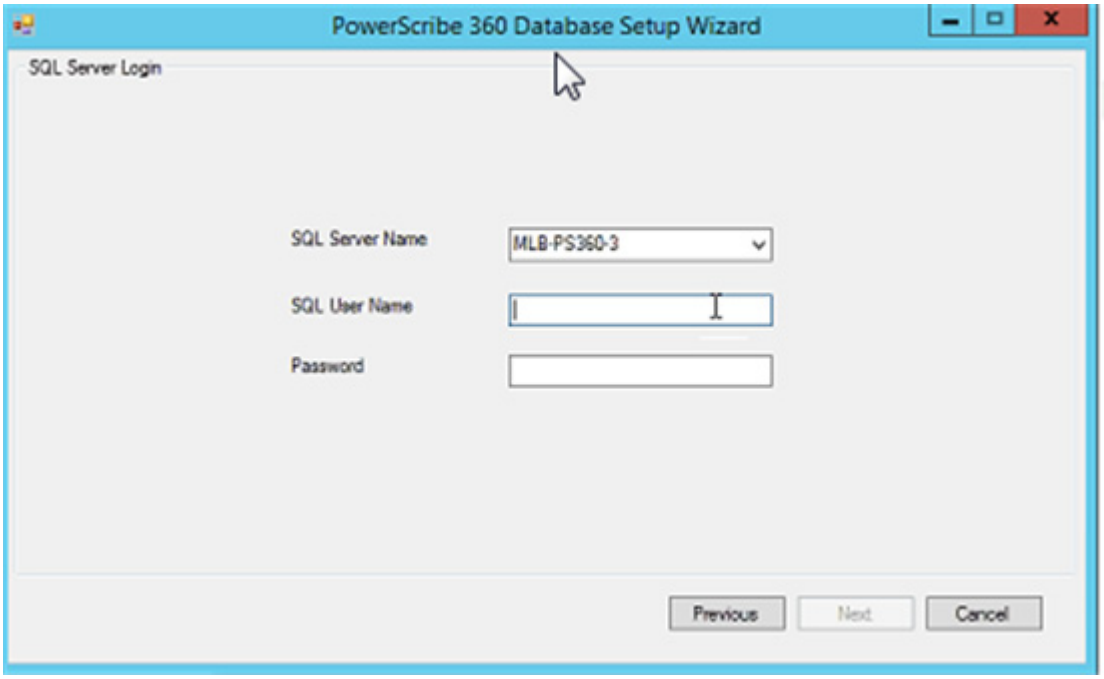
1. In the **X:\Software\360_Install\<*Version*>\Step_01_DBSetup_*X.x.xx.x*** folder, double-click **DBsetup.exe**.

2. Click **Run**.

   The Configuration File dialog displays.



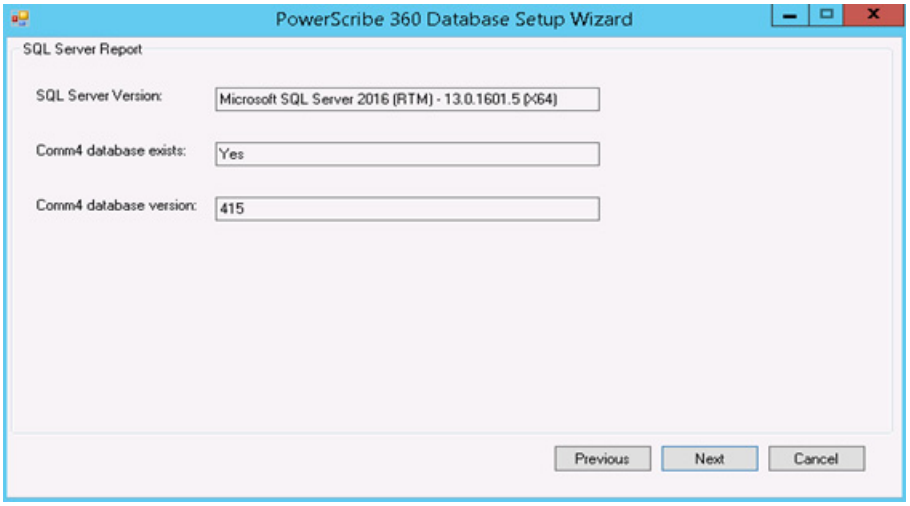
3. The SQL Server Login dialog displays; click **Next**.



4. Enter the Server Name.

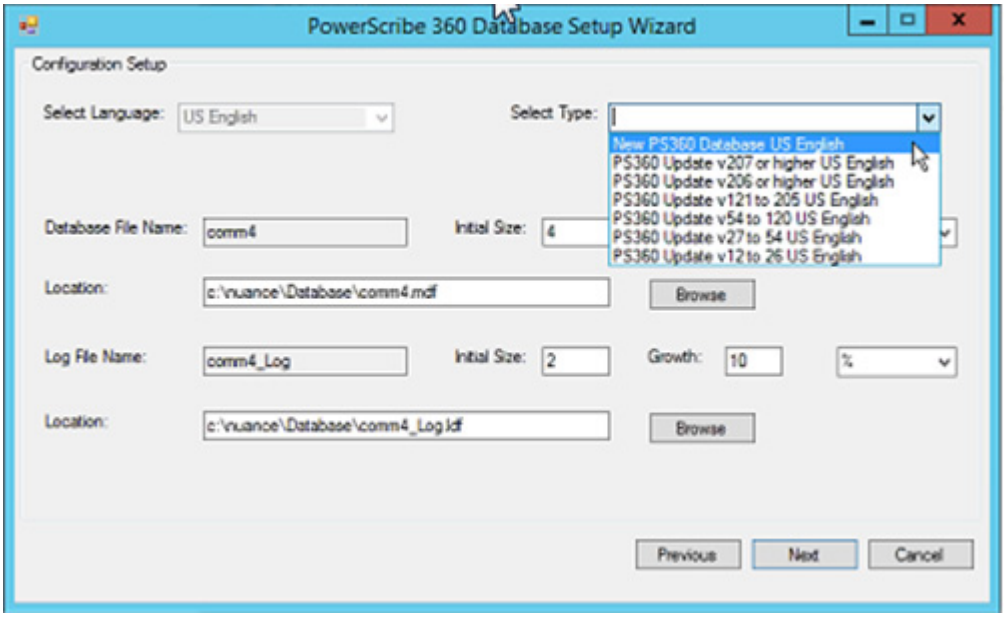
NOTE *If the server is a cluster, use the SQLClusterName.*

5. Enter the SQL User Name **sa**.
6. Enter the Password.
7. Click **Next**.



8. Take note of the Comm4 database version.
9. Click **Next**.

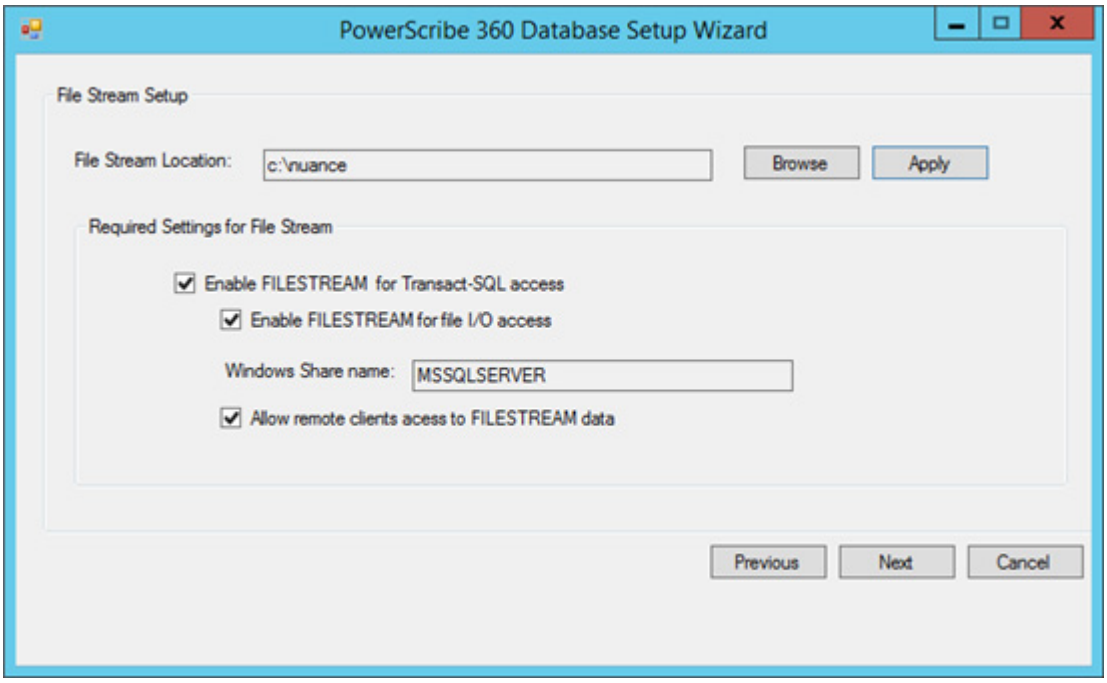
The Configuration Setup dialog displays.



10. From Select Type, select the proper upgrade selection. **Do not** select New PS360Database US English.
11. Click **Next**.

NOTE

For V3.5 and above, the File Stream Setup dialog displays.

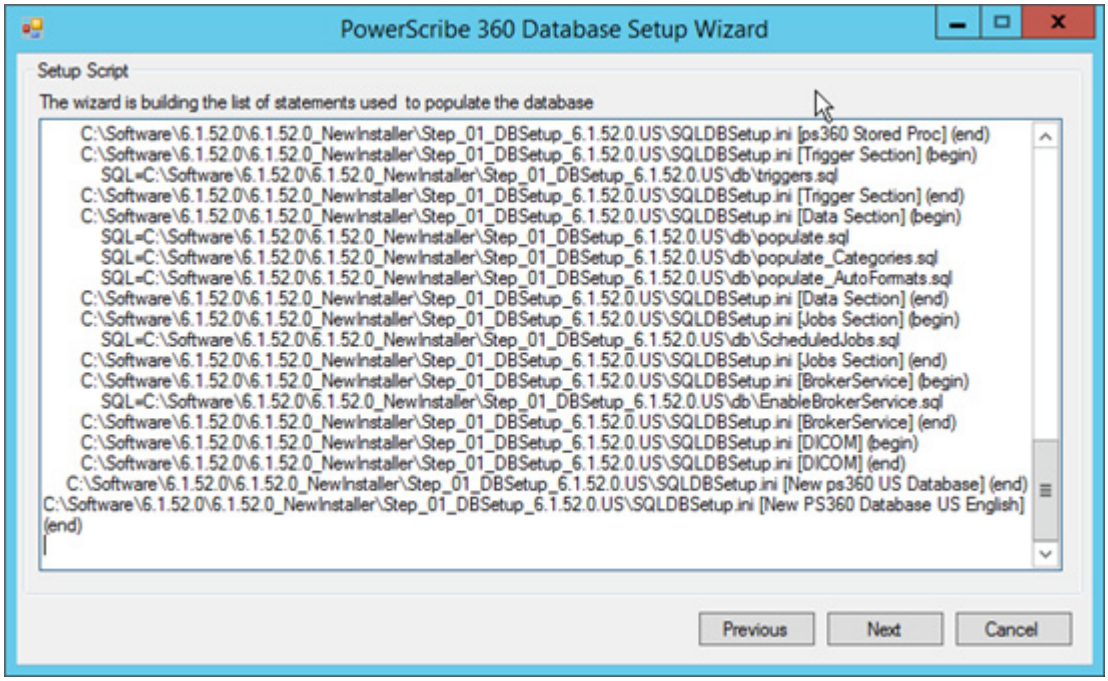


12. Change the File Stream Location drive to X:\Nunace\FileStream.

In order to activate the boxes below, you need to update the location directory.

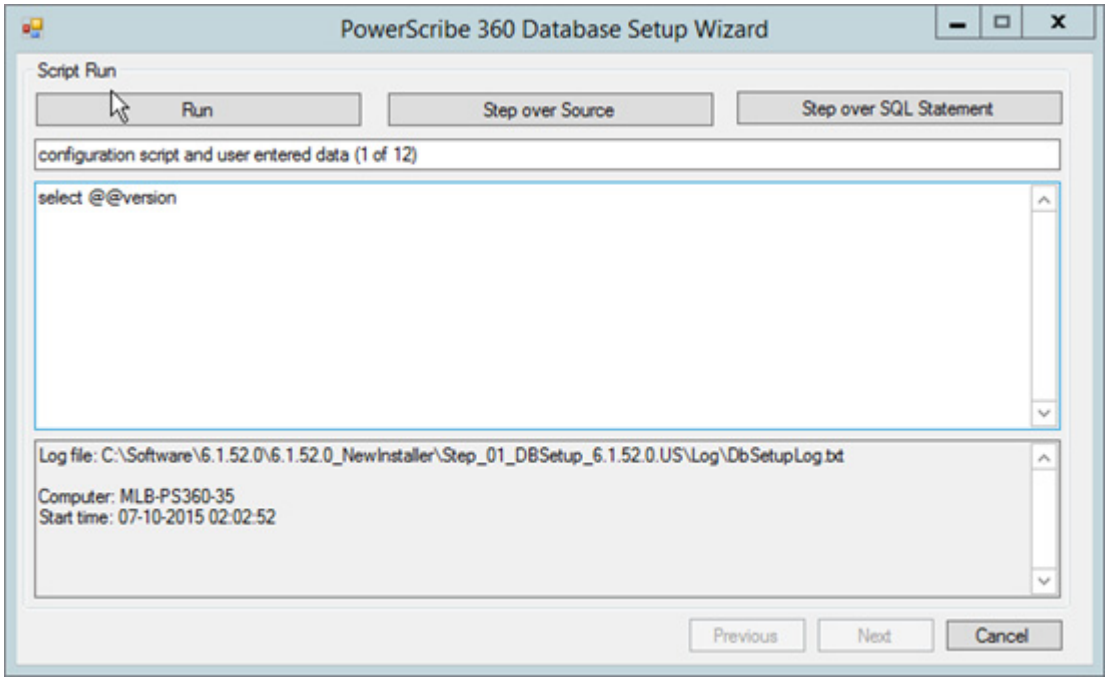
13. Click **Apply**, and then click **Next**.

    The Setup Script dialog displays and the wizard builds the list of statements used to populate the database.



14. Click **Next**.

The Script Run dialog displays.



15. Click **Run**.

    Wait for the installation to finish.

16. Click **OK** on the Success dialog.
17. Click **Exit**. The new upgrade of the database is complete.

    a. Right-click the Database Properties and select **Options**.

    b. From the Recovery model list, select **Full**.

18. Click **OK**.

Update Database Statistics (V 3.5.1 and below ONLY)

1. Download the PS360 Update All Statistics.txt file from Confluence.
2. Save the file with the sql extension.
3. Open the script in SQL Management Tool.
4. Run the script against the COMM4 Database.

Set DB Recovery Level

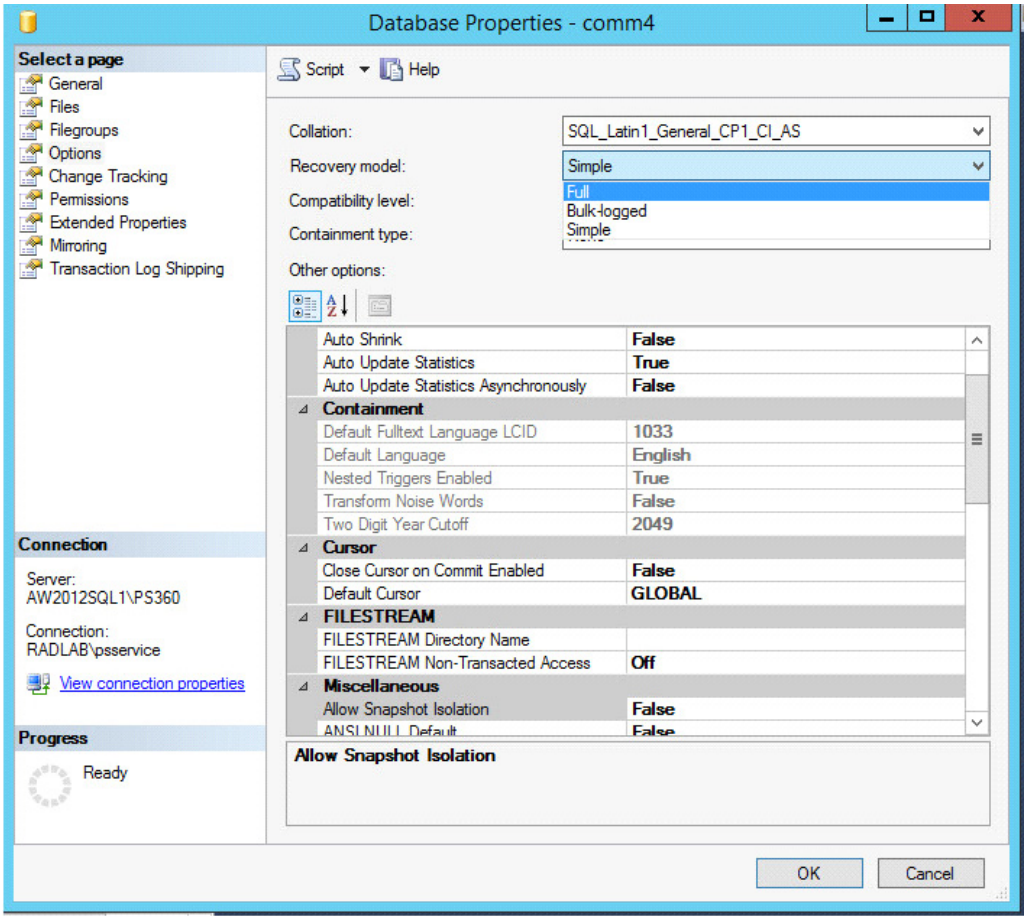
Next, use the following steps to prep the database to be added back to the Availability Group.

When the database upgrade is finished, the Comm4 Database will need to be changed from Simple Recovery Model to Full.

1. Right-click the **Comm4** Database, and select **Properties**.

The Database Properties dialog displays.

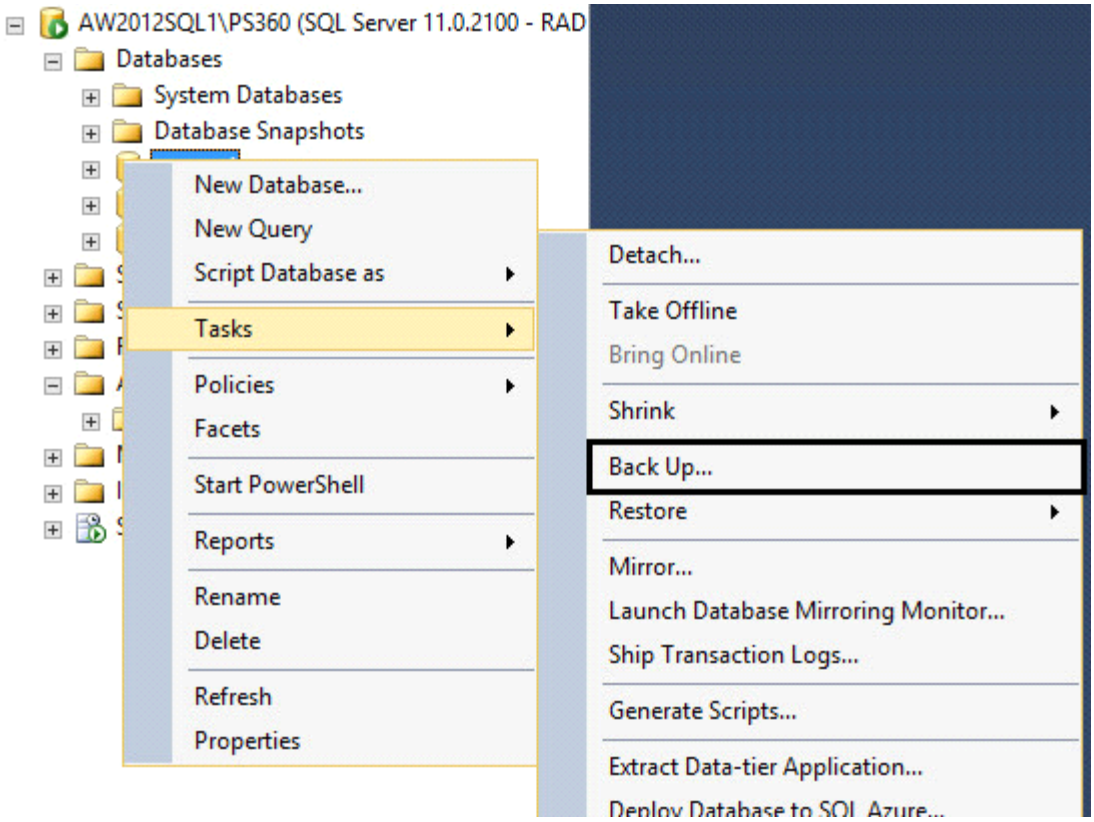
2. Select **Options**.
3. From the Recovery Model list, select **Full**.



4. Click **OK**.

Backup the Comm4 Database

1. Right-click the **Comm4** database.
2. Select **Tasks**.
3. Select **Back Up**.



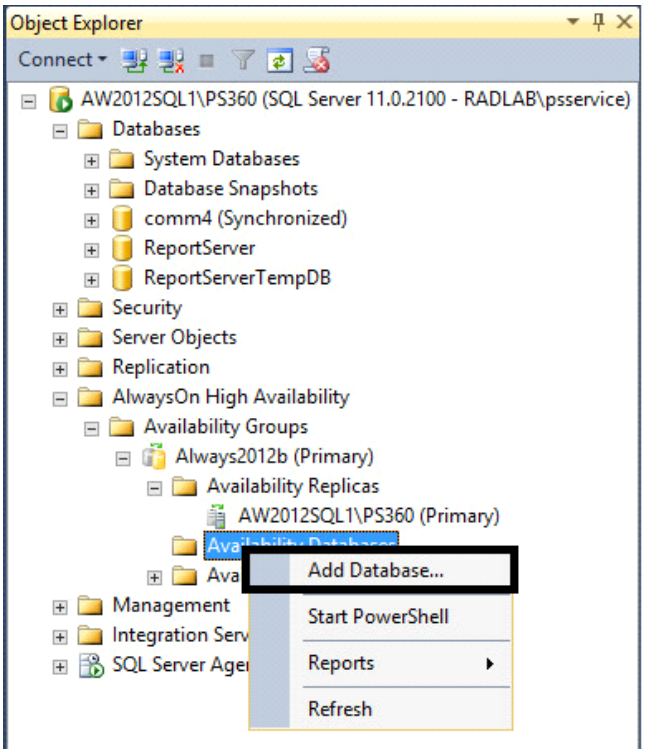
NOTE *If needed, change the backup location. Any location is fine, just be sure to set the Backed Up flag to True.*

4. Click **OK**.
5. When the backup job is finished, click **OK**.

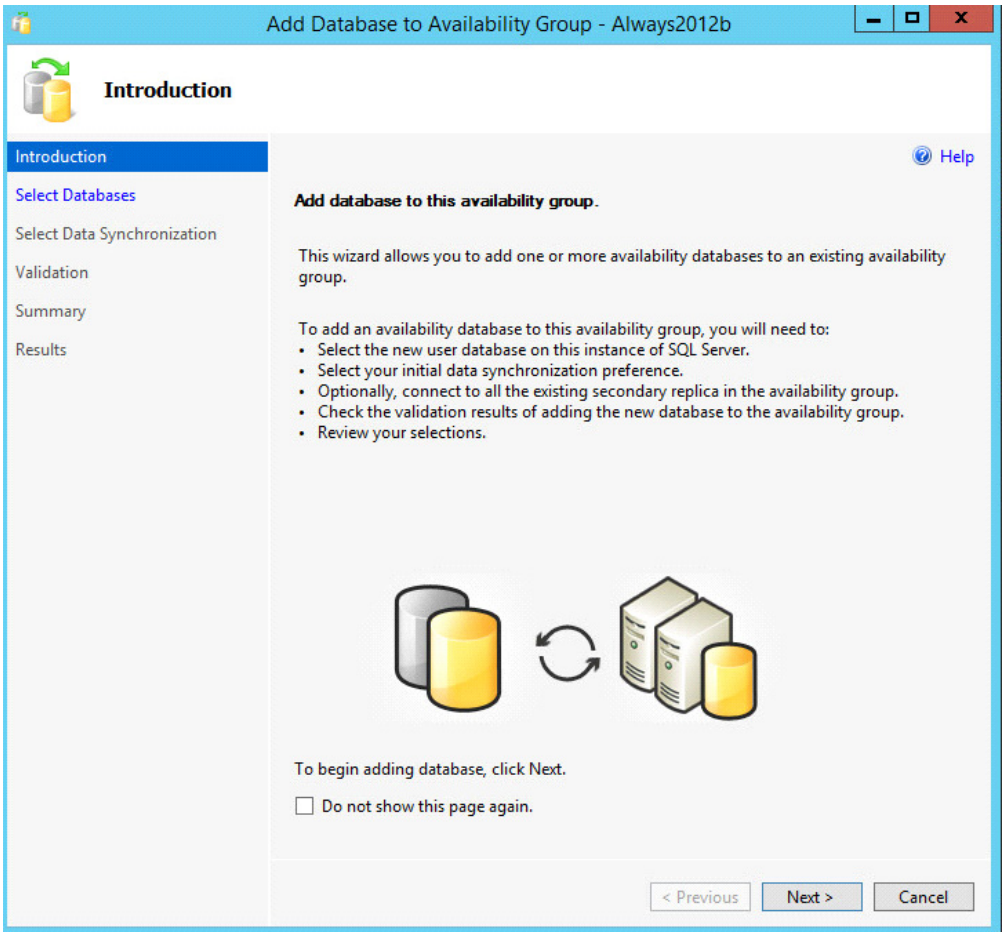
Add Comm4 Database Back into Availability Group (For systems with Hot Spare at v3.5.1 and above)

1. Expand **AlwaysOn High Availability**.
2. Expand **Availability Databases**.

3. Right-click **Availability Databases** and select **Add Database**.

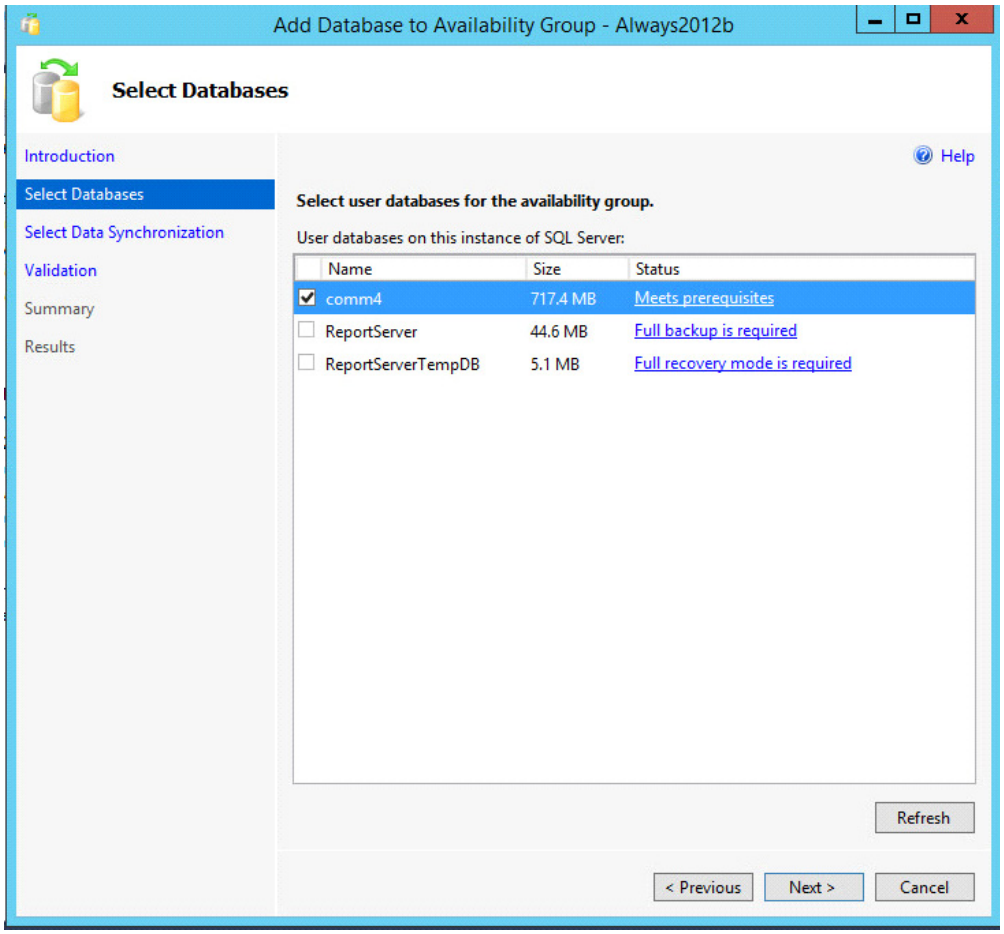


The Add Database to Availability Group Introduction dialog displays.



4. On the Add Database to Availability Group dialog, click **Next**.

The Add Database to Availability Group Select Databases dialog displays.



5. Check the **Comm4** database.

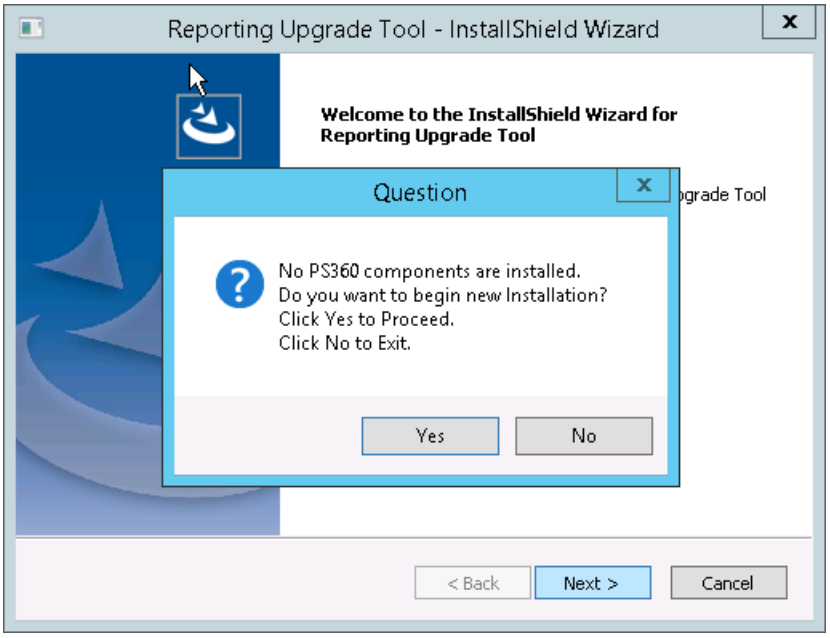
NOTE *If Comm4 is grayed out, re-run prerequisites steps for Full Backup or Full recovery mode.*

6. Click **Next**.

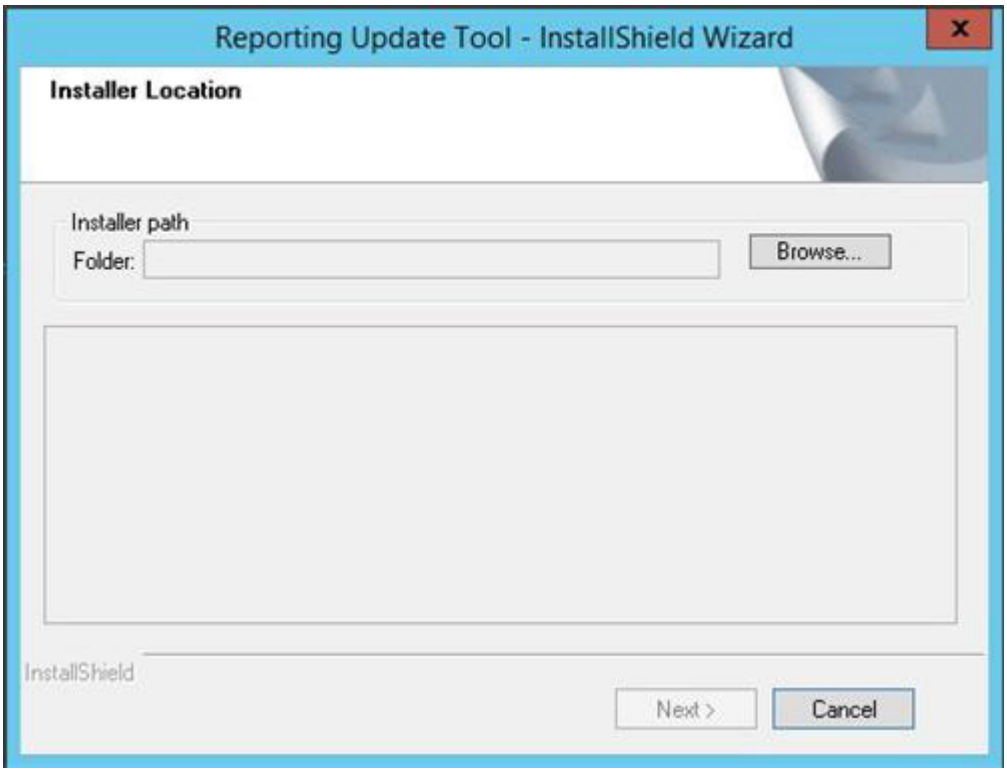
Completing the Upgrade - Installing Your New Version

1. Right-click the Reporting Upgrade Tool exe, and select **Run As Administrator**.
2. Click **Next**.

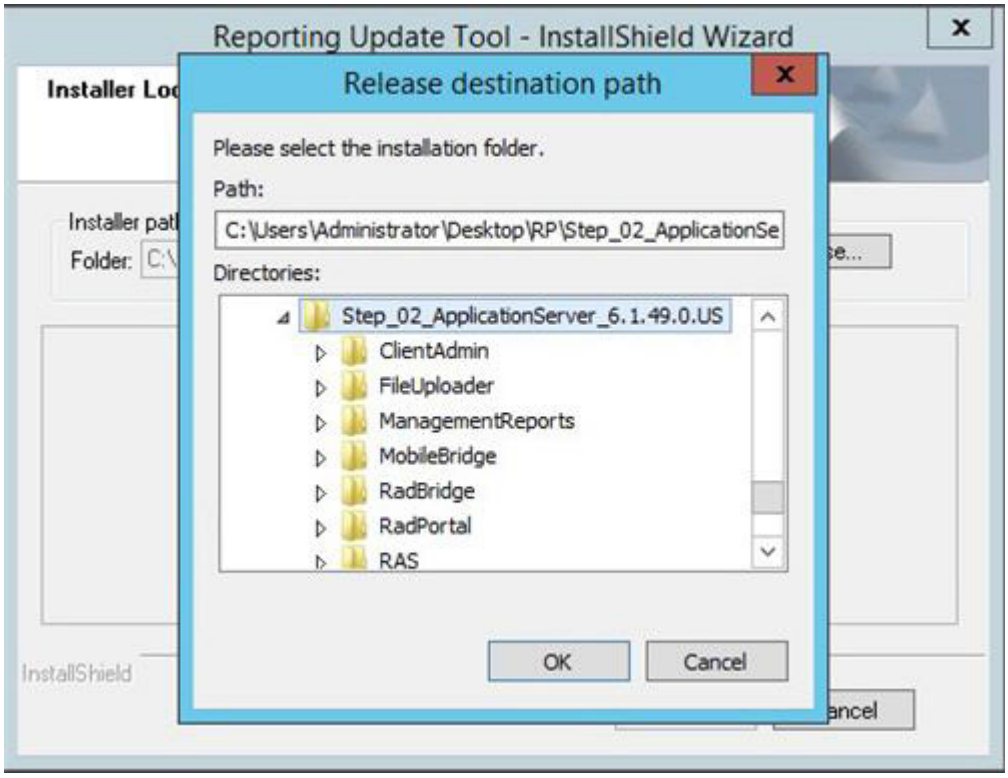
   A popup question dialog displays.



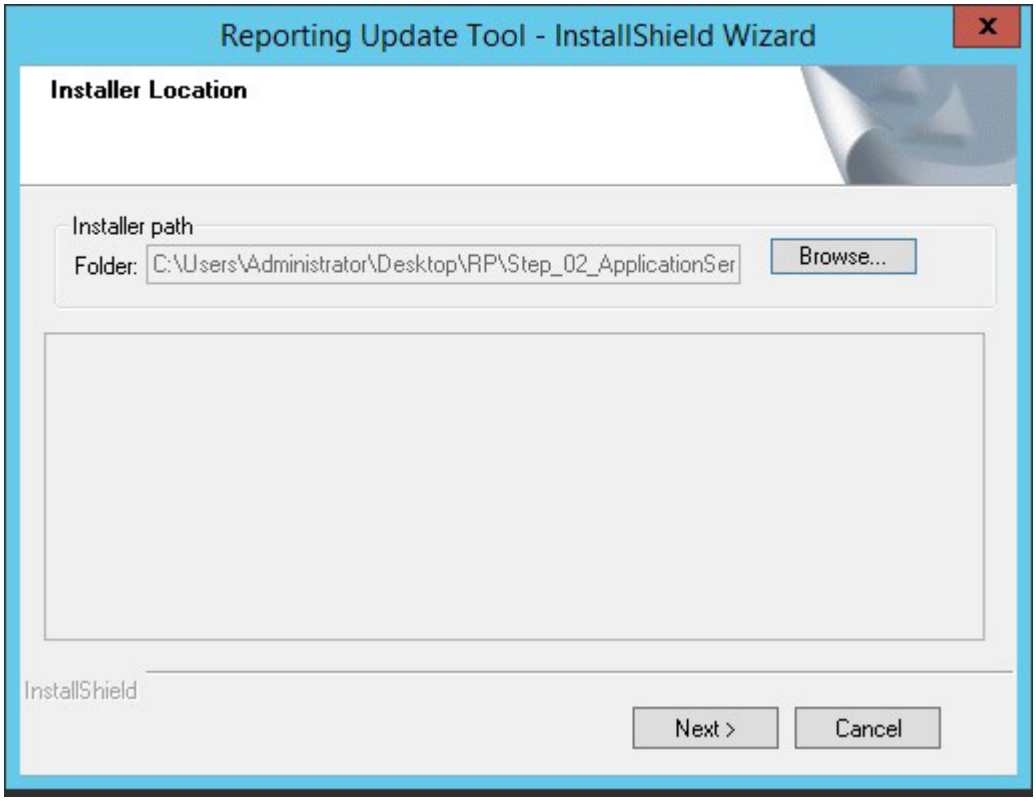
3. Click **Yes**. The Installer Location dialog displays.



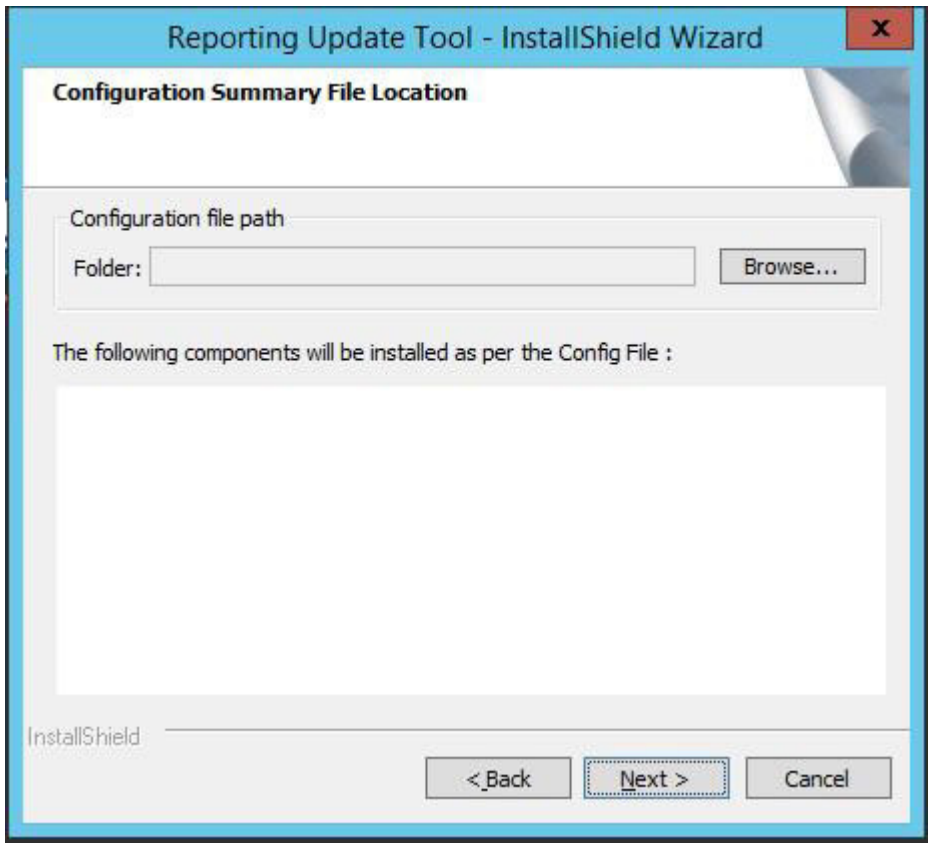
4. Click **Browse** and navigate to the location of the extracted Step 2 folder for the new PowerScribe 360 version.



5. Click **OK**. The Reporting Update Tool utility will validate the path to check if the new Installer. The **Next** button will not be enabled until a path is provided.
6. Click **Next**.



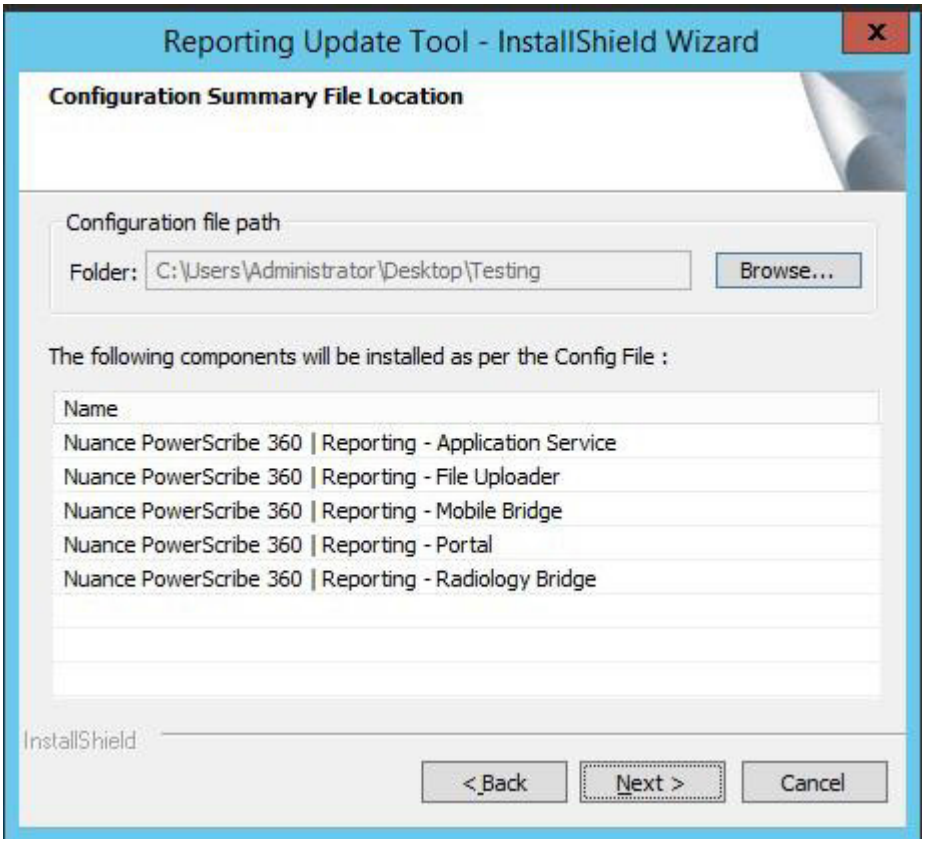
The Configuration Summary File Location dialog displays.



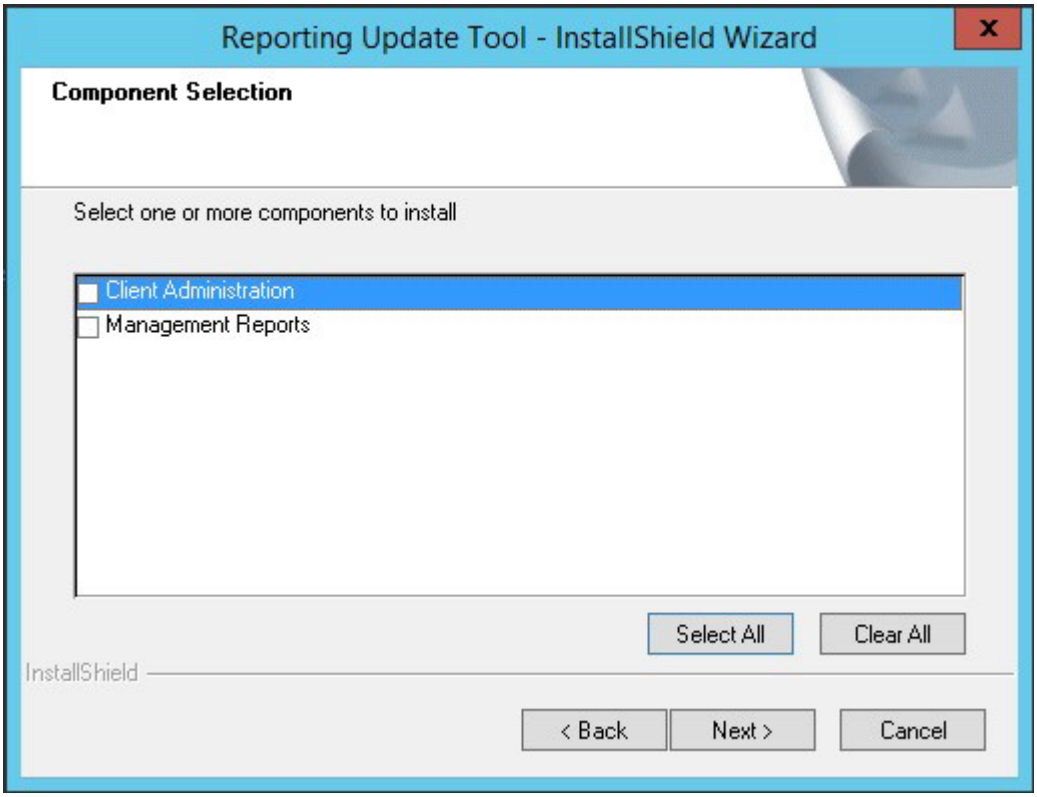
7. Click **Browse** and navigate to the location of the PS30_ConfigurationInformation.xml file you saved earlier. The **Next** button will not be enabled until a path to PS360_ConfigurationInformation.xml is provided.

8. Click **Next**.

   The Configuration Summary File Location dialog lists the components included in the new version along with those which were previously not installed on that server.

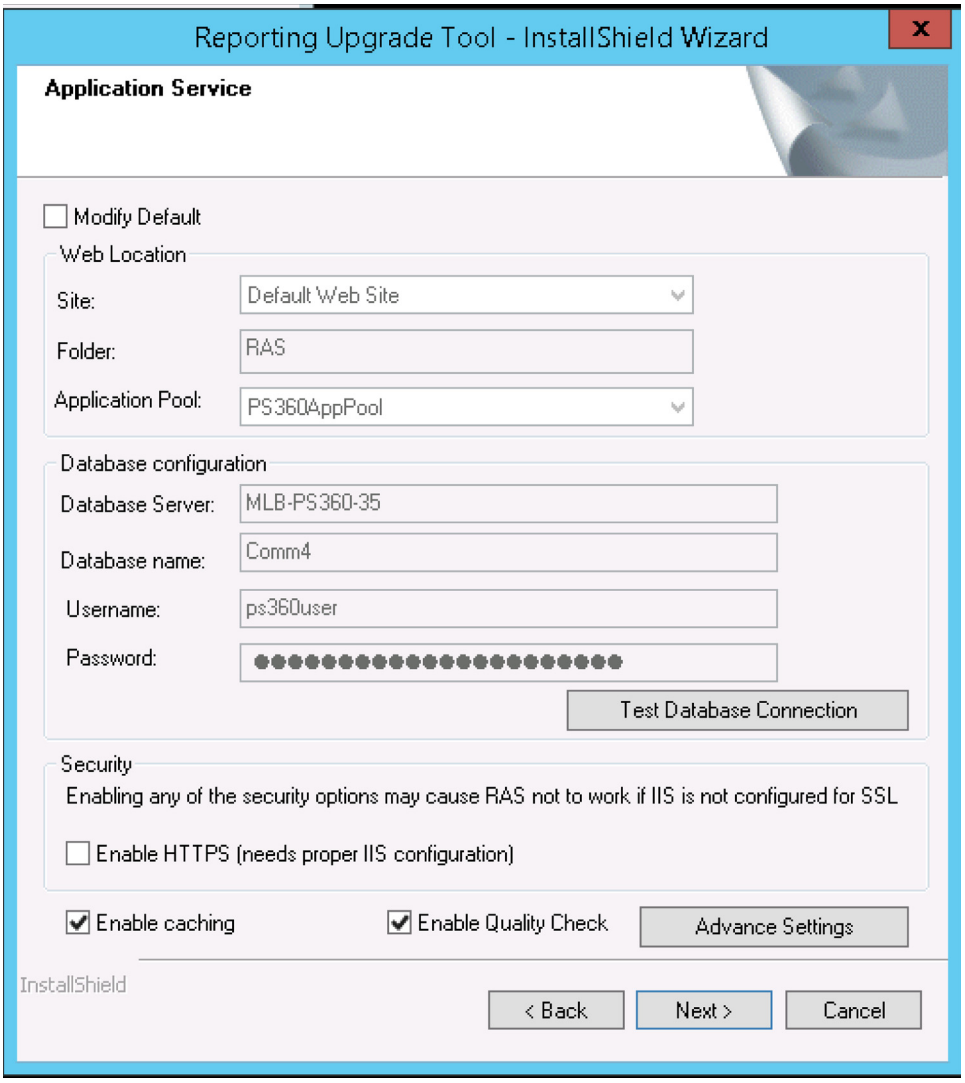


Optional Screen: If there are components that were not previously installed the Component Selection dialog displays.

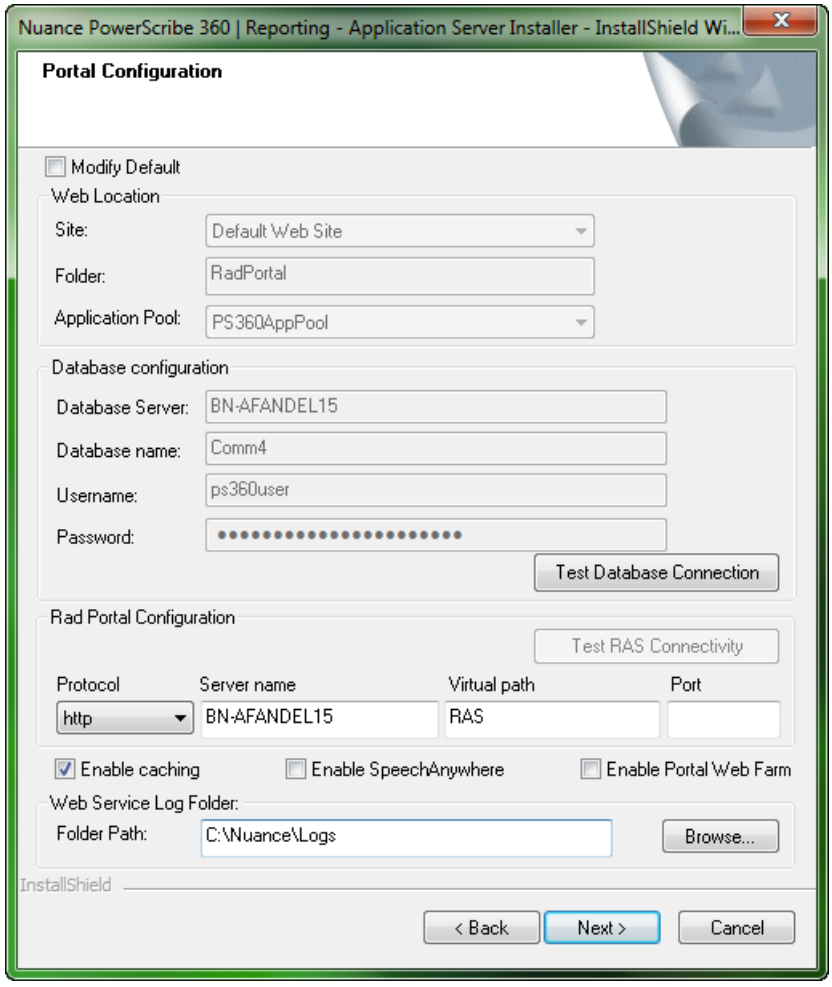


9. Check any component that was not previously installed, if you want them to install now, and then click **Next**.
10. Selected components will be installed with their default values. Dialogs for each installed component are displayed along with configuration information which is extracted from the Configuration Information File. These settings should not be changed to keep the configuration exactly like the previous version. Click **Next** for each displayed dialog.

Below are two sample screen shots you see of dialogs that will display.



11. When the Portal Configuration dialog displays, be sure to check the Enable caching box if it is not checked.



NOTE

*The **Web Service Log Folder field** option is available on the Portal Configuration dialog during upgrades to V4 and higher.*

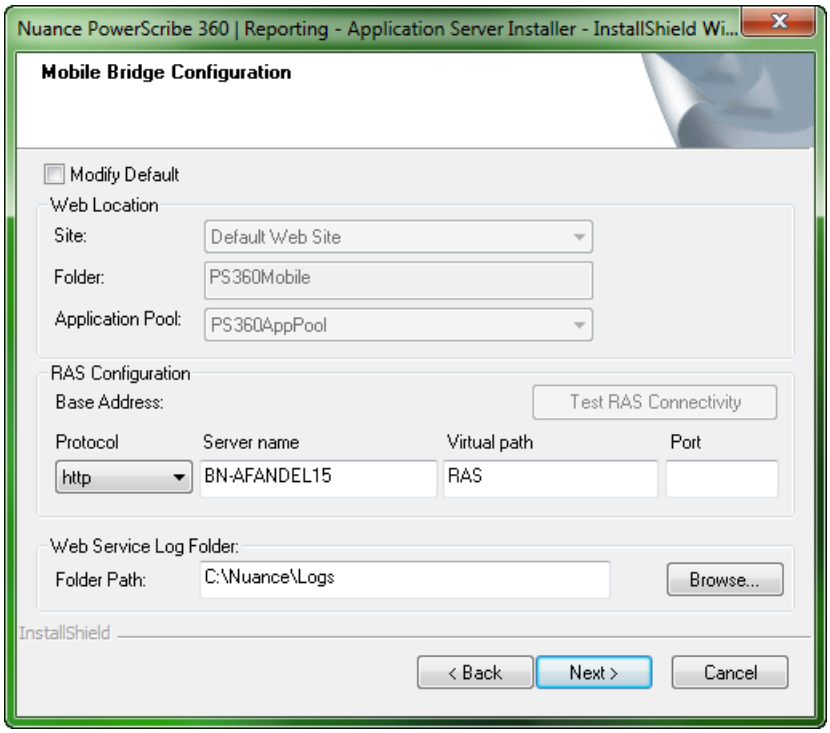
12. **OPTIONAL STEP:** If the Web Service Log Folder on a system upgrade to V4 and higher is *not* C:\Nuance\Logs, change the folder path to point to the Nuance\Logs directory.

13. When the Mobile Bridge Configuration dialog displays, be sure to check the Enable caching box if it is not checked.

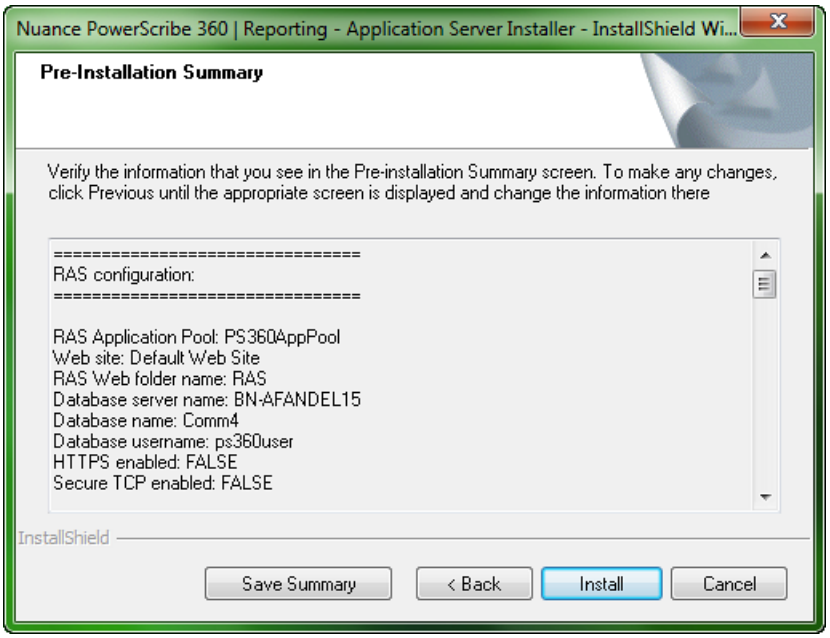
NOTE

*The **Web Service Log Folder field** option is available on the Mobile Bridge Configuration dialog during upgrades to V4 and higher.*

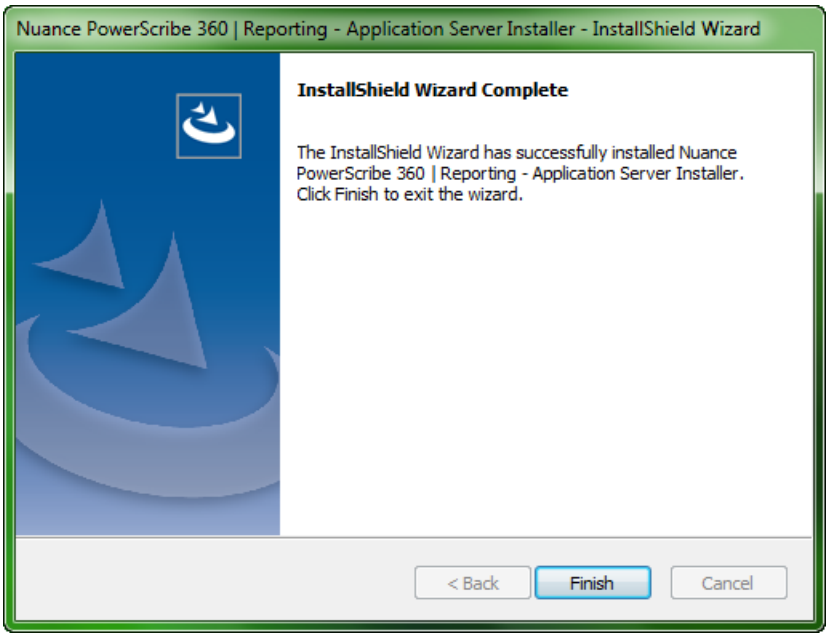
14. If the Web Service Log Folder on a system upgrade to V4 and higher is *not* C:\Nuance\Logs, change the folder path to point to the Nuance\Logs directory.



15. Once all of the install dialogs have been completed, the Pre-Installation dialog displays. Click **Install**.



16. Once all the components are installed, the InstallShield Wizard Completed dialog displays. Click **Finish**.



Client Administration Configuration Tool

IMPORTANT

For a Cluster Configuration, use the Application Cluster Virtual Name for the URL and the SQL Virtual Cluster Name for SQL connections.

If you are upgrading a DOD or a site where the server does not have access to the Internet, download and use the latest version of the PS360 Client Cab File Signer. The tool can be downloaded from the DML under PowerScribe 360 Reporting\Support Utilities\Client Cab File Signer.

The PS 360 Client Cab File Signer utility provides the means to create a PS 360 signed ClientSetup.cab file outside of using the Client Administration application on the PS 360 application server. Using this utility in conjunction with the updated Client Administration application to allow building the ClientSetup.cab file without signing, customers like the Department of Defense that do not allow access to the signing timestamp server can deploy from the Application server URL.

To disable Cab signing in the ClientAdmin Utility, edit the ClientAdmin.exe.config and set TurnOffCabSigning to True. The feature is supported in PS 360:
v3.5.1,
v3.0.1 (PS360v301ClientAdminUpdate-4-7-2016.zip),
v2.5.3 (PS360v253ClientAdminUpdate-4-7-2016.zip) and
v2.0.3 (PS360v203ClientUpdate-50713-5-31-2016.zip)

Once the ClientSetup.cab is created with the utility, use it to replace the one located in the <drive>:\inetpub\wwwroot\PS360ReportingClient\Client folder.

The tool will sign the ClientSetup.cab using sha256. This should allow the site to install MS KB 3123479.

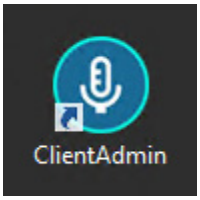
PS 360 v3.5.1 has been updated to support sha256. This tool is not required for PS 360 v3.0.2, v3.5.1 and greater.

To use this tool, you must first download and install the proper hot fix version of the Client Cab File Signer Utility.

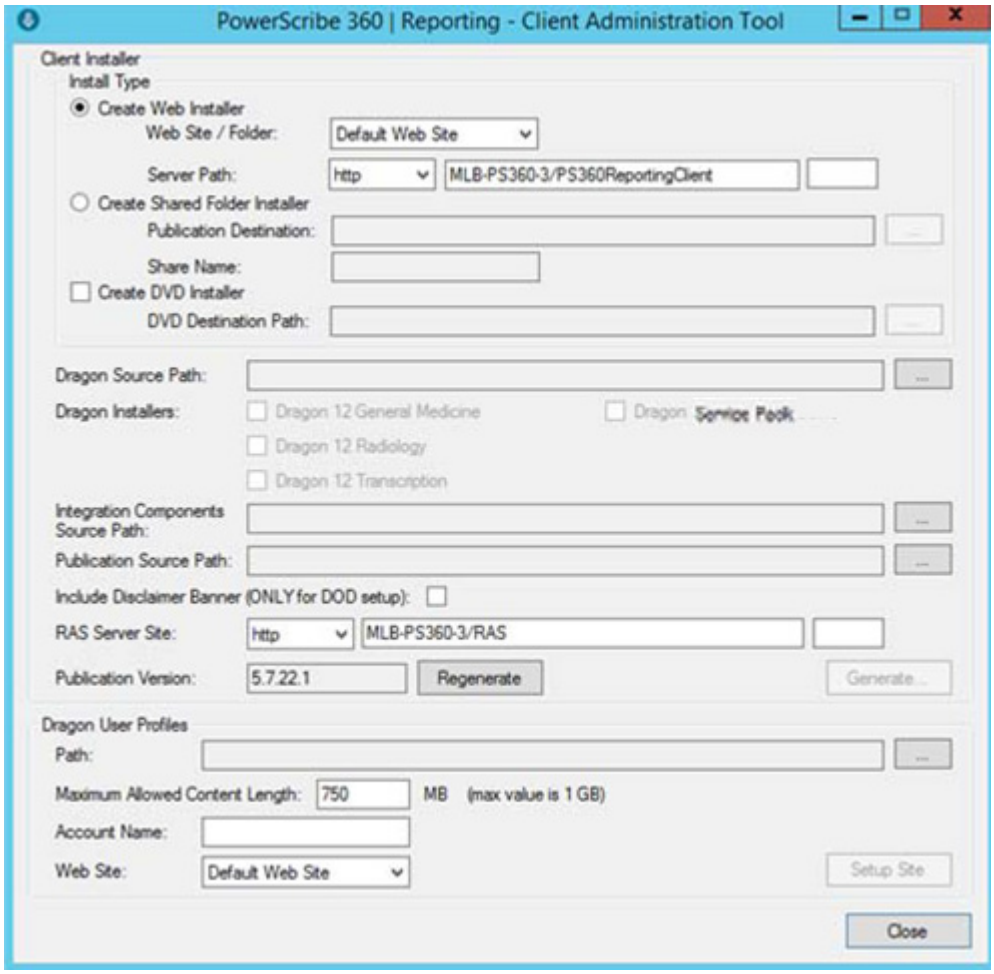
- v3.5.x
- v3.0.1
- v2.5.3
- v2.0.3

Run Client Admin Utility

1. Click the new Client Administration icon on the desktop.



The Client Administration Tool dialog displays.



2. Check the **Create Web Installer** option with Default Web Site and PS360ReportingClient for the Web Site/Folder options.

NOTE

Do not select the shared folder installer.

   a. If you are installing to a cluster, set the URL to the virtual cluster name.

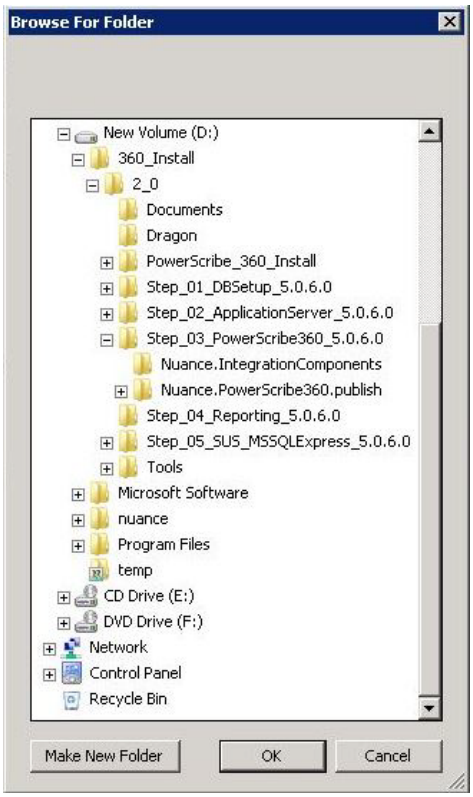
3. Check the **Create DVD Installer** box.
   a. Set the DVD Destination Path: X:\Nuance\DVD Install
4. Set the **Dragon Source Path**.

IMPORTANT

You should be installing the latest version of the Dragon software for your new version.

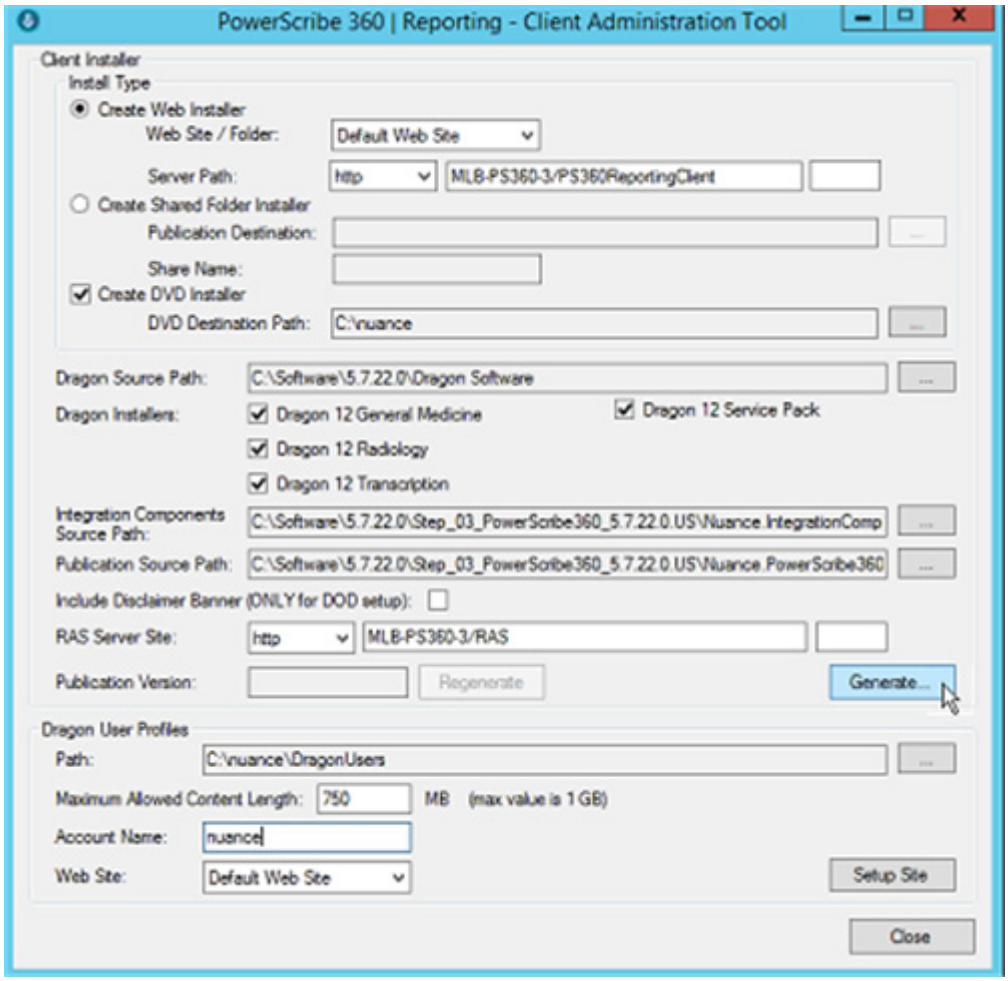
   a. To find this source path, use the ellipses button for this entry and browse to the location where you extracted the Dragon disk/image files.

   The application will detect **Dragon Installers** available and check them appropriately.
5. Enter the **Integration Components Source Path** and the **Publication Source Path**.
   a. To find these source paths, use the ellipses buttons for each entry and browse to the location where you extracted the Step_03_PowerScribe360_X.x.xx.x files. These will be in the path under that step.



6. Click **OK**.

The Client Administration Tool dialog displays.

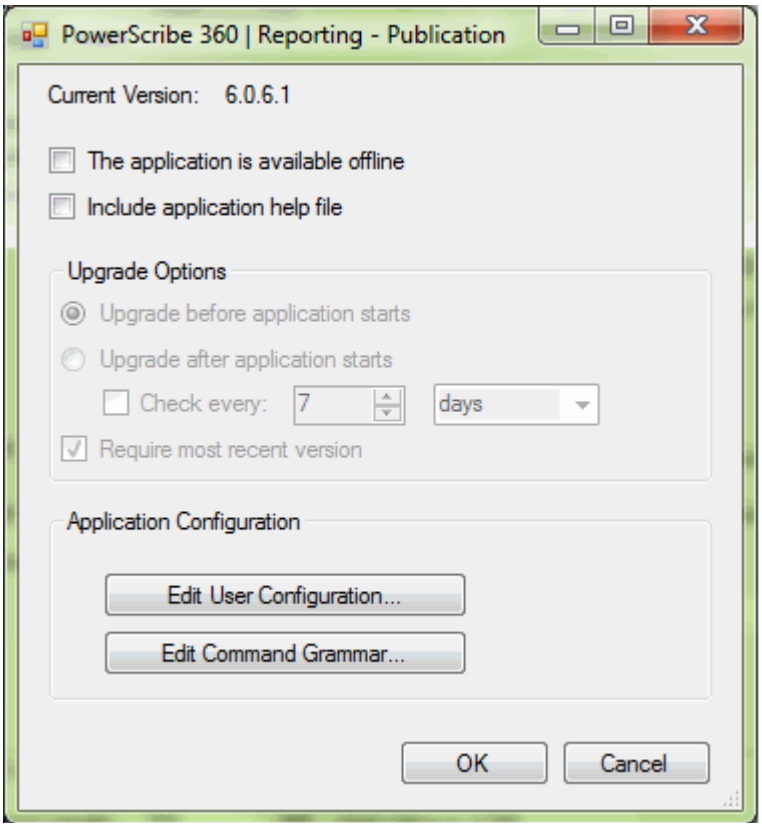


NOTE

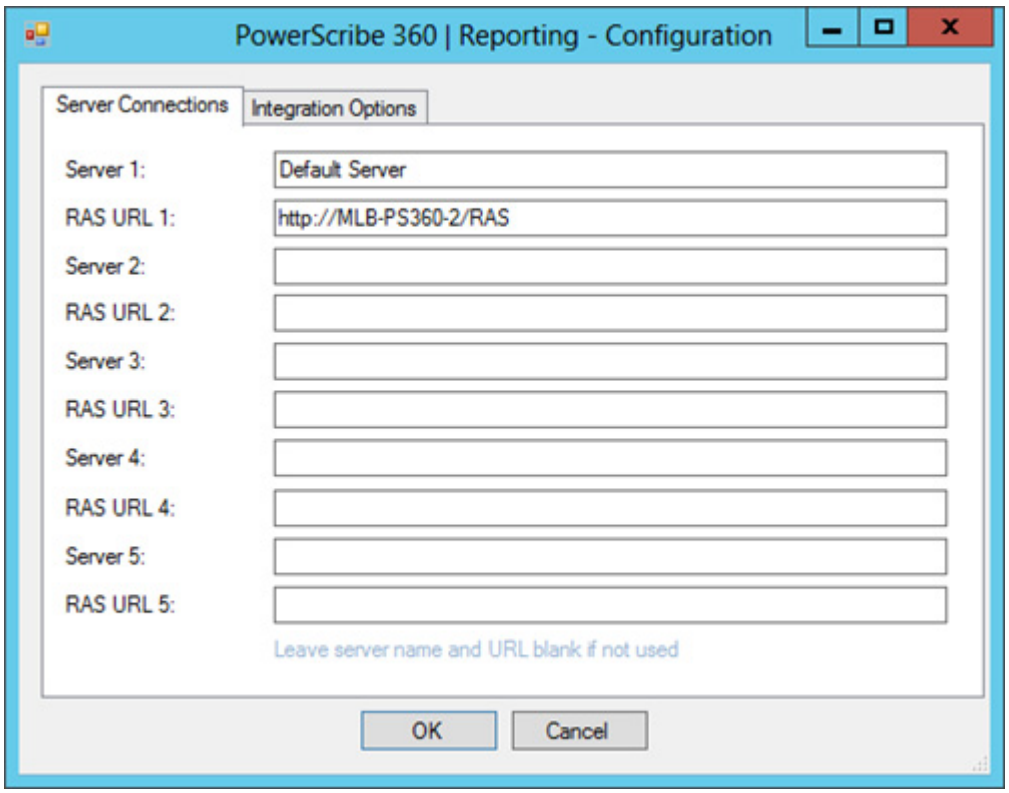
If this is a DOD facility, you should enable and add a site security message by checking the box.

7. Verify the RAS server site URL setting. If installing to a cluster, you must change the server name to the virtual cluster name.
8. Click **Generate**.

The Publication dialog displays.



9. Click **Edit User Configuration**.



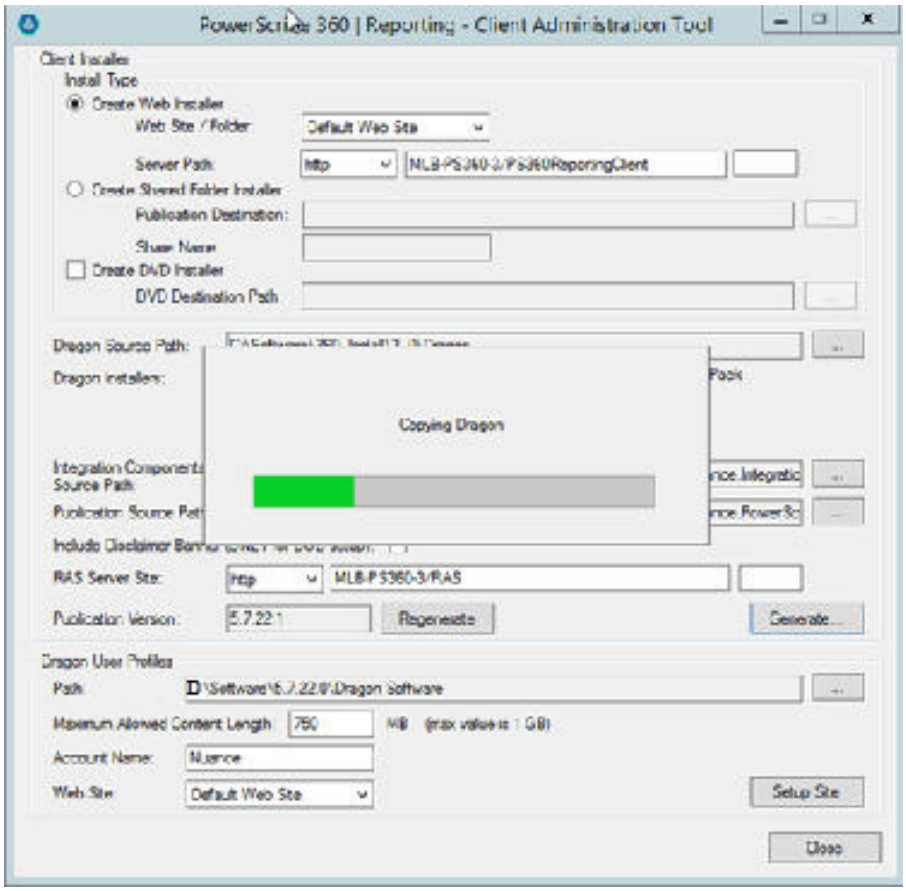
Confirm that the **actual server name** is entered in place of localhost.

10. Click on the **Integration Options** tab.
11. Enter or verify that the port is 9090 and click **OK**.

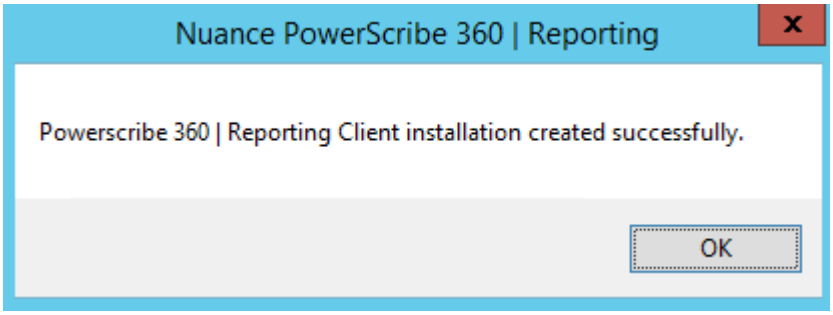
    The Publication dialog displays.

12. Click **OK** to generate the publication. Wait while the publication is generated. You are returned to the Client Administration Tool dialog.

    After the generation of the publication, you will note that the Publication Version now appears.



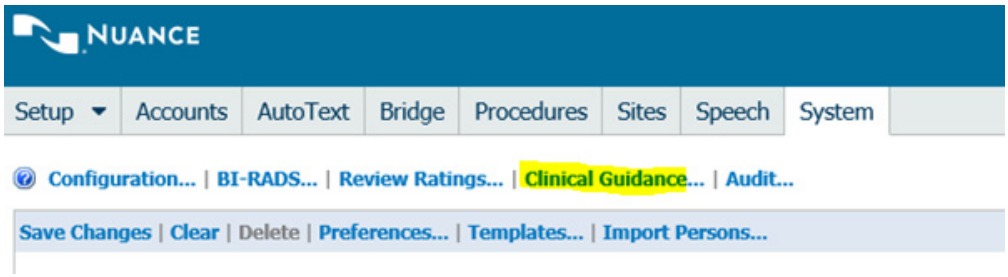
The PowerScribe 360 Reporting Client successful install dialog displays.



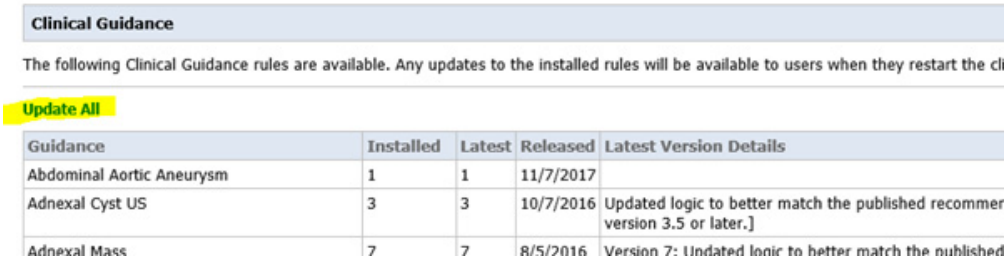
13. Click **OK**.
14. Click **Close**.

Update Clinical Guidance Rules

1. Log into the Admin Portal.
2. From the System tab, click **Clinical Guidance**.



3. In the new window, click **Update All**.



If site will FAX out of PS360
Downgrade PDF version on Application Server

If the site is using PS360 for faxing (direct from PS360), you will need to uninstall the version of PDF that was installed with the application server (8.1) and down grade / install Nuance PDF v7.1.

This issue impacts v3.x and v4.x and is not required for other versions.

Apply Post Installation Hot Fixes

Download and apply all available hot fixes for the version you have upgraded. Hot fixes to apply for each version are listed below.

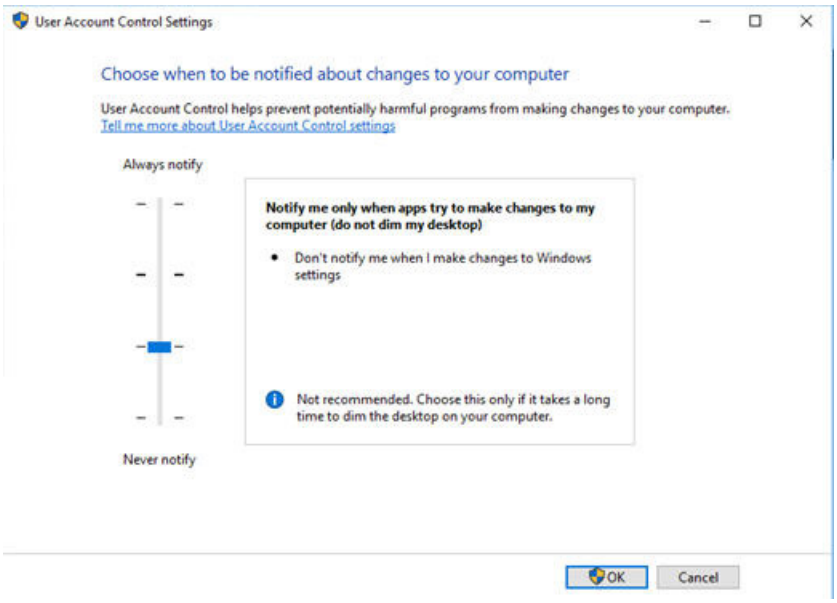
NOTE

Review the Patches and Hot Fixes Table for the latest" updates, so the installer can be sure what additional HFs have to be applied on top of patches. For example, 3.0.1 Patch 2 contained a RadBridge and RadPortal update, however newer RadBridge and RadPortal hot fixes override what was in the patch.

Enable UAC

In order for Remote Diagnostics to properly operate, it requires that the User Account Control (UAC) settings be enabled on the servers. This should be set to the second (2nd) lowest setting.

1. From **Start** select **Control Panel**.
2. On the **Control Panel**, click **User Accounts**.
3. On the **User Accounts** window, click **User Accounts**.
4. On the **User Accounts** tasks window, click **Turn User Account Control on**.
5. Adjust **UAC** to the level shown below:



6. Click **OK**.
7. Click **Restart Now** to apply the change right away, or click **Restart Later**, and then close the **User Accounts** tasks window.

Mobile Server

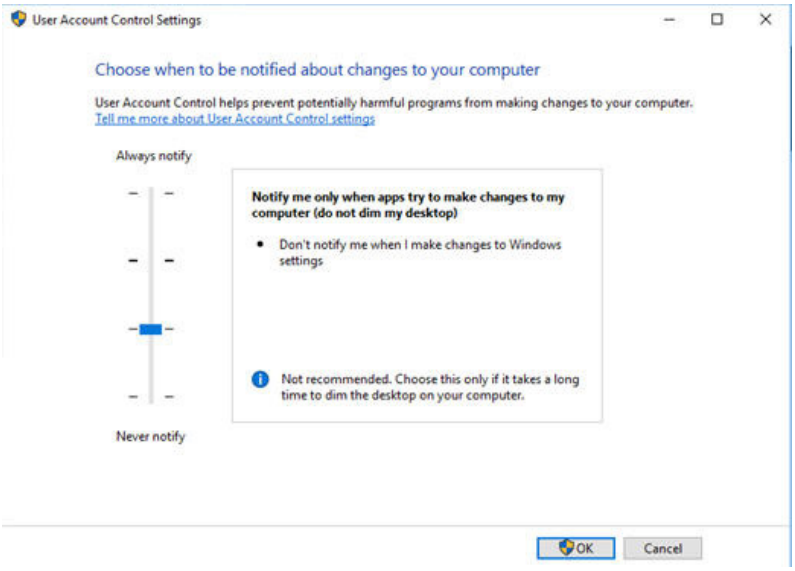
If the mobile Server application was not installed on the main Application Server, perform the upgrade process on the Mobile server platform.

1. Verify the Remote Diagnostics configuration.

Enable UAC

In order for Remote Diagnostics to properly operate, it requires that the User Account Control (UAC) settings be enabled on the servers. This should be set to the second (2nd) lowest setting.

1. From **Start** select **Control Panel**.
2. On the **Control Panel**, click **User Accounts**.
3. On the **User Accounts** window, click **User Accounts**.
4. On the **User Accounts** tasks window, click **Turn User Account Control on**.
5. Adjust **UAC** to the level shown below:



6. Click **OK**.
7. Click **Restart Now** to apply the change right away, or click **Restart Later**, and then close the **User Accounts** tasks window.

Speech Server (SUS)

Verify Dragon Version

If you are performing an upgrade from a previous version of PowerScribe 360 Reporting:

1. Verify that the SUS server has the latest version of Dragon Software installed.
2. To verify the Dragon version, perform the following on the SUS server:
   a. From start, click **Dragon SDK Client edition 12.5**.
   b. Click **show Dragon Log**. This will open the C:\Users\<Windows User>\AppData\Roaming\Nuance\Dragon SDK Client Edition12 directory.
   c. Double-click **dragon.log**.

      The Version is provided at the top of the dragon.log.

      For example: 08:20:03.105 Dragon NS ActiveX Components: File C:\Program Files (x86)\Nuance\Dragon SDK Client Edition12\Program\dnstk10.dll: Version 12.52.150.151
   d. If the Version is lower than the latest version, you must upgrade the Dragon client on the SUS server and SUS nodes before upgrading the SUS application.

Upgrade Dragon SDK Medical Software on SUS

1. Copy the **Dragon12DOT5PS360SP##.exe** file to the SUS machine.
2. Double-click the file.
3. Click **Update**.
4. Click **Finish**.
5. Reboot the server (if prompted).

Verify SUS Version

1. Verify the SUS version is the latest version.
   a. If the versions are up to date for Dragon and SUS, set the Services to run under the services account. Use the same services account you used for the services on the application SQL server.
   - DistributedManagementFramework: Agency
   - SQL Server
   - SQL Server Agent
   - SPARK host manager service
   - SPARK speech node manager
   - SPEECH utility server
   - SPARK core services

   b. If the Dragon is up-to-date, but SUS is not, skip to Uninstall Applications section below.
   c. If the neither versions are up to date for Dragon or SUS, continue to the next step.

Uninstall Applications

Uninstall SUS (if not correct version):

1. Stop the following services:
   - **SPARK host manager service**
   - **SPARK speech node manager**
   - **SPEECH utility server**
   - **SPARK core services**
2. Open **Windows Task Manager** and click the **Processes** tab.
3. Sort the processes alphabetically by **Image Name**.
4. Highlight the **Nuance.ConversionServer.ClientApp.exe** process, click **End Process**, and confirm the action.
5. From the **Control Panel/Programs and Features,** uninstall the **Speech Utility Server** software.
6. Open Microsoft SQL Server Management Studio.
7. Right-click the **SPARK database** and delete it.

Uninstall SQL Express (if not correct version)

Go to **Control Panel/Programs and Features** and uninstall the **MS SQL Express** software.

Verify the Folders are Properly Configured

On SUS, verify that the folder named Nuance (and it's sub folders) have Full Control for both the folder permissions and the share permissions assigned to the service account you created.

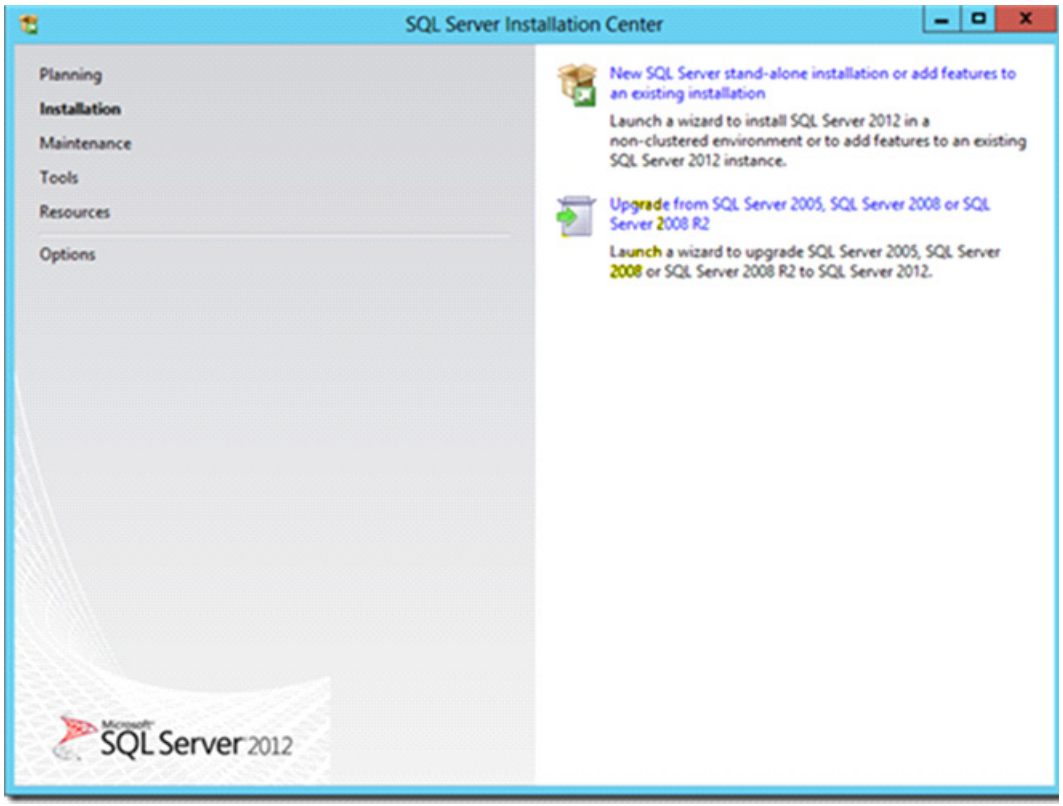
Ensure the Everyone account is not assigned to folder or share permissions.

Upgrade Microsoft SQL Server Express

IMPORTANT

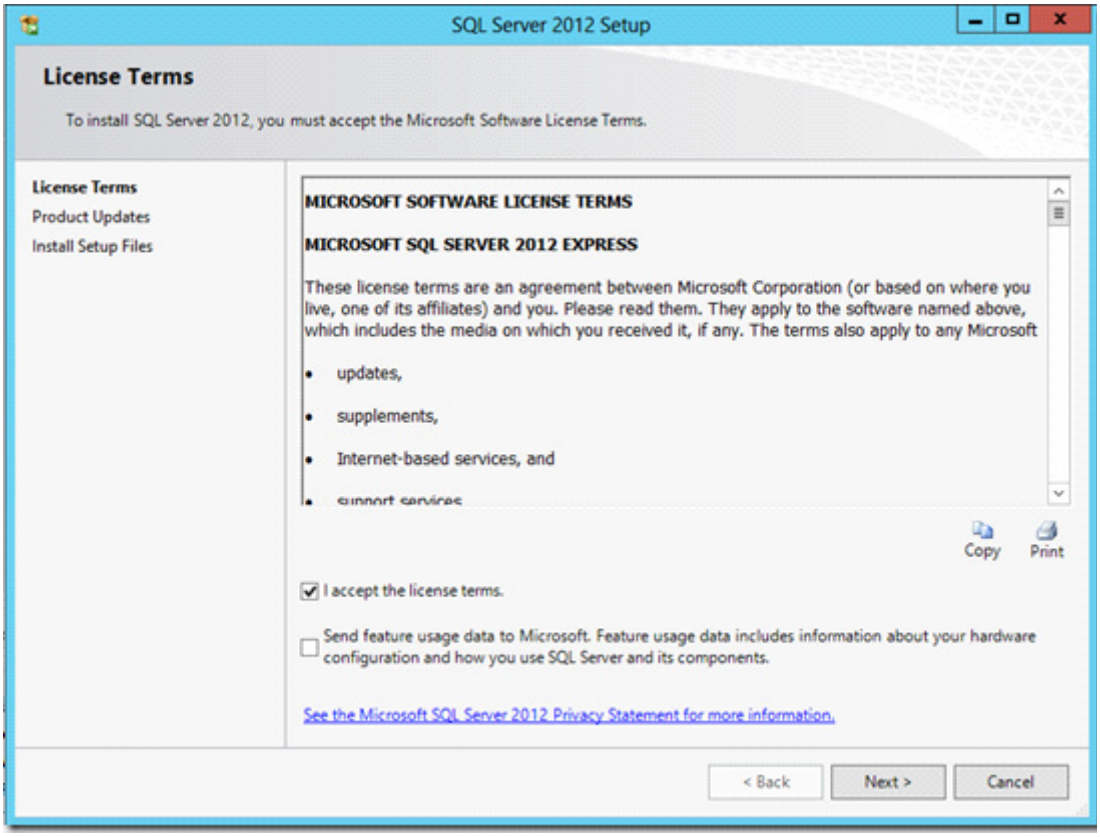
You should always upgrade to the latest Microsoft SQL Express software version supported by your version.

1. Download and extract the zip folder.
2. Double-click the installation file. The SQL Server Installation Center dialog displays.



3. Select **Upgrade from SQL Server 2005, SQL Server 20008, or SQL Server 2008 R2**.

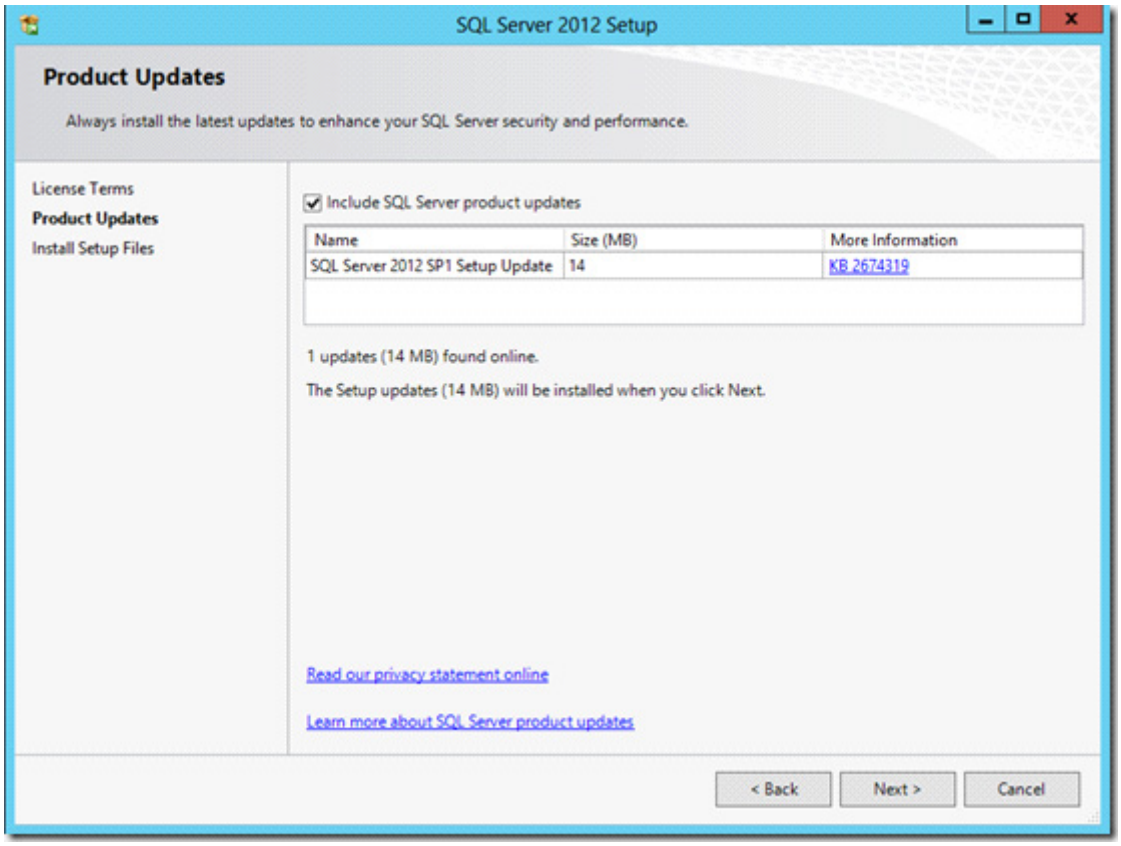
The License Terms dialog displays.



The wizard lists information about product updates available to install.

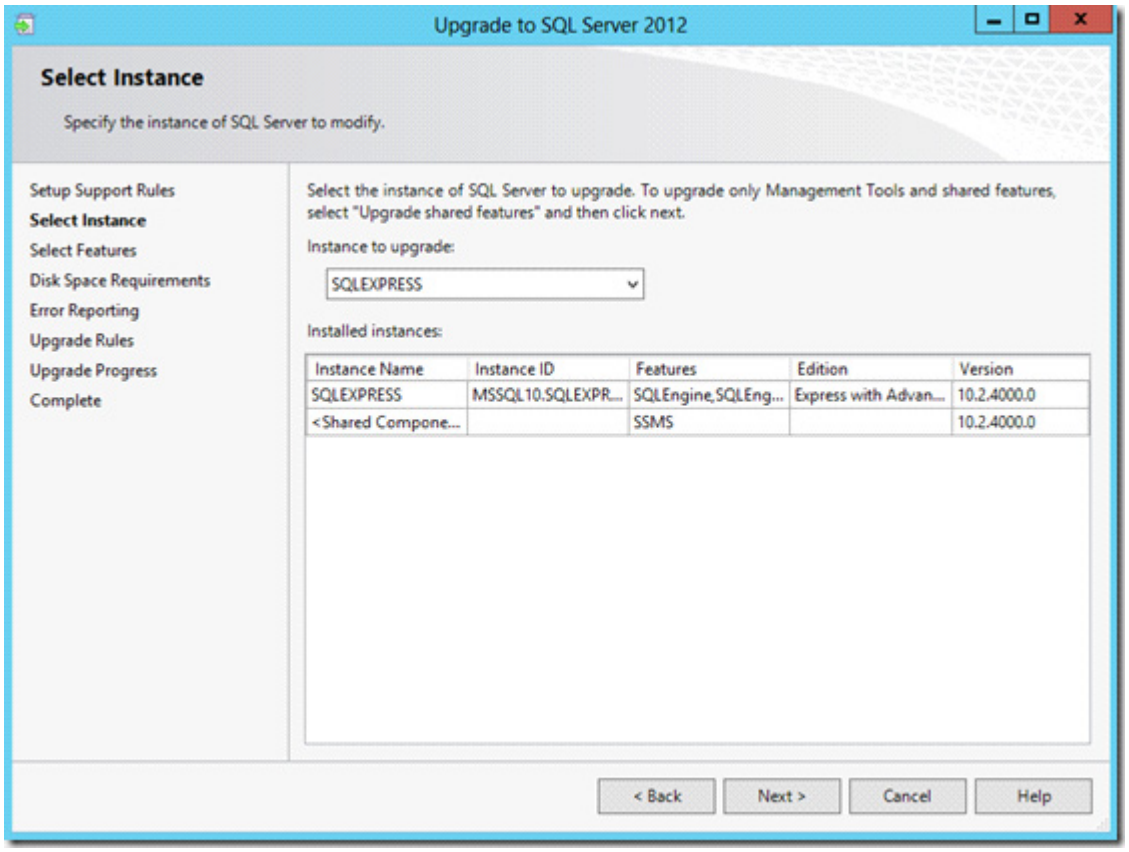
4. Check **I accept the license terms**, and click **Next**.

The Product Updates dialog displays.



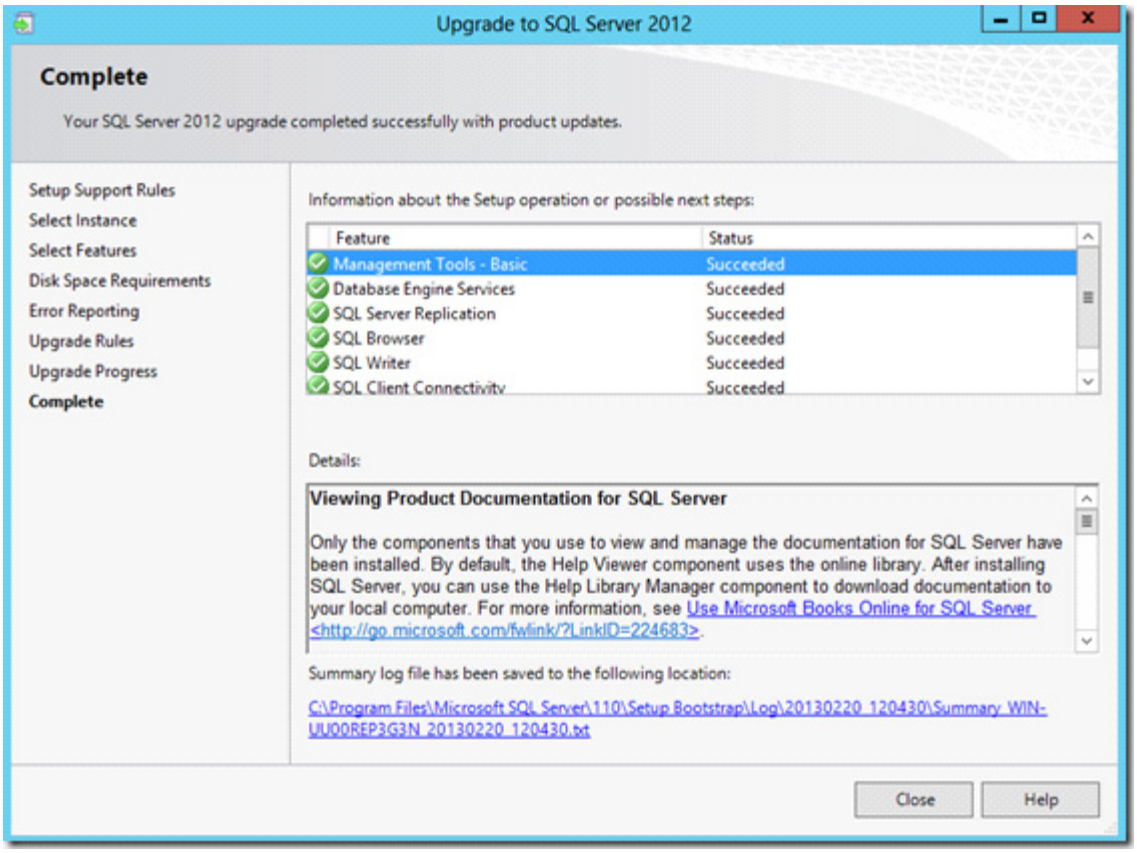
5. Check **Include SQL Server product updates**, and click **Next**.

The Select Instance dialog displays.



6. Click **Next**.

The Complete dialog displays.

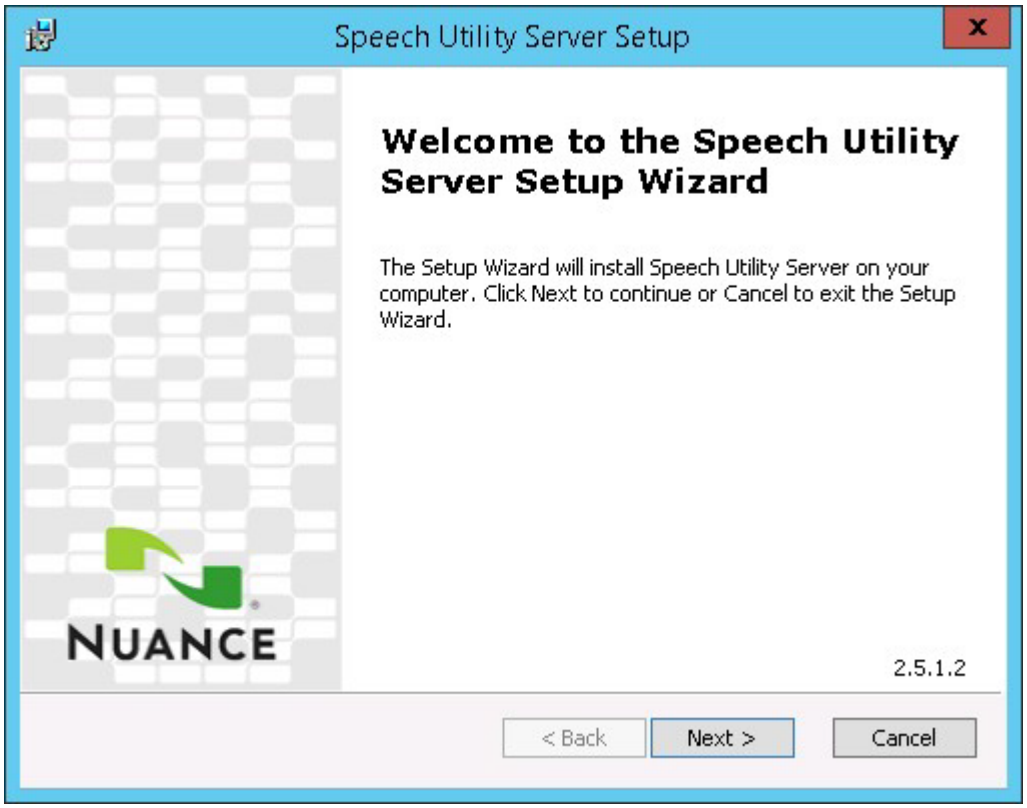


7. Click **Close**.

Install the SUS Software

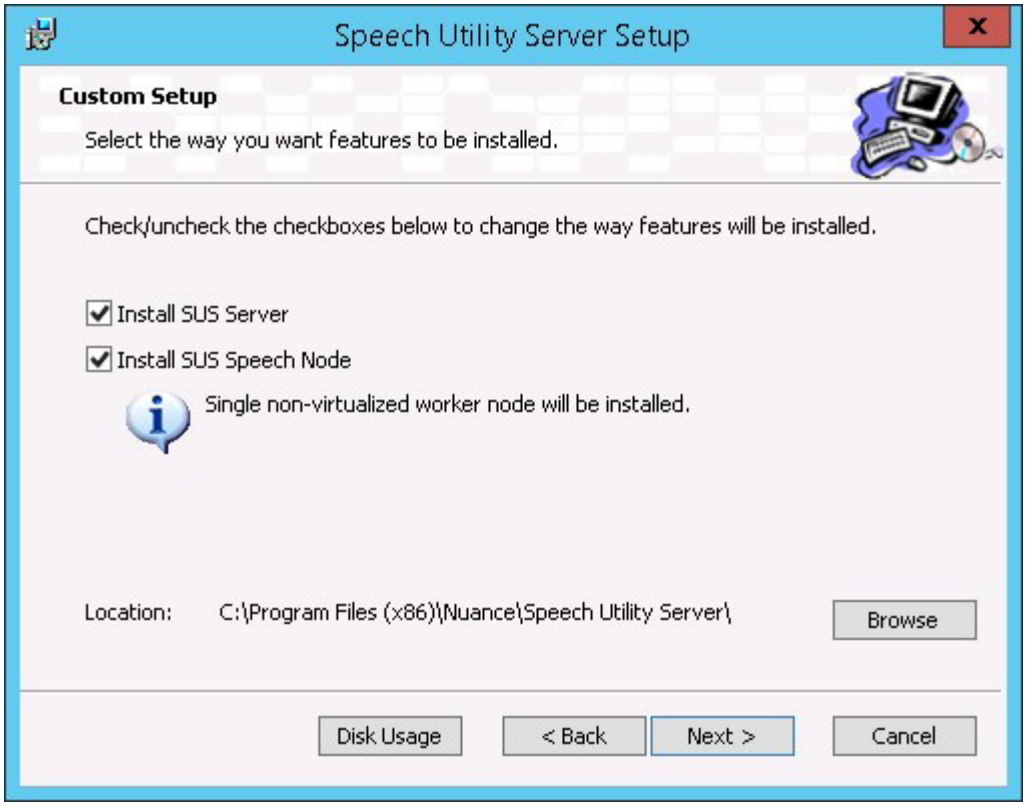
Step 2 - Welcome Window

Navigate to the **setup.exe** and double-click it to start the installation.



Step 3 - Feature Selection Window

1. Click **Next** on the Welcome dialog to display the Custom Setup dialog.



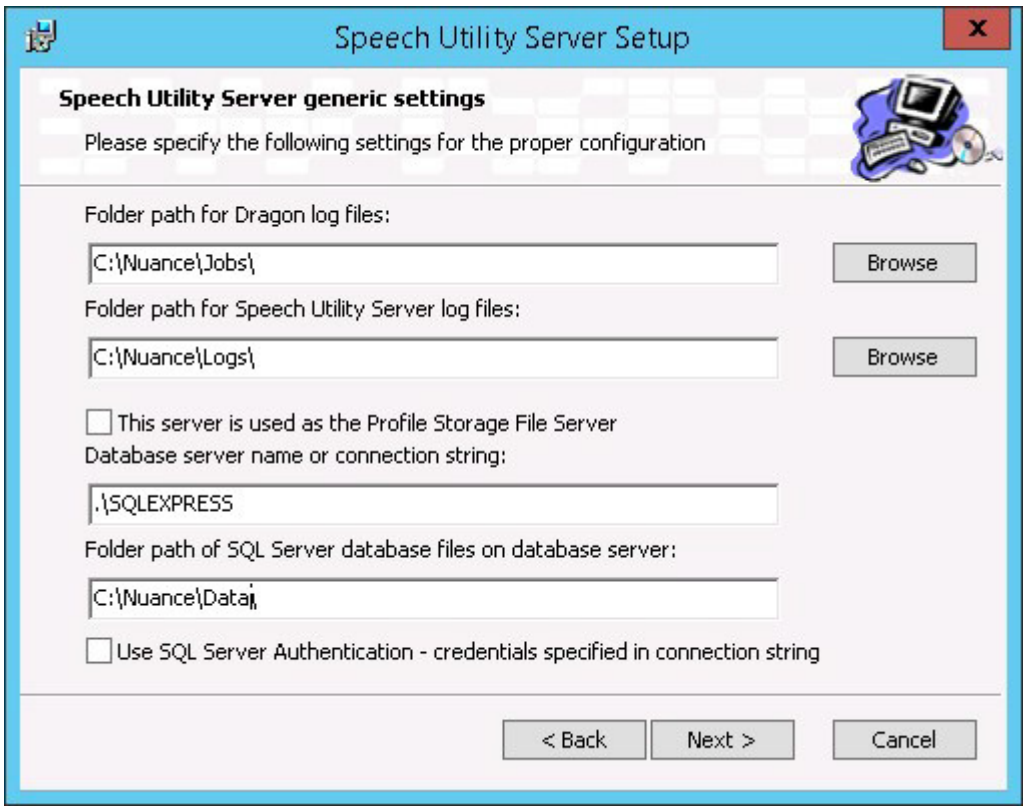
2. If this is the main SUS Server or a Profile Storage SUS server, check both of the following:
   - **Install SUS Server**
   - **Install SUS Speech Node**

   OR

   - If this an additional SUS Server, check only the **Install SUS Speech Node** option.
3. Click **Next**.

Step 4 - Server Settings Window

After completing the steps above with the proper selections, click **Next** to continue to reach the dialog below to display the Speech Utility Server Setup dialog. You must enter the destination directories for the logs. The following is an example:



1. Enter/verify the location for the paths to the Dragon log files and SUS log files for this server, using the correct drive letters and folder names.

DECISION

If this is going to be a Profile Server, check This server is used as the Profile Storage file server.

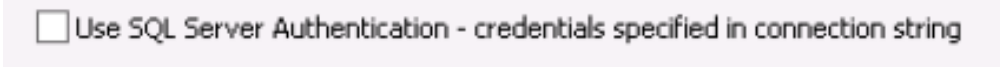
2. Set the database server name or connection string to:

   .\SQLEXPRESS

3. Set the Folder path for the SQL database files to **X:\Nuance\Data**.

   If using a different server hosting SQL, be sure to specify the proper drive letter on the DB server.

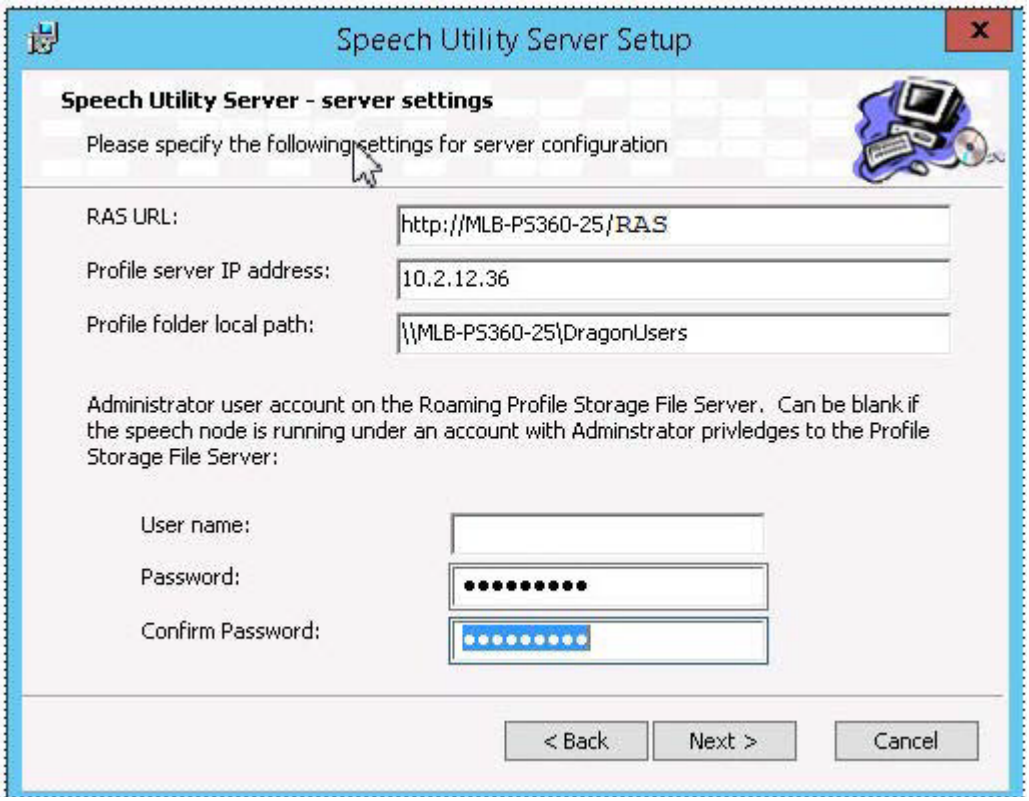
   Be sure to check Use SQL Server Authentication - credential specified in connection string.



4. Click **Next** to continue to reach the following dialog and enter the server settings.

Step 5 - RAS and Profile Storage File Server Settings

The following dialog is only an example.



RAS URL

For non-cluster configurations, use the host name for the Application Server.

For cluster configurations, use the FileShare Service Host Name.

Profile Server IP Address

For non-cluster configurations, this is the IP address of the file server that acts as the Roaming Profile storage and must be specified here. ***Do not use the host name.***

For cluster configurations, use the IP address assigned to the FileShare Service Host Name.

NOTE *If this is a Remote Profile Storage Server, the option will not be shown.*

Profile Folder Local Path

This is the location where the user profiles are stored, for example:

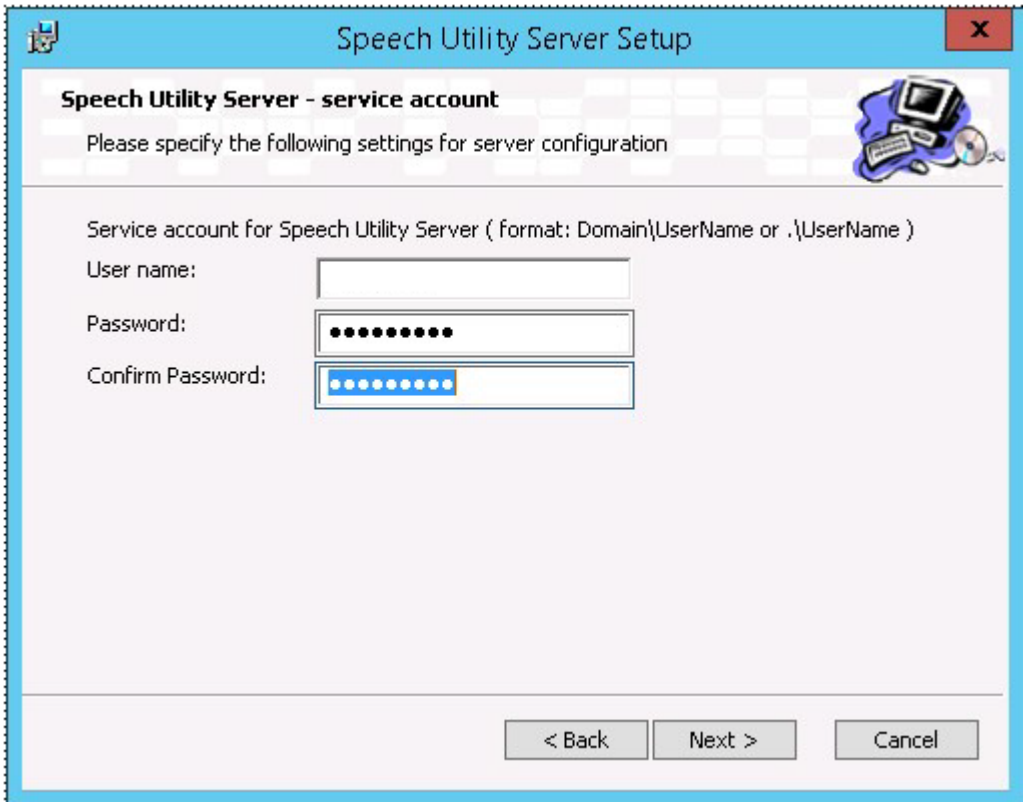
- Location on the application server where user profiles are stored \\<servername>\DragonUsers.

NOTE *If this is a Remote Profile Storage Server, the option will not be shown.*

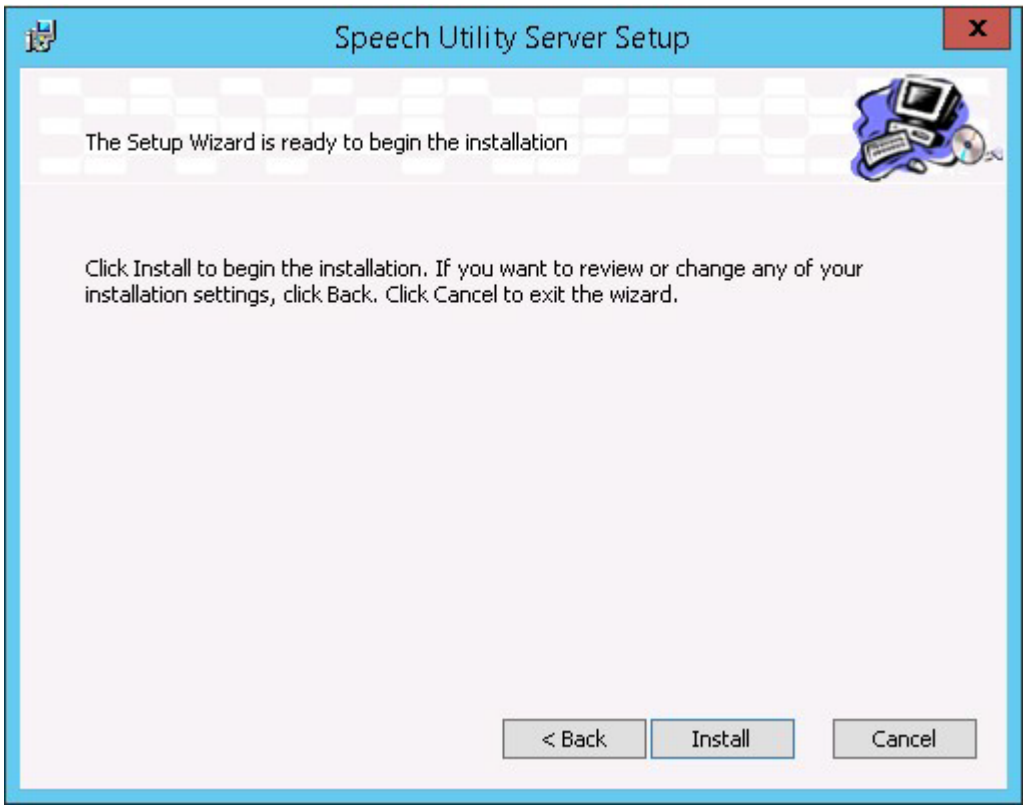
5. Enter Service account name and password as \<Service Account>.

Step 6 - Service Account for SUS

After clicking **Next** in the section above, the following dialog displays.



6. Enter the Windows Service Account Name and password account you used on the Application, SQL, and Mobile server.
7. After entering the information, click **Next** to display another dialog for the Speech Node that is nearly the same as the one above.
8. Enter the same Windows Service Account Name and password account you used on the Application, SQL, and Mobile server.
9. Click **Next**.



10. Click **Install**.

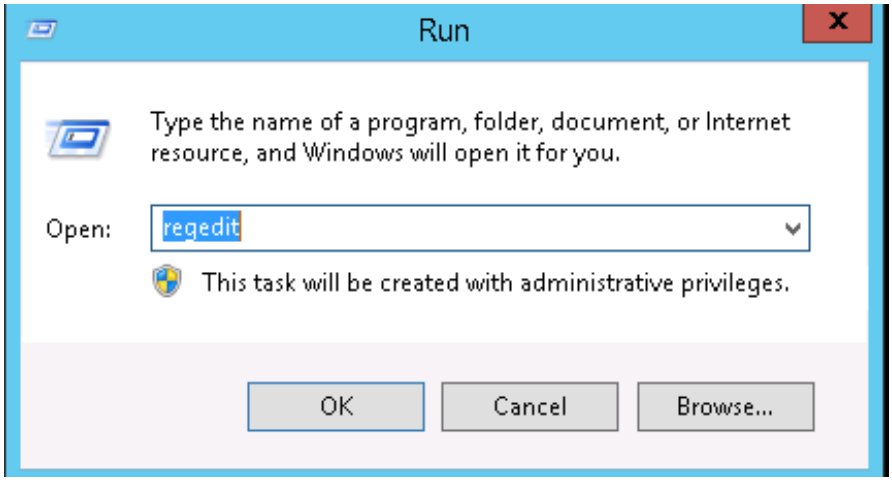
    SUS uses a tool to execute commands remotely on the file server hosting the User profiles.

    The installer launches the PSEXEC tool at the end of the installation to force the user to accept the EULA if you have never accepted it on the same box.

After the installation is complete, the following dialog displays.

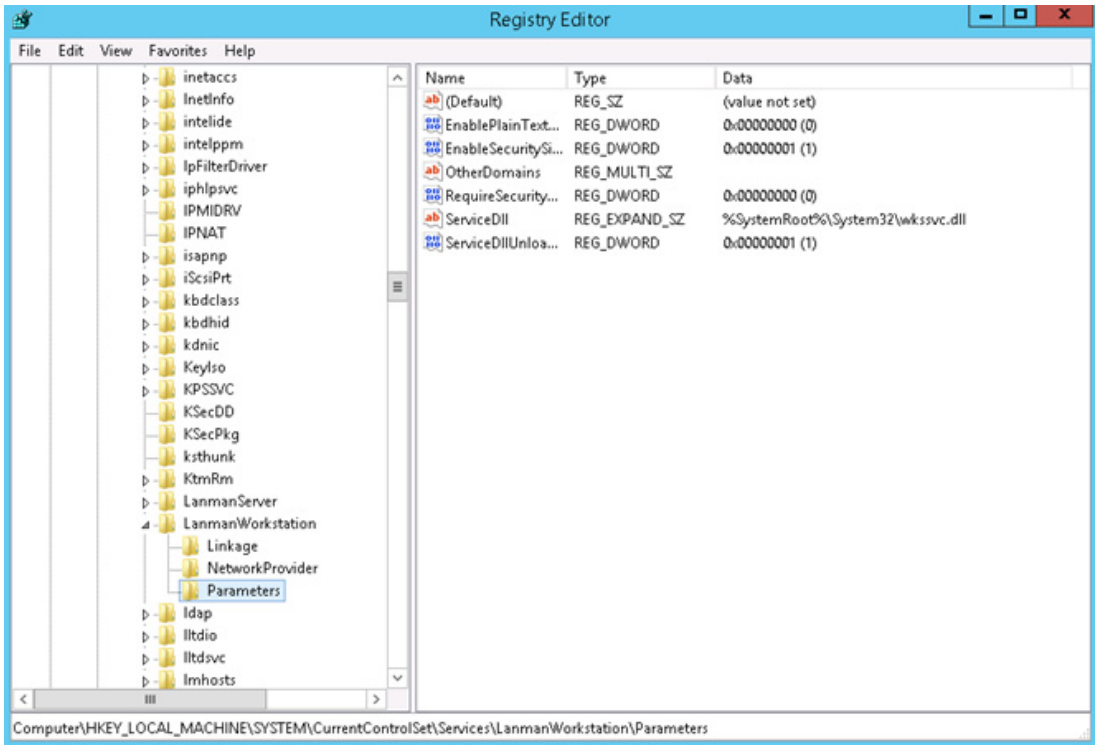
11. Click **Finish** and close all windows.
12. Edit the Registry as follows:
    a. Right-click **Start**, and select **Run**.

b. In the Open box, type **Regedit** to run the program.



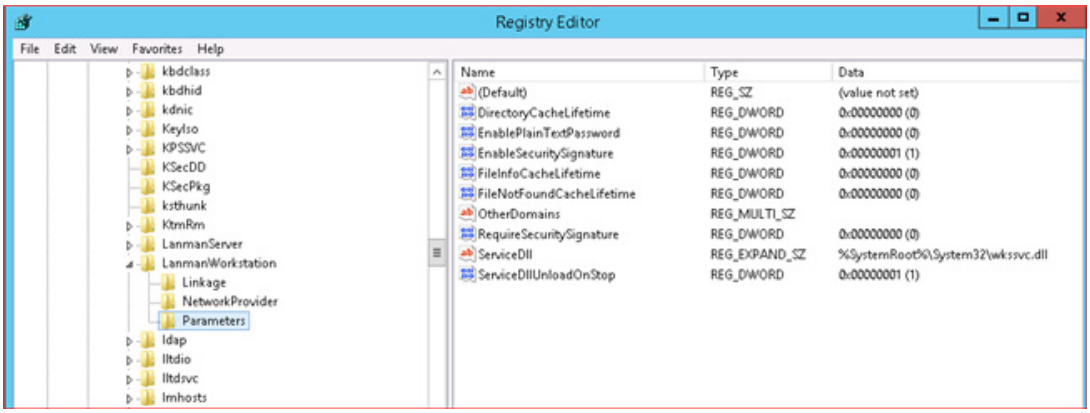
The Registry Editor opens.

c. Navigate to:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanworkstation\Parameters



d. Create the DWORD entries below:

- **FileInfoCacheLifetime with value data of 0**
- **DirectoryCacheLifetime to 0**
- **FileNotFoundCacheLifetime to 0**

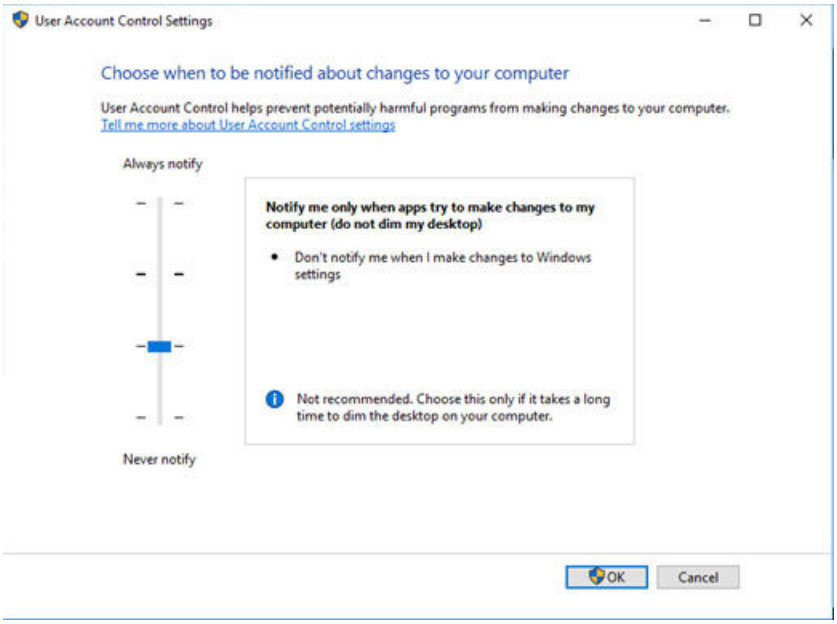


13. Reboot the server.

Enable UAC

In order for Remote Diagnostics to properly operate, it requires that the User Account Control (UAC) settings be enabled on the servers. This should be set to the second (2nd) lowest setting.

1. From **Start** select **Control Panel**.
2. On the **Control Panel**, click **User Accounts**.
3. On the **User Accounts** window, click **User Accounts**.
4. On the **User Accounts** tasks window, click **Turn User Account Control on.**
5. Adjust **UAC** to the level shown below:



6. Click **OK**.
7. Click **Restart Now** to apply the change right away, or click **Restart Later**, and then close the **User Accounts** tasks window.
8. Verify Remote Diagnostics Configuration.
9. Reboot the server.

PowerXpress

For upgrade instructions, see PowerXpress Upgrade Manual, PN 889812.

Enable UAC

In order for Remote Diagnostics to properly operate, it requires that the User Account Control (UAC) settings be enabled on the servers. This should be set to the second (2nd) lowest setting.

1. From **Start** select **Control Panel**.
2. On the **Control Panel**, click **User Accounts**.
3. On the **User Accounts** window, click **User Accounts**.
4. On the **User Accounts** tasks window, click **Turn User Account Control on**.
5. Adjust **UAC** to the level shown below:

Set Services to use the Services Account

Verify the following services are running under the same Windows Services account.

- DistributedManagementFramework: Agency
- PX2008

Uninstall MSSQL Express

1. Open Control Panel > Programs and Features.
2. Select MSSQL Express, and choose Uninstall.

Upgrade Add-On Products / Modules

Hot Spare

Re-enable the SQL AlwaysOn if the system has a hot spare. Refer to Hot Spare Installation and Configuration — 889715.

Upgrade ModLink

For upgrade instructions, see the Installation Guide, PN LX-DOC-ML2.3.0-IN-EN-REV.

Upgrade ModLink Web Forms

For upgrade instructions, see the Core Server Installation Guide, PN LX-DOC-PCS3.6.0-IN-EN-REVA.

Upgrade mPower

Backup DB

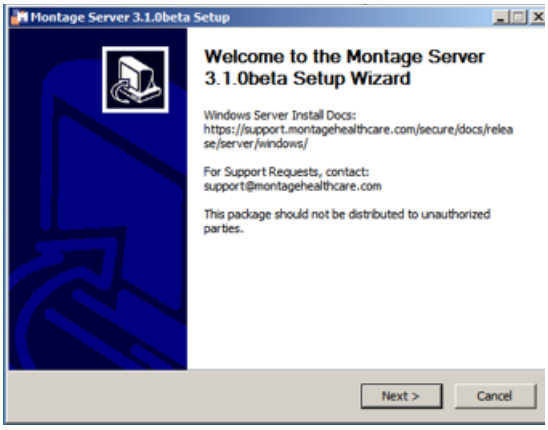
Move this copy to another server for security. Refer to iSupport Solution 19963: mPower Backup and Restore Procedures.

Upgrading

You must first upgrade the system to Montage 3.0 before proceeding with a newer version. Refer to PN 889681 — PowerScribe® 360 Reporting Montage Installation Manual for upgrading to 3.0 if necessary.

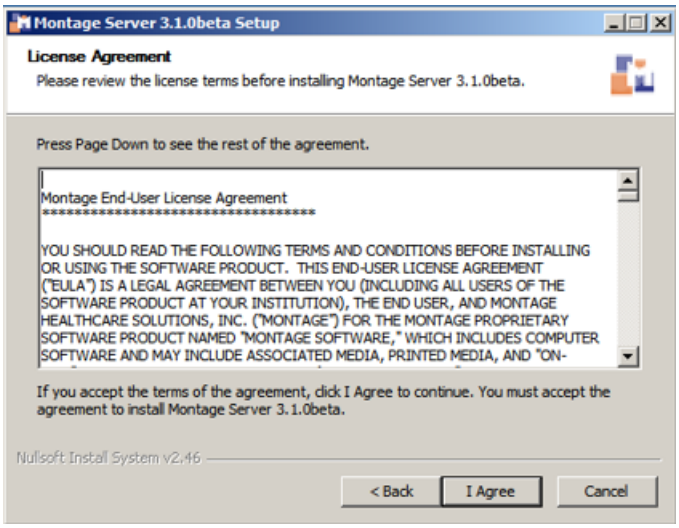
1. Run the Montage installer. It will detect and upgrade all required components.

   The Welcome dialog displays.



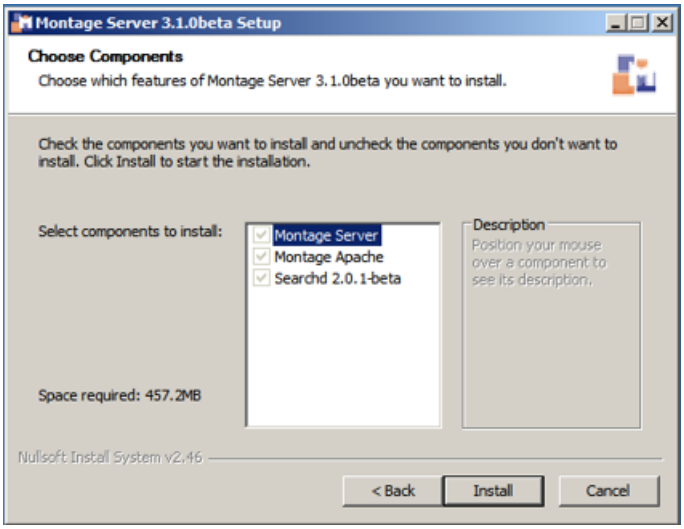
2. Click **Next.**

The Montage License Agreement dialog displays.



3. Click **I Agree**.

   The Montage installation will install all components listed. Checks to determine the system state are encompassed within the install components.



4. Click **Install**.

   The installer will take a few minutes.

Reboot Server

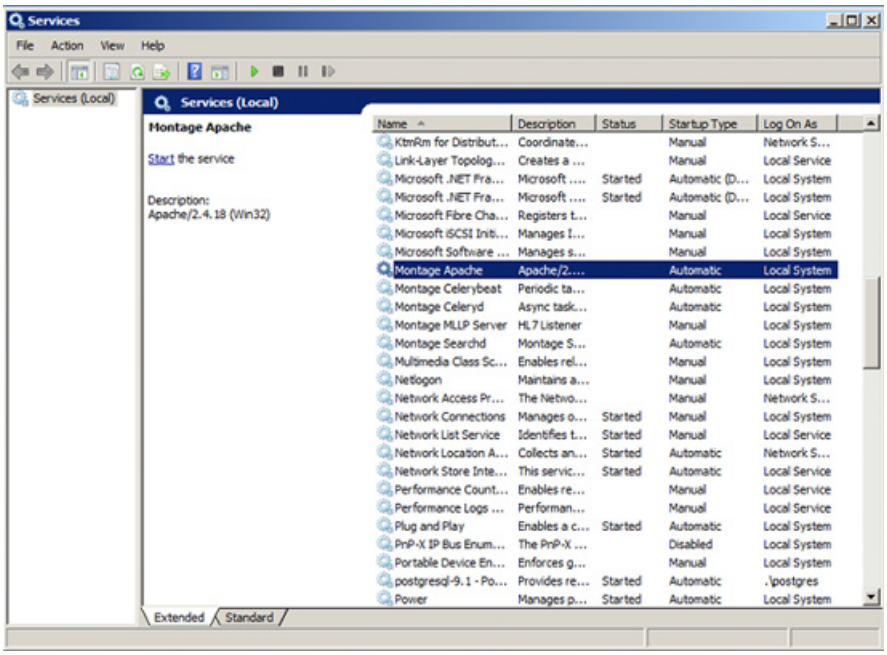
Reboot the Server.

Check Services

Once mPower is upgraded, you need to confirm that the Serves are started.

Verify that the “Montage Searchd”, “Montage Celeryd”, and “Montage Celerybeat” services are running. If they are stopped, start them.

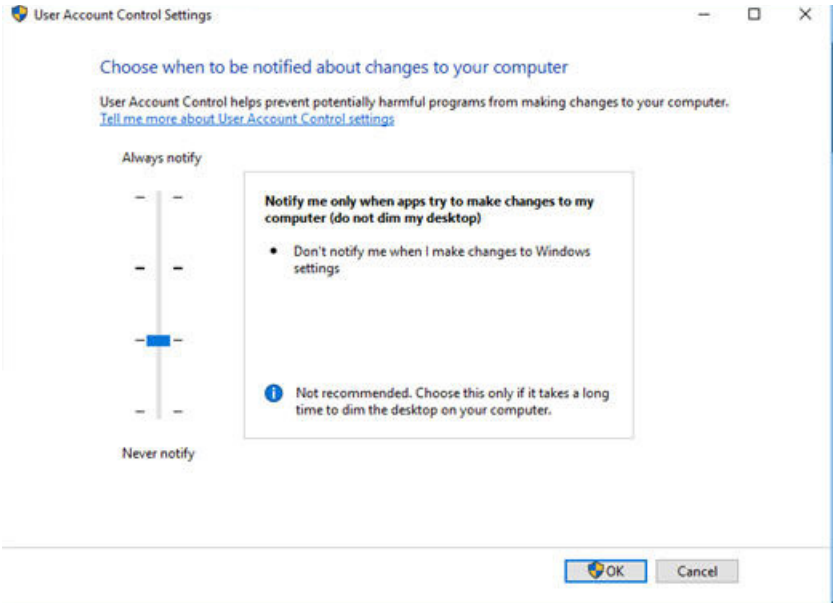
WARNING: Only start “Montage MLLP Server” if it Montage is receiving HL7 messages.



Enable UAC

In order for Remote Diagnostics to properly operate, it requires that the User Account Control (UAC) settings be enabled on the servers. This should be set to the second (2nd) lowest setting.

1. From **Start** select **Control Panel**.
2. On the **Control Panel**, click **User Accounts**.
3. On the **User Accounts** window, click **User Accounts**.
4. On the **User Accounts** tasks window, click **Turn User Account Control on**.
5. Adjust **UAC** to the level shown below:



6. Click **OK**.
7. Click **Restart Now** to apply the change right away, or click **Restart Later**, and then close the **User Accounts** tasks window.
8. Verify Remote Diagnostics Configuration.

Set Services to use the Services Account

Verify the following services are running under the services account.

- DistributedManagementFramework: Agency

Appendix 1 - Troubleshooting

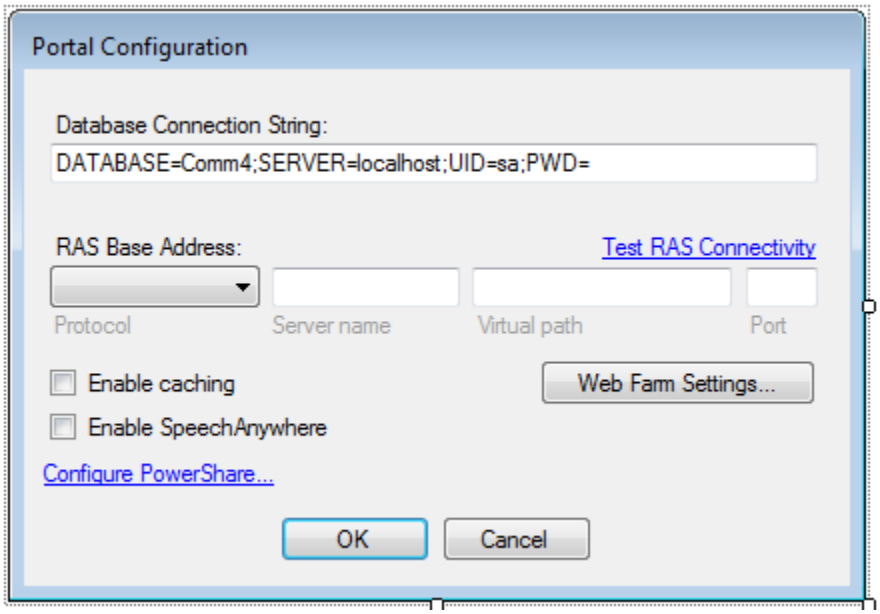
Password Conversion Issues

If, after performing the upgrade, and you cannot log into the Portal with the correct ADMIN password, you may need to rerun the password conversion. This can fail during the upgrade process if the connection to RAS is interrupted.

To convert the passwords if the upgrade password fails during the upgrade process, perform the following:

1. From the C:\inetpub\wwwroot\RadPortal folder, right-click **PortalConfigUI.exe** and select **Run as Administrator**.

   The Portal Configuration dialog displays.



2. On the Portal Configuration dialog, click **OK**.

NOTE *If there are any account passwords that need to be converted, the Utility will convert them and will present a dialog with the following:*

"Security upgrade succeeded. {0} account passwords have been converted to one-way salted hashes." << {0} Number of accounts converted.

Login Issues

V4.0 DBSetup Update - BypassLDAP Flag

ISSUE: Unable to login to default administrator account after running v4.0 DBSetup update.

In version 4.0, during the DBSetup process, a new flag, BypassLDAP, is added to the accounts table. If LDAP is enabled on the system prior to running the DBSetup, the BypassLDAP flag is set to 0 (false). This can potentially lock access to the default administrator (admin) account.

If this occurs, run the following script to set the BypassLDAP flag to 1 (true) to login to the default administrator account.

```
update account
set bypassldap = 1
where loginname = 'admin'
```

Note this can also occur if LDAP is turned on, but the configuration is incorrect or the LDAP server is inaccessible, all accounts that do not have the BypassLDAP flag set to true would be inaccessible.

Appendix 2 - Microsoft Windows Configuration Guidelines

Microsoft Windows should be installed by the facility using their internal guidelines and practices. Below is a set of guidelines for Roles and Features that should configured as part of the installation.

IMPORTANT

The IIS must be installed and configured on the C drive for PowerScribe 360 Reporting Application Server and for the Mobile server.

If you are setting up a server for Mobile server, WebDAV is not required. WebDAV is only used by the Application server.

Only the most current .NET Framework version is required for proper PowerScribe 360 Reporting v4.0.1 (SP1) and higher installation and operation when using Windows 2016 and MSSQL 2016. In this case older versions of .NET (i.e., .NET 3.5) should not be installed.

The minimum features to install are below. The facility may have chosen to install more features as needed according to their internal policies and processes.

1. Install the following Server Roles
    - A. File And Storage Services (default install)
        - a. File and iSCSI Services
            - File Server
        - b. Storage Services
    - B. Web Server (IIS) (default install)
    - C. Fax Server (optional, check if Fax will be used)
2. Install the following Features
    - A. NET Framework 3.5 Features (only for Windows 2012 or if using SQL 2014 or SQL 2012)
        - a. .Net Framework 3.5
        - b. ASP.Net 3.5
    - B. . NET Framework 4.6 Features
        - a. NET Framework 4.6
        - b. ASP.NET 4.6
    - C. Message Queuing Services

a. Message Queuing Server
b. Directory Service Integration
c. HTTP Support
d. Message Queuing Triggers

D. WCF Services

a. HTTP Activation
b. Message Queuing (MSMQ) Activation
c. Named Pipe Activation
d. TCP Activation
e. TCP Port Sharing

3. Install the following Web Server Role Services

A. Common HTTP Features (ALL)

B. Health and Diagnostics

a. HTTP Logging
b. Logging Tools
c. Request Monitor
d. Tracing

C. Performance (All)

D. Security (All)

E. Application Development

a. .Net Extensibility 3.5
b. .Net Extensibility 4.6
c. ASP.Net 3.5
d. ASP.Net 4.6
e. ISAPI Extension
f. ISAPI Filters

F. Management Tools

a. IIS Management Console
b. IIS 6 management Compatibility
   - IIS 6 Metabase Compatibility
c. IIS Management and Scripts and Tools

Appendix 3 - Microsoft SQL Server Installation Guidelines

The MS SQL application should be installed by the facility using their internal guidelines and practices. Below is a set of recommendations and guidelines that should be selected during the install.

Complete Installation steps with explanations can be found at HERE.

1. The minimum features to install are below. The facility may choose to install more features as needed according to their internal policies and processes.
   a. Database Engine Services
   b. Reporting Services – Native
   c. SQL Server management Studio (Tools) – If installing SQL 2016, you will have to install this feature separately after the main installation is complete
2. It is recommended to use the default instance, however a named instance can be used.
3. The SQL services should be set to run under an appropriate account according to the site's internal guidelines.
4. The services should be set to Automatic Startup. It is not required to use NT Authority\System.
5. Mixed Mode Authentication **MUST** be used.

The SA account must never be deleted or disabled and is used during installation and updates of the database only. The customer will need to provide Nuance with a sysadmin account to install PowerScribe.

Best Practice

- The ***"SA"*** password entered should be provided by the customer's site administrator consistent with the customer's internal password policies. Nuance recommends the use of strong/complex passwords.
- Passwords should only be communicated over secure encrypted channels and/or stored in secure encrypted locations.

6. Be sure to add the local administrator account and service account as a SQL server Administrator.

7. The data directories should be set according to the site's internal policies and should be set to afford the temp DB and logs sufficient space to grow.

Manual Revision History

Note: In this table the most recent changes are first by date.

Date	Sec	Page	Change (Paragraph, Sentence, Figure, Table, etc.)	Initials
9/28/18	All	All	Added Best Practices.	BW