

Adding New Users

This document applies to the following ERP system(s):

AccountMate	Microsoft Dynamics GP	Sage 500
Acumatica	Microsoft Dynamics SL	Sage X3v5
Alere	QAD EE	Sage X3v6
CCH	QAD SE	SAP B1
Deltek Vision	Ross	Syspro
FiresStream	Sage 300	Traverse

This guide describes the steps required to install BizInsight and BizContent for additional users in your organization.

This document presumes that BizInsight is installed and fully functioning for at least one user within your organization.

Overview

Step 1: Locate Installation Files	1
Step 2: Assign BizInsight Security to Users	3
Step 3: Assign rights in SQL Server Security	11
Step 4: Assign rights in Reporting Services	17
Step 5: Add User to Column Based Security	19
Step 6: Install Oracle Data Access Components (ODAC)	24
Step 7: Install BizInsight	25
Installing BizInsight for the Non-Administrative User	32
Step 8: Configure BizInsight	35
Step 9: Verify the BizInsight Installation	47
Appendices	48
Manually Installing BizContent Add-ins	49
CheckTCP/IP, SQL Browser and Firewall Exceptions	60
BizInsight Column Based Security Overview	86
Assign BizInsight Security to Users	92

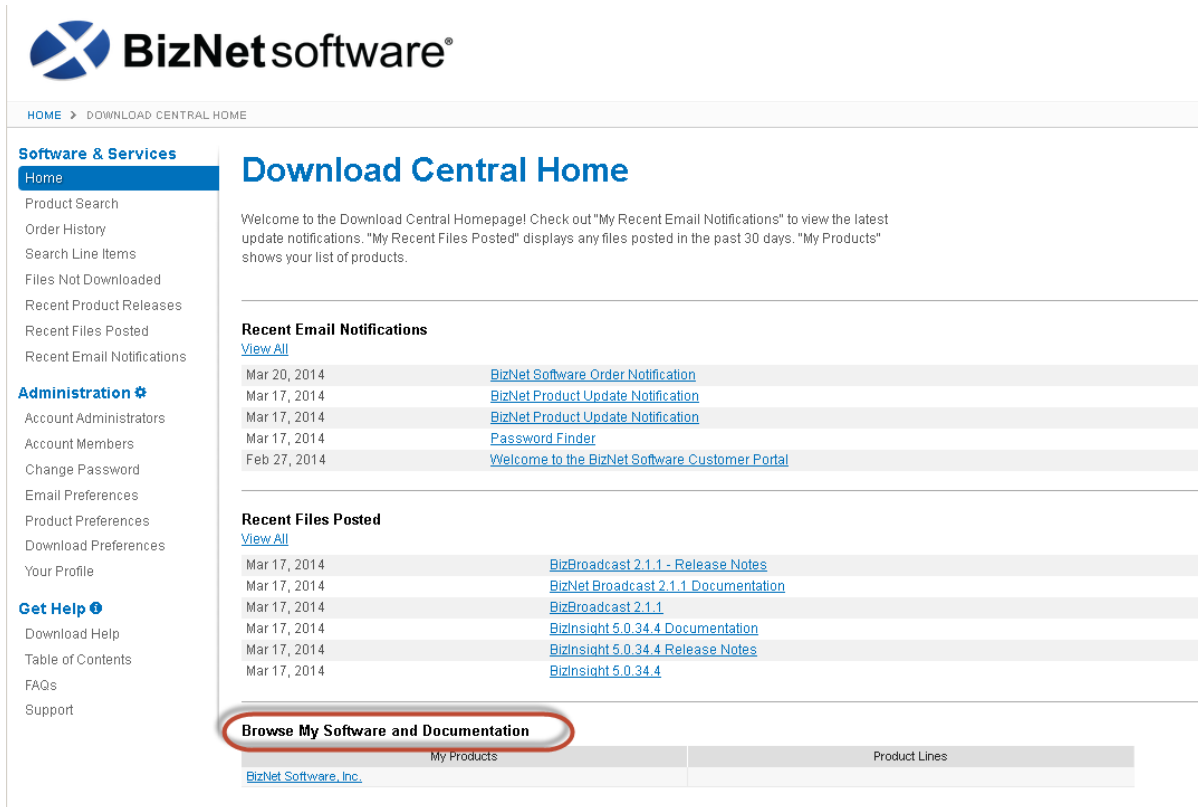
Step 1: Locate Installation Files

In preparation for installation, you need to confirm which version of BizInsight is installed on current BizInsight users' workstations so that you are sure to install the same version being run elsewhere. To do this, open Excel on an existing BizInsight user's workstation and click on the **About** button of the BizInsight Excel ribbon.

Once you have determined the current version, click on the **Application Settings** button and copy the path provided for the Configuration Path parameter, open Windows Explorer and browse to that directory. Look in that directory or in the level above for an Install Files folder or a folder for the BizInsight version that is currently installed. Where the installation files have been saved will vary from customer to customer but it is recommended in our documentation that they be saved near the BizInsight shared directory so there is a high likelihood that you will locate the necessary installer in this location or nearby.

If you are not able to locate the installer files for the currently installed BizInsight version, download the latest version from the BizNet Software customer portal, (<http://biznet.flexnetoperations.com>). In general, it is o.k. for BizInsight users to be on different BizInsight versions but there is always a chance that the latest version requires a configuration change that will necessitate all users be updated.

All files can be found under "Browse My Software and Documentation".



BizNetsoftware®

HOME > DOWNLOAD CENTRAL HOME

Software & Services

- Home
- Product Search
- Order History
- Search Line Items
- Files Not Downloaded
- Recent Product Releases
- Recent Files Posted
- Recent Email Notifications

Administration

- Account Administrators
- Account Members
- Change Password
- Email Preferences
- Product Preferences
- Download Preferences
- Your Profile

Get Help

- Download Help
- Table of Contents
- FAQs
- Support

Download Central Home

Welcome to the Download Central Homepage! Check out "My Recent Email Notifications" to view the latest update notifications. "My Recent Files Posted" displays any files posted in the past 30 days. "My Products" shows your list of products.

Recent Email Notifications

[View All](#)

Mar 20, 2014	BizNet Software Order Notification
Mar 17, 2014	BizNet Product Update Notification
Mar 17, 2014	BizNet Product Update Notification
Mar 17, 2014	Password Finder
Feb 27, 2014	Welcome to the BizNet Software Customer Portal

Recent Files Posted

[View All](#)

Mar 17, 2014	BizBroadcast 2.1.1 - Release Notes
Mar 17, 2014	BizNet Broadcast 2.1.1 Documentation
Mar 17, 2014	BizBroadcast 2.1.1
Mar 17, 2014	BizInsight 5.0.34.4 Documentation
Mar 17, 2014	BizInsight 5.0.34.4 Release Notes
Mar 17, 2014	BizInsight 5.0.34.4

Browse My Software and Documentation

My Products	Product Lines
BizNet Software, Inc.	

Following are the files you will need to download:

BizInsight 5.0.35.1

BizInsight Tools.zip - this download file contains several tools that you might need to use during implementation. It can be found with the BizInsight product download file.

BizContent - download all BizContent files to which you are entitled (required)

Step 2: Assign BizInsight Security to Users

Each BizInsight user's Windows account name must be added to a .users file in the admin shared directory in order for that user to perform any BizInsight action. You will use the License Administration Tool to perform these steps.

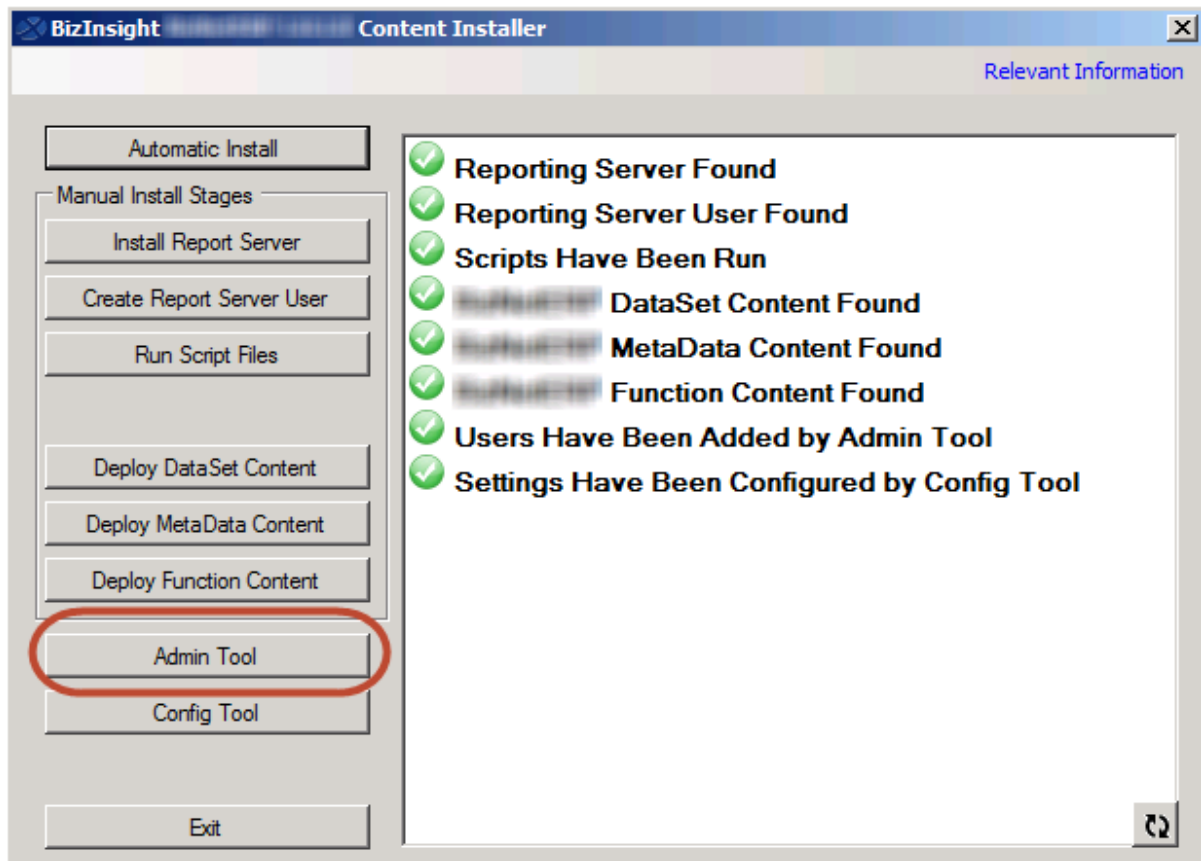
To assign BizInsight security to your users, do the following:

1. On the server, double-click any content installer desktop icon. If the content installers were installed without desktop icons, browse to the installation directory and double-click the file named "BizNet Content Installer.exe". If the content installer was uninstalled, reinstall it.



If you do not want to reinstall the content installer, see "Manual Steps" on page 9.

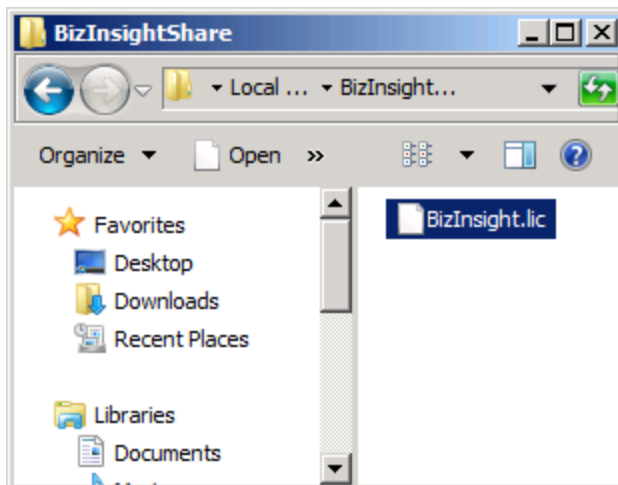
- Click on the **Admin Tool** button.



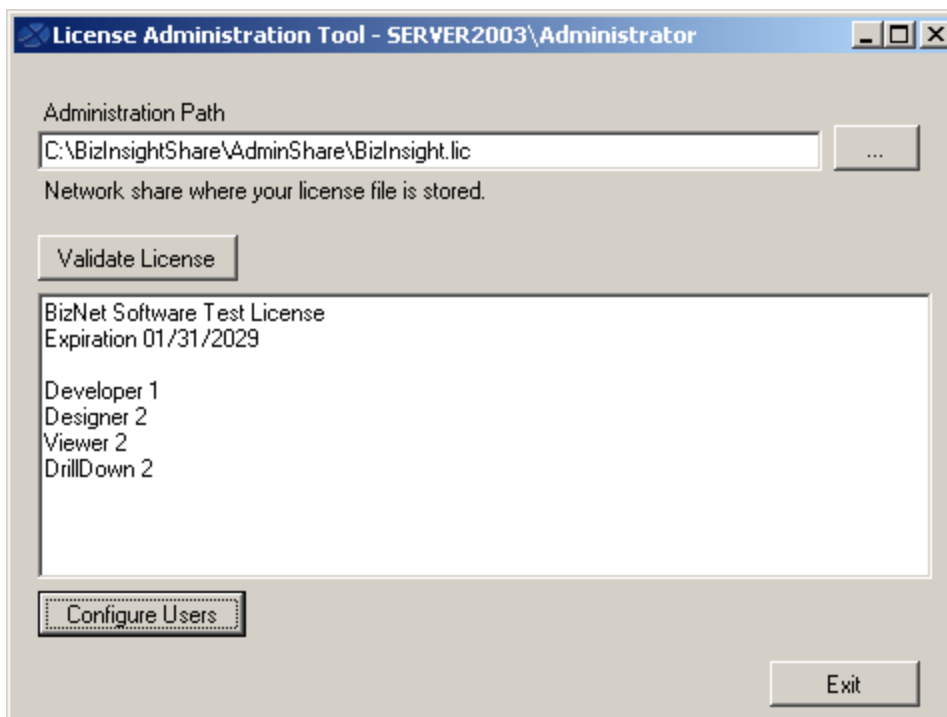
- Click on the ellipses and browse to the admin share folder of your BizInsight shared directory.



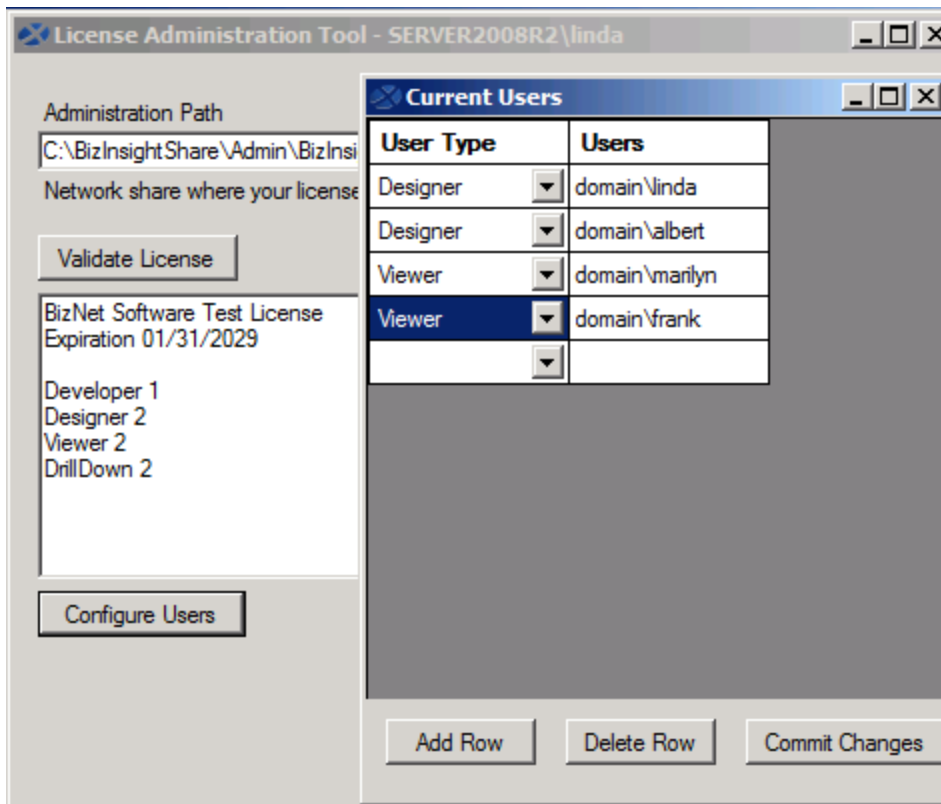
4. Select your BizInsight license file and click Open.



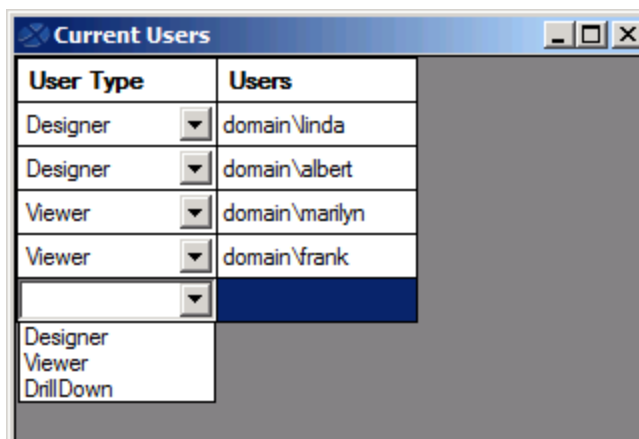
5. Click on the **Validate License** button to check how many licenses you currently have. Your current license count will be displayed.



6. Click on the **Configure Users** button. The **Current Users** dialog will open.

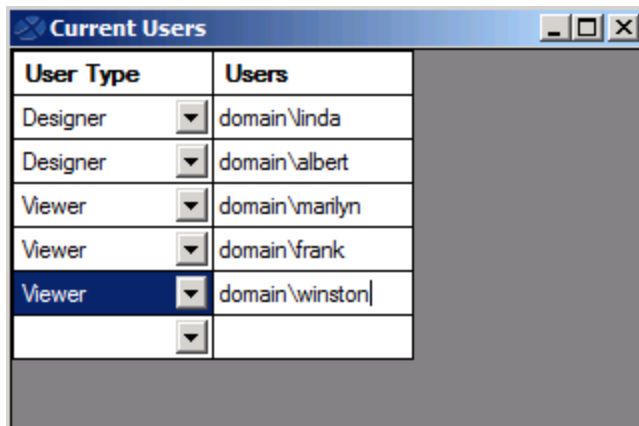


7. You will now add your new BizInsight user and assign them a user type. Click on the **User Type** drop down and select the desired user type. If you want your user to be a Designer, choose Designer from the drop down list.

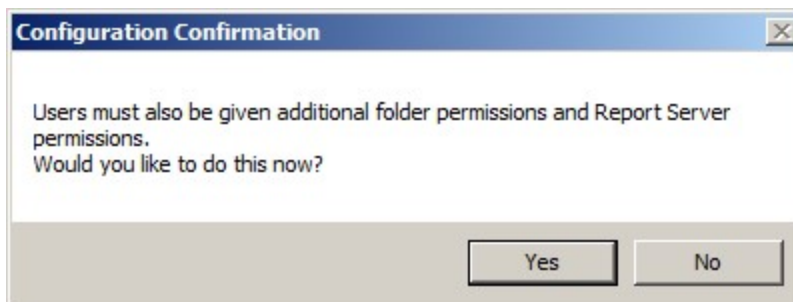


8. Type the user's name in the **Users** field in the format of domain\username.

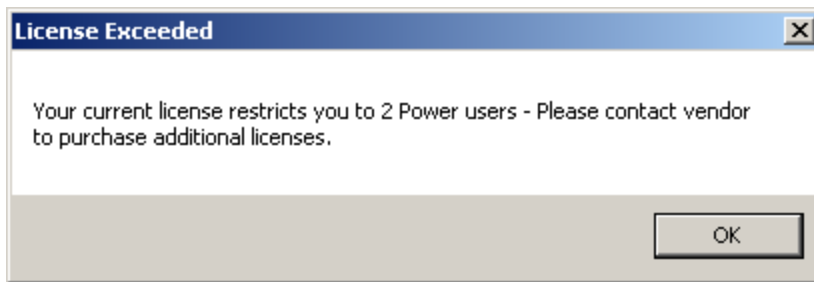
WARNING Do **not** add your own login using the Admin Tool unless you know for sure that you have another login available with sysadmin rights to the SQL Server instance. Early versions of the content installer (pre version 1.6) will remove existing permissions for users, including those with sysadmin rights. If uncertain, skip this step and confirm sysadmin access will not be lost then return to complete the Admin Tool step.



9. Click on the **Commit Changes** button when finished. You will be presented with a message asking if you want to grant the user additional security permissions. Click **Yes**.

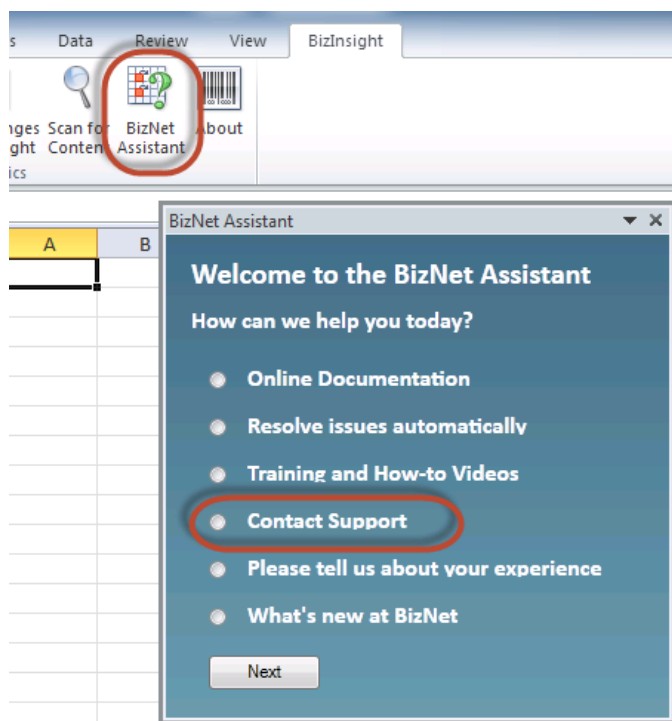


If you have entered more names for a particular user type than you have licenses, you will get an error similar to the following.



You will be returned to the **Current Users** dialog where you can remove a row so that you comply with the number of licenses your company purchased. Select the row to remove and click the **Delete Row** button.

To purchase additional licenses, use the BizNet Assistant button to open a support ticket indicating that you need to purchase additional licenses.



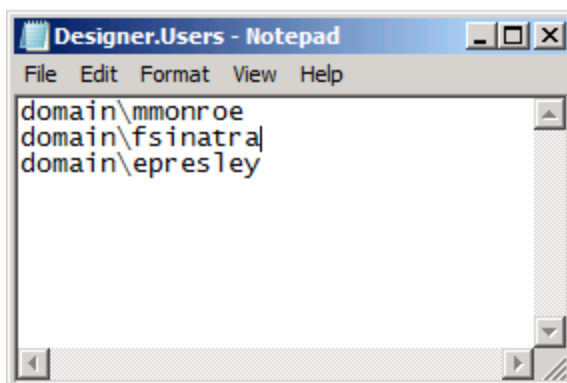
When you receive your new license, move your old license from the Administration Path shared directory and save the new license there. Do not rename the old license and leave it in the Administration Path; it must be removed from the directory in order for the new license count to take effect.

Manual Steps

1. In the Admin shared directory, open the .users file with Notepad that corresponds with the BizInsight permissions the user should have. For example, if the user should have Designer permissions, you would open the Designer.users file.

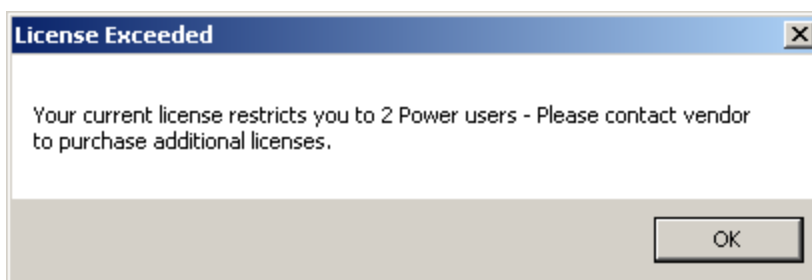
Tip If you are not sure where to find the Admin shared directory, go to an existing user's workstation, open Excel and click on the **Application Settings** button on the BizInsight ribbon and copy the path provided for the Administration Path.

2. In the .users file, add the Windows account name of the BizInsight user. For more information on the different user types, refer to the User Types section of the User Guide.



3. Save and close the file.

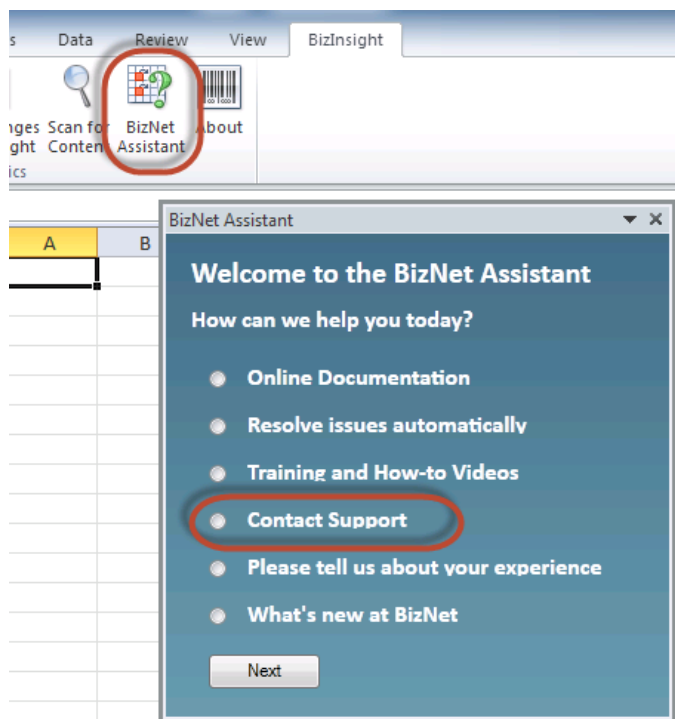
IMPORTANT As you add Windows account names to the .users files, add only as many as you have licenses. If you add more Windows account names than you have licenses or you have an extra line return in the file, users will get an error message similar to the following when they open Excel after BizInsight is installed.



If you are not sure how many licenses you have, open the .lic file that is in the Admin

shared directory with Notepad and check how many licenses are shown for the user type you are adding.

To purchase additional licenses, use the BizNet Assistant button to open a support ticket indicating that you need to purchase additional licenses.



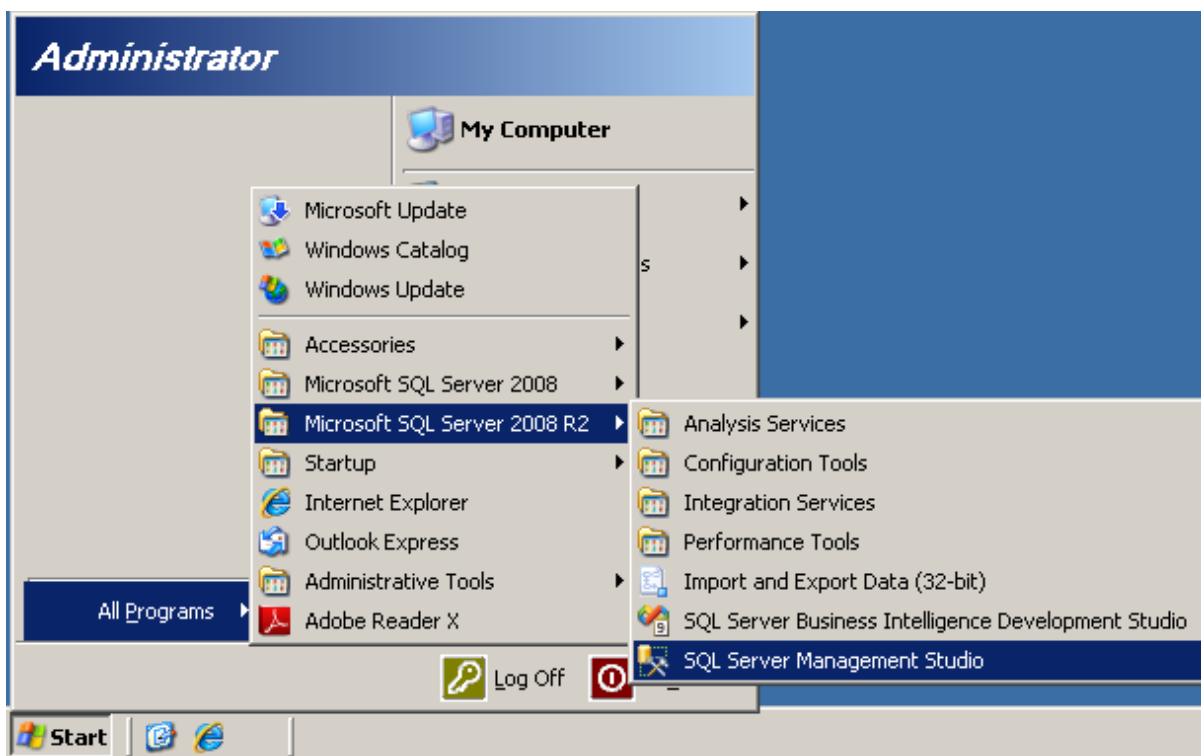
When you receive your new license, move your old license from the Administration Path shared directory and save the new license there. Do not rename the old license and leave it in the Administration Path; it must be removed from the directory in order for the new license count to take effect.

Step 3: Assign rights in SQL Server Security

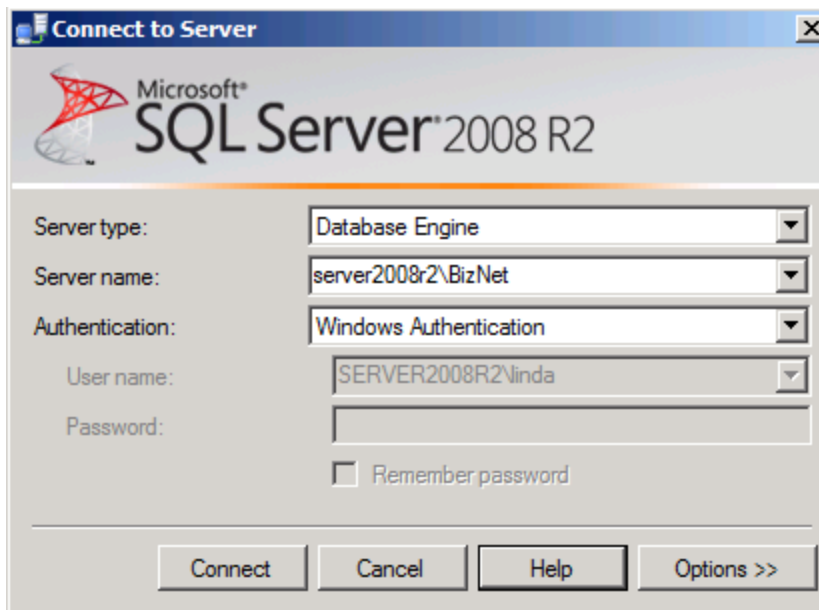
BizInsight users will need permissions to retrieve data from the accounting system database. If you did not use the Content Installer Admin tool, users will also need to be given rights to the SQL MetaData databases.

NOTE If you are managing SQL Server security with an Active Directory group, just add the new BizInsight user to that Active Directory group and go to the next step.

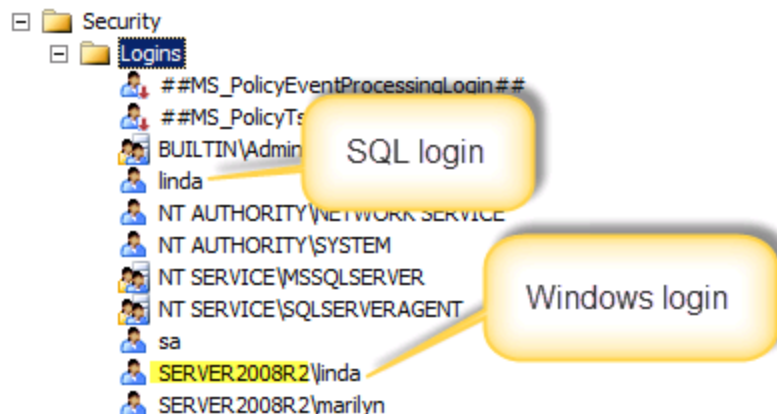
1. Click on **Start >Programs > Microsoft SQL Server Version > SQL Server Management Studio**.



2. The **Connect to Server** dialog will open. Connect to the SQL Server instance that hosts your accounting system database.

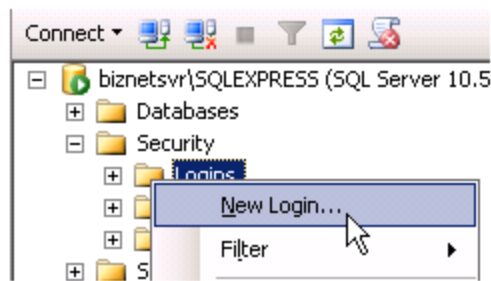


3. In the left pane, expand **Security**. Look for your existing users to determine whether they have been setup to use their Windows domain account or a SQL Server account. You can tell one from the other by the presence of the domain in front of the user name.



NOTE If the user's login already exists in SQL Server, right-click their login id and choose Properties. Then click [here](#) to jump to the User Mapping step.

4. Right-click on Logins and click **New Login**.



5. In the Login – New dialog box, enter the user’s name in the **Login name** field. If your existing users were setup with their Windows logins, click on **Search** to browse for an existing Windows login id. If your existing users were setup with a SQL account, type the new user’s login id and change the radio button to SQL Server authentication.

Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Script Help

Login name: YourDomain\davis Search...

☒ Windows authentication

☐ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☒ Enforce password expiration

☒ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential Add

Mapped Credentials

Credential	Provider
------------	----------

Remove

Default database: master

Default language: <default>

OK Cancel

Connection

Server: Server2003

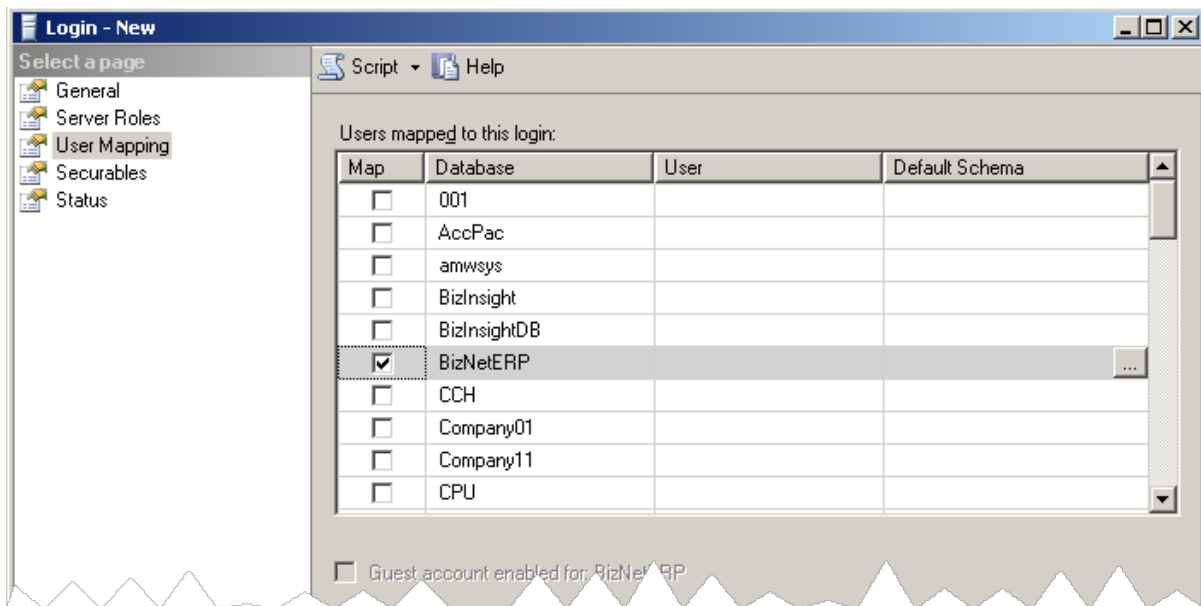
Connection: SERVER2003\Administrator

[View connection properties](#)

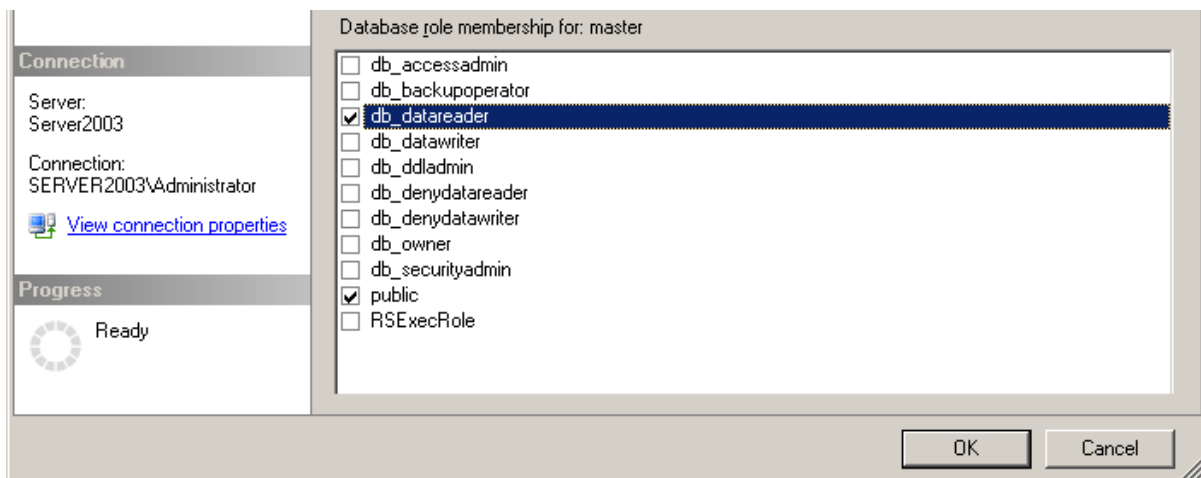
Progress

Ready

- Click on **User Mapping** in the left pane. Check the **Map** checkbox next to the accounting system database.

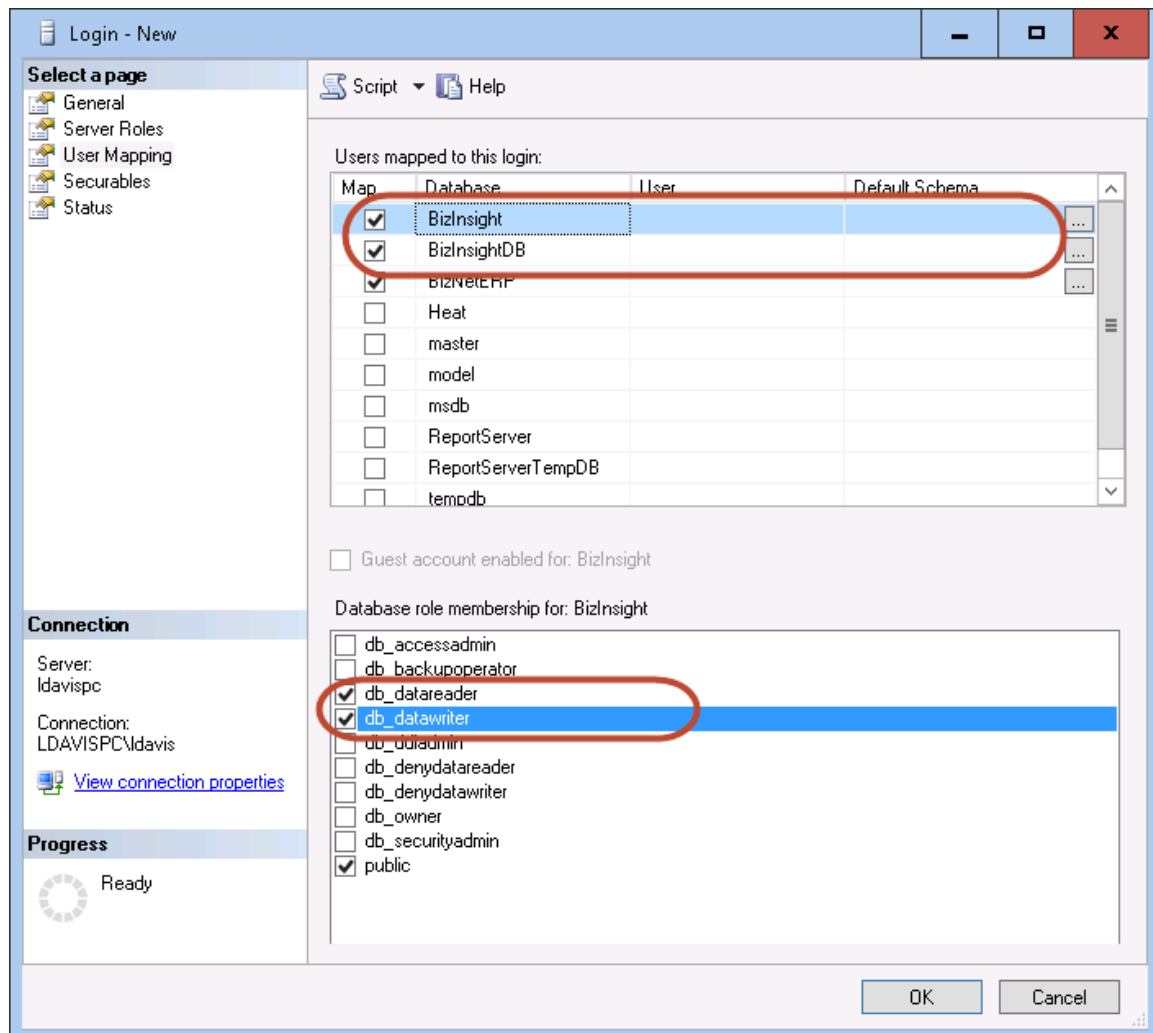


- Once the database is checked in the upper pane, check the **db_datareader** role membership in the bottom pane. Click **OK**.



- If the accounting system stores company data in separate databases, repeat the steps of checking the database and the **db_datareader** role for each company database.

9. If the SQL MetaData databases (BizInsight and BizInsightDB) are not checked, be sure to check both of them and give the user db_datareader and db_datawriter rights to those two databases.



Step 4: Assign rights in Reporting Services

This step probably has been addressed by the Content Installer Admin tool. In the event an error occurred while users were being assigned security rights or you did not use the Admin Tool to assign BizInsight security to the new user, follow these steps to assign them rights to the Reporting Services items.

NOTE If you are managing Reporting Services security with an Active Directory group, make sure the user is a member of that group and that group has been added to Reporting Services security.

All BizInsight users must have rights granted to them in Reporting Services. Reporting Services uses role-based security to secure access to items managed by the report server.

IMPORTANT Starting with the BizInsight build , the minimum pre-defined role necessary for a BizInsight user is Content Manager. A script is provided in the document titled "**Installing SQL Server and Reporting Services**" to create a custom role named "" that will assign only the minimum permissions required for the XMLFast feature.

SQL Server Reporting Services
New Role Assignment

Home | My Subscriptions | Site Settings

Search for:

Use this page to define role-based security for Home.

Group or user name:

Select one or more roles to assign to the group or user.

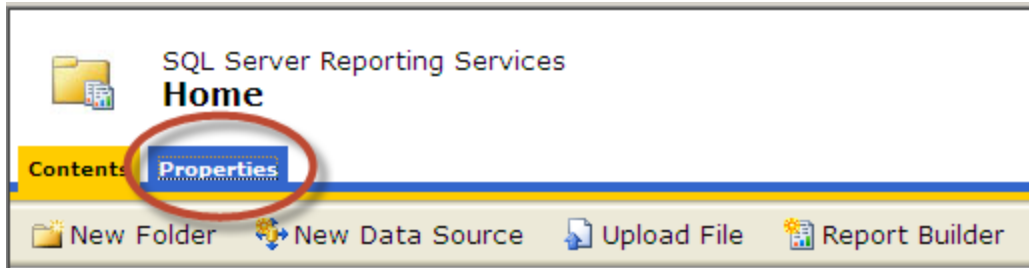
<input type="checkbox"/> Role	Description
<input type="checkbox"/> Browser	May view folders, reports and subscribe to reports.
<input type="checkbox"/> Content Manager	May manage content in the Report Server. This includes folders, reports and resources.
<input type="checkbox"/> My Reports	May publish reports and linked reports; manage folders, reports and resources in a users My Reports folder.
<input type="checkbox"/> Publisher	May publish reports and linked reports to the Report Server.
<input type="checkbox"/> Report Builder	May view report definitions.

OK Cancel New Role

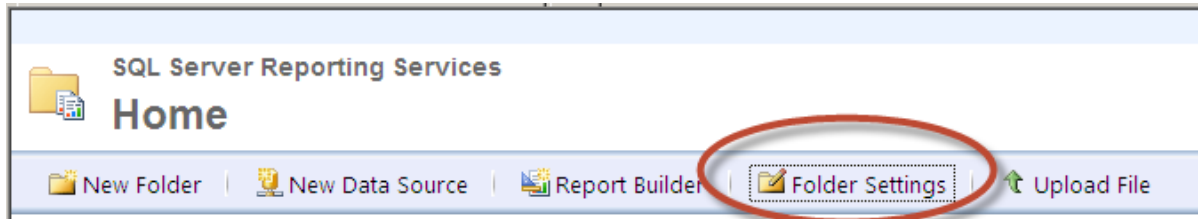
Reporting Services Security is accessed by browsing to the Reporting Services Report Manager URL (ex. http://servername/reports). Go to the Application Settings dialog of your currently working BizInsight user and copy the Reporting Services URL that is listed in the dialog. Modify the "reportserver" part of the URL to "reports" then paste into a browser.

IMPORTANT If Reporting Services is installed on a **Windows Server 2008 or higher** server and User Account Control ("UAC") is enabled, you must elevate your privileges when you start Internet Explorer. To do this, press **CTRL+Shift** and then right-click on Reporting Services Configuration Manager and select **Run as administrator**.

For SQL Server Reporting Services 2005 and 2008, go to the **Properties** tab:



For SQL Server Reporting Services 2008 R2, click on the **Folder Settings** button.



The following screenshot shows an example of a Reporting Service site with user security configured. The user named "linda" has been given Content Manager permissions.

Report Manager - Windows Internet Explorer

http://server2003/Reports/Pages/Folder.aspx?ItemPath=/&SelectedTabId=PropertiesTab

File Edit View Favorites Tools Help

★ Favorites ☆ Suggested Sites Free Hotmail Web Slice Gallery

Report Manager

SQL Server Reporting Services Home

✕ Delete | 👤 New Role Assignment

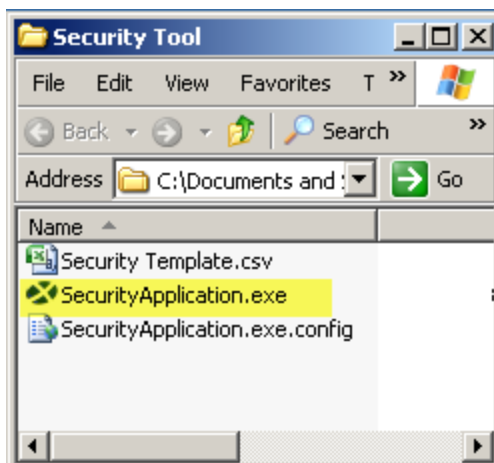
Security

<input type="checkbox"/>	Group or User ↓	Role(s)
<input type="checkbox"/>	Edit BUILTIN\Administrators	Content Manager
<input type="checkbox"/>	Edit SERVER2003\Administrator	Content Manager
<input type="checkbox"/>	Edit SERVER2003\aeinstein	Content Manager
<input type="checkbox"/>	Edit SERVER2003\cclay	Content Manager
<input type="checkbox"/>	Edit SERVER2003\epicuser	Content Manager
<input type="checkbox"/>	Edit SERVER2003\epresley	Content Manager
<input type="checkbox"/>	Edit SERVER2003\fsinatra	Content Manager
<input type="checkbox"/>	Edit SERVER2003\ldavis	Content Manager
<input type="checkbox"/>	Edit SERVER2003\linda	Content Manager
<input type="checkbox"/>	Edit SERVER2003\olivier	Content Manager
<input type="checkbox"/>	Edit SERVER2003\mmonroe	Content Manager

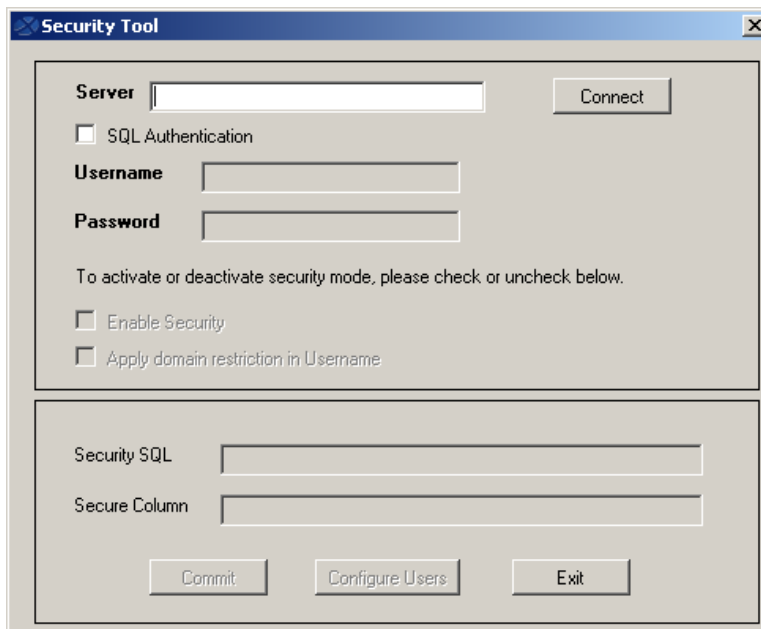
Step 5: Add User to Column Based Security

If your company has implemented the Column Based Security feature, you will need to specify the items to which this user will be restricted. The Security Tool for BizInsight is an application that activates or deactivates column security and configures restriction for user access. When the column based security mode is activated, all content modules installed on the server are impacted. See " BizInsight Column Based Security Overview" on page 86 for more information about Column Based Security.

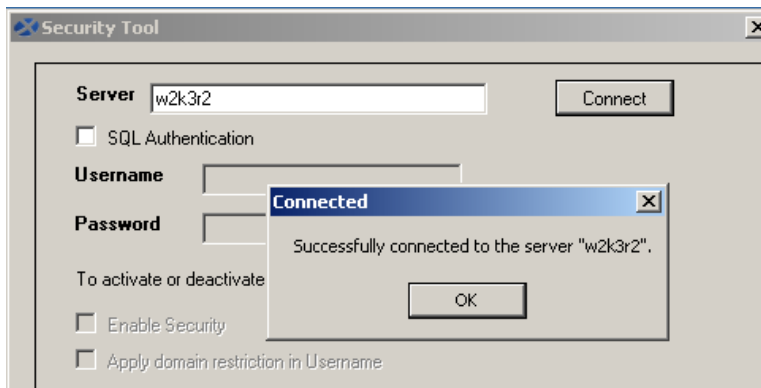
1. If you have not already downloaded the BizInsight Tools.zip., log into the BizNet Software portal (<http://biznet.flexnetoperations.com>) and download the file. You will find the tools with the BizInsight download file.
2. Extract the contents and open the Security Tool folder..
3. Double-click the **Security Application.exe** to launch the Security Tool.



- The Security Tool dialog will open.



- In the **Server** field, type in the Server name and, if applicable, the instance name for the SQL Server that hosts the SQL metadata databases (BizInsight and BizInsightDB). The connection will be made using Windows Authentication by default. Check the **SQL Authentication** checkbox to switch to SQL credentials and supply those credentials in the Username and Password fields. Click **Connect**.



- If the **Enable Security** checkbox is not checked, security is not enabled and you can close the tool.

Security Tool

Server: server2008r2 [Connect]

☐ SQL Authentication

Username: []

Password: []

To activate or deactivate security mode, please check or uncheck below.

☐ Enable Security

☐ Apply domain restriction in Username

Report Server URL: []

Format: "http://server/reportserver"

7. Type in the user's Windows login id in the Username field.

☒ Enable Security

☐ Apply domain restriction in Username

	Username	Value
..	linda	
*		

If the **Apply domain restriction in Username** checkbox is checked be sure to provide the domain name for the Username field.

☒ Enable Security

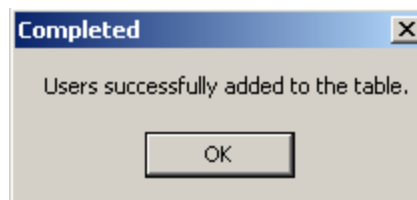
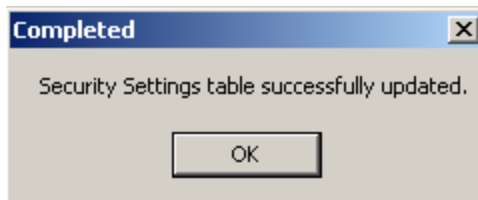
☒ Apply domain restriction in Username

	Username	Value
..	domain\linda	
*		

8. Type in the Values to which the user will be denied access. Separate multiple values with commas.

<input checked="" type="checkbox"/> Enable Security <input checked="" type="checkbox"/> Apply domain restriction in Username		
	Username	Value
	domain\linda	Epic01.Epic03
*		

9. When all usernames and values have been entered, click the **Commit** button. The application will commit the changes to the ColumnSecurity table. Click **OK** to the next two messages and the Dialog will update and display rows for each username/value combination.



	Username	Value
▶	Albert	Epic01
	Marilyn	Epic01
	Marilyn	Epic03
	Frank	Epic06
*		

Buttons: Import File, Delete Row(s), Commit, Back, Exit

10. Use the **Delete Row(s)** button to remove any entries that are not wanted. Be sure to highlight the entire row to be deleted.

	Username	Value
	Albert	Epic01
	Marilyn	Epic01
▶	Marilyn	Epic03
	Frank	Epic06
*		

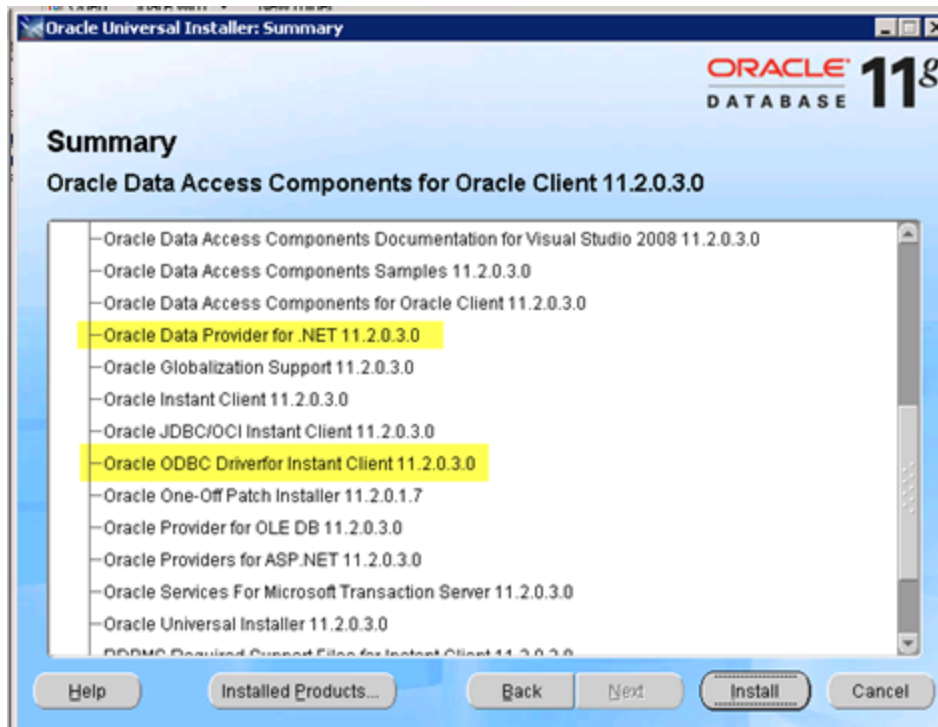
Buttons: Import File, Delete Row(s), Commit

11. Click **Exit** to close the tool.

For security to be fully implemented, each BizInsight workstation must be configured to use SQL metadata databases. This is covered in the section titled "Configure BizInsight" later in this guide.

Step 6: Install Oracle Data Access Components (ODAC)

If your accounting system is using an Oracle database, you must install the Oracle ODBC driver and ODP.Net on each client workstation in order for BizInsight to be able to retrieve data from the Oracle database. If your accounting system does not use an Oracle database, this step can be skipped.



The version shown in the screenshot is for illustration only.
Install the ODAC version appropriate for your Oracle database



IMPORTANT

When installing the Oracle Client, it is insufficient to install the Runtime Engine as that does not install the Oracle ODBC driver.

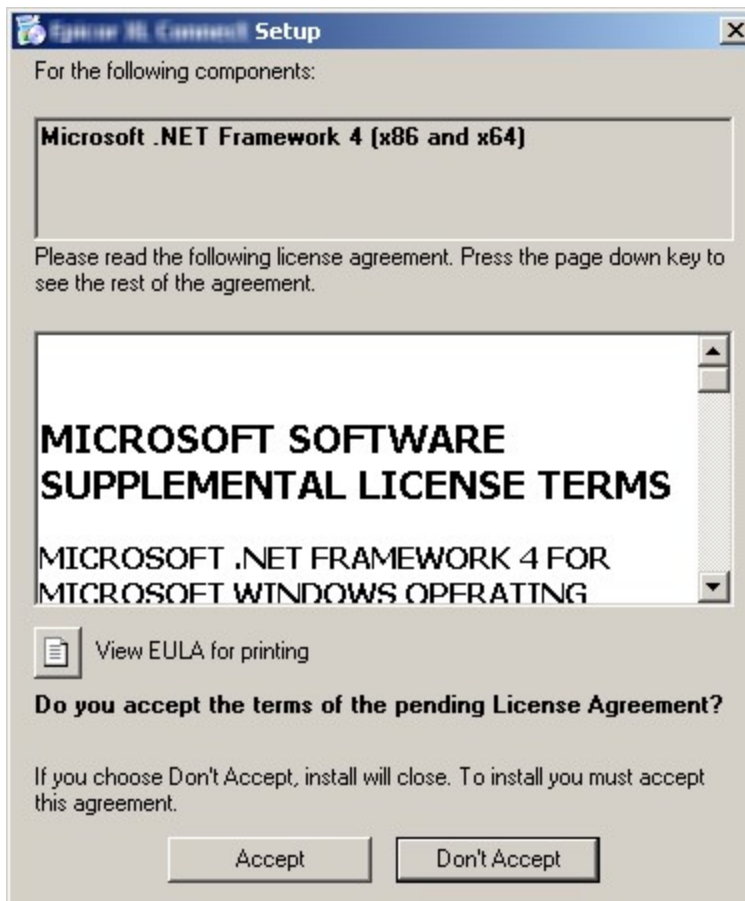
Step 7: Install BizInsight

IMPORTANT If you are using BizInsight in a Terminal Services/Citrix environment, do not perform the following installation steps because BizInsight is already installed on the server. Instead, log onto the Terminal Services/Citrix server as the new user, browse to the reg5 sub-directory of the BizInsight installation folder and double-click the file named "**Register BizInsight for Excel xxxx OnDemand.bat**". Move to the next step, "Configure BizInsight".

1. Locate the BizInsight product installation files that you downloaded from the portal site and extract the contents.
2. Extract the .zip contents to any directory that is accessible from the client workstation.
3. Double-click the **Setup.exe**.

NOTE As of the 5.0.35.2 release, there is a single Setup.exe for all supported Office versions.

4. The installation will check to see if Microsoft .Net Framework 4.0 is installed. If not installed, the following dialog will display. Click **Accept**.



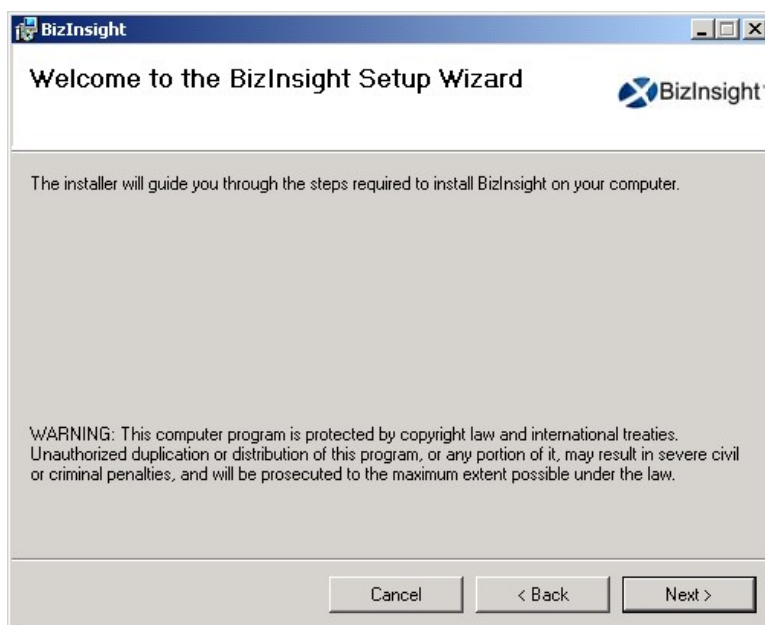
5. The installation will then check to see if the Microsoft Office Primary Interop assemblies for the installed Excel version are installed as well as a specific Microsoft Update that is necessary for proper Excel add-in functionality. If not found, the following dialog will display. Click **Install**.



6. The splash dialog will open. Click **Next** to continue.



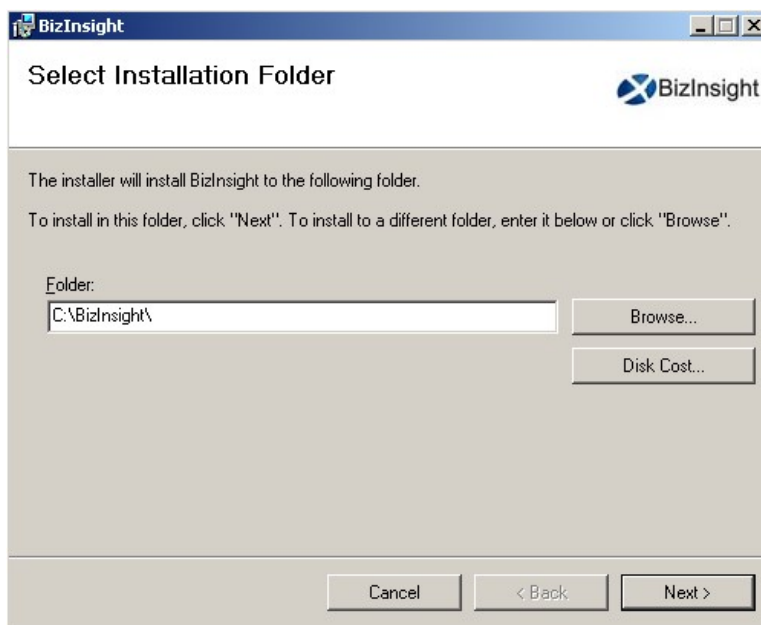
7. The Welcome dialog will open. Click **Next** to continue.



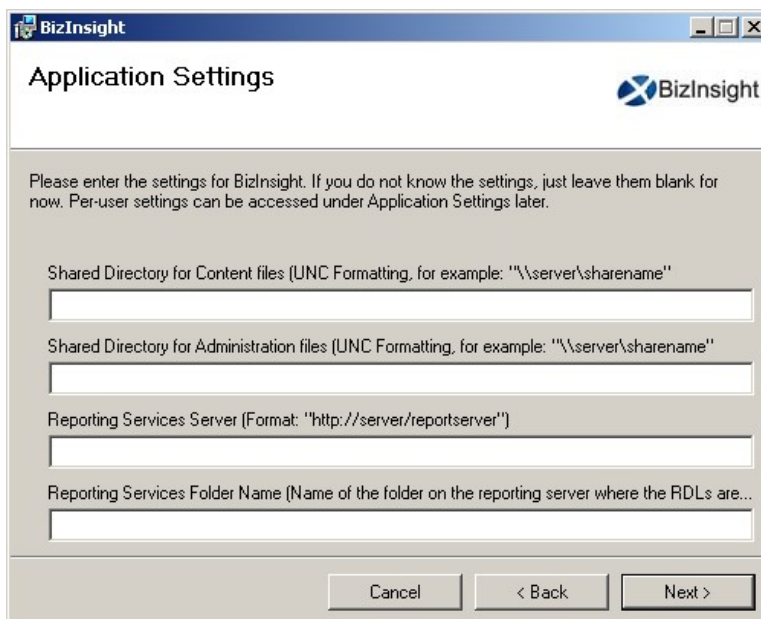
8. The **License Agreement** dialog will open. Read through the agreement and if you agree with the terms, click the **I agree** radio button and then click **Next**.



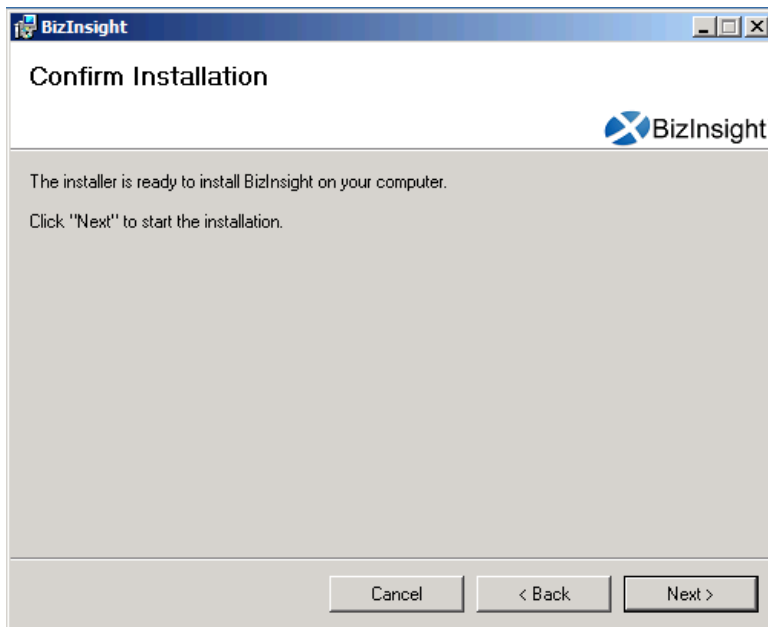
9. Accept the default installation directory or browse to a location of your choice. Click **Next**.



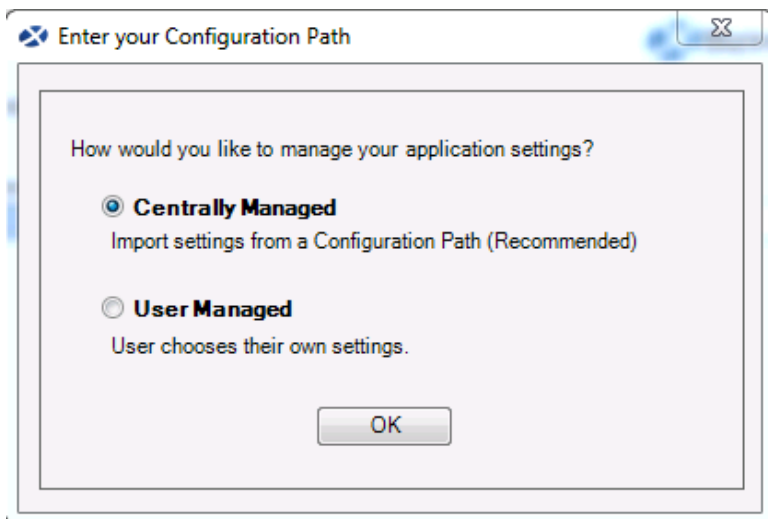
10. If you are installing a BizInsight version older than 5.0.35.1, the installer will prompt for some key paths. Leave the fields blank and click **Next**. You will enter these values in the next section.



11. Click **Next** at the **Confirm Installation** dialog.

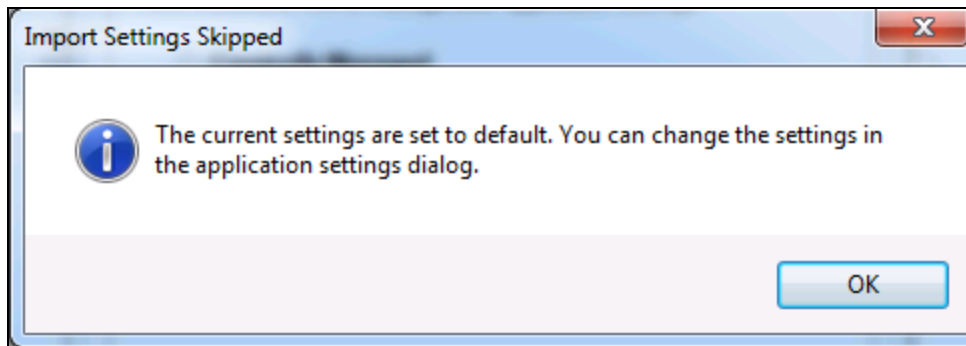


12. When installing BizInsight versions 5.0.35.1 or higher, the **Enter your Configuration Path** dialog will open. If you have an app.config file produced by a Content Installer in your Configuration Path, leave the default option. Click **OK**.

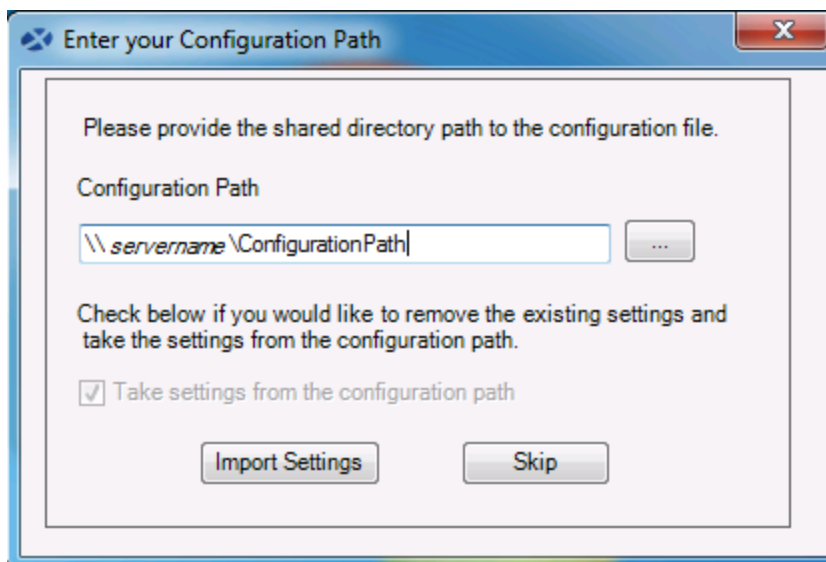


If you do not have a Content Installer created app.config file, choose the **User Managed** radio button to proceed. You will need to supply the key paths when configuring BizInsight for the user. When you click OK, the Import Settings Skipped dialog will open.

Click **OK**.

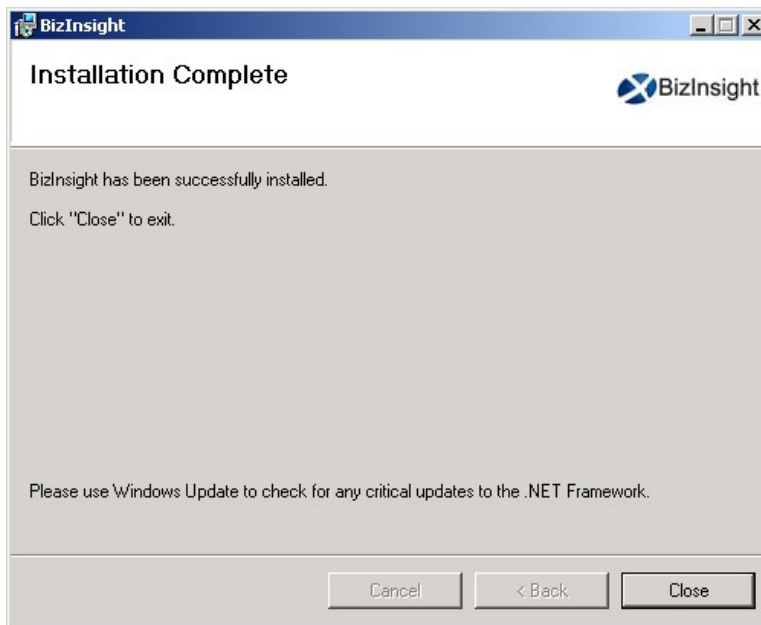


13. If the Centrally Managed option was selected, click the Browse button and browse to the Configuration Path shared directory.



Click **Import Settings**.

14. Once the installation completes, click **Close**.

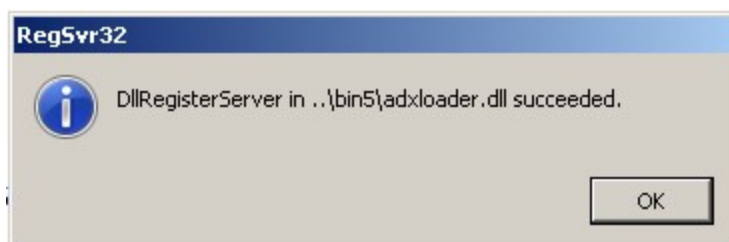
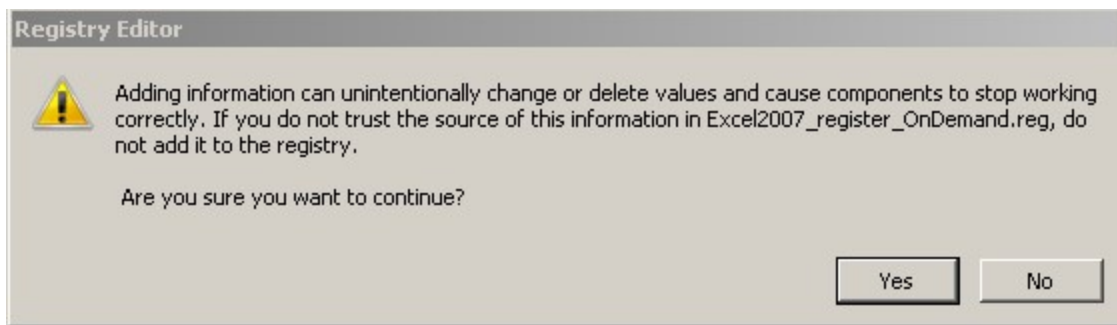


Installing BizInsight for the Non-Administrative User

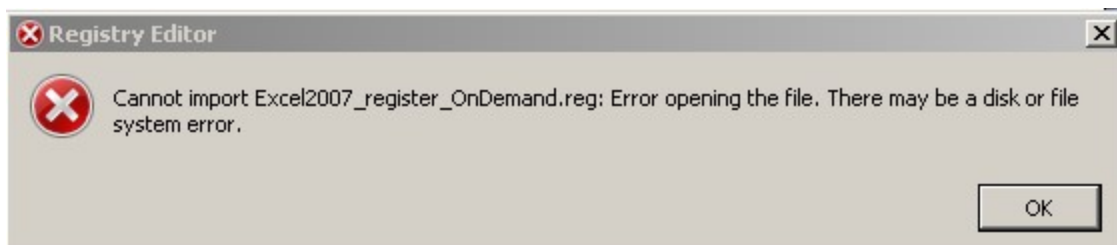
If you have installed BizInsight while logged in as a different login than the BizInsight end user, you will need to perform the following additional steps in order to get BizInsight functioning for this user.

1. After completing all of the preceding steps to install BizInsight, log out of the client workstation and log back in as the BizInsight user.
2. Open Windows Explorer and browse to the reg5 subdirectory of the BizInsight local directory.
3. Double-click the file named "**Register BizInsight for Excel xxxx OnDemand.bat**", where "xxxx" is the Excel version (2003, 2007, 2010 or 2013).

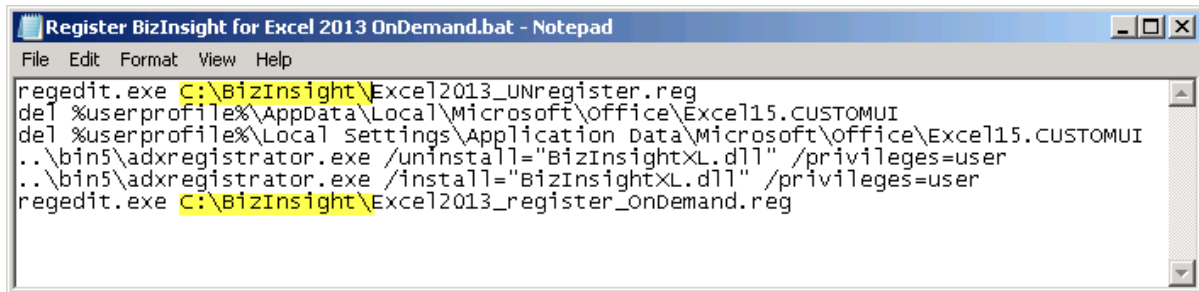
4. If the workstation is running Windows 7 with User Account Control (“UAC”) enabled, click Yes to all UAC pop-ups. Click Yes or OK to all dialogs that open.



IMPORTANT If you get the following error when running the .bat file, you must edit the file named “Register BizInsight for Excel xxxx OnDemand.bat” to add the file directory path to each regedit.exe line.



To edit the "Register BizInsight for Excel xxxx OnDemand.bat", open it with Notepad and add the file directory path to each regedit.exe entry in the file. For example:



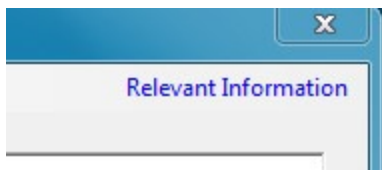
```
Register BizInsight for Excel 2013 OnDemand.bat - Notepad
File Edit Format View Help
regedit.exe C:\BizInsight\Excel2013_UNregister.reg
del %userprofile%\AppData\Local\Microsoft\Office\Excel15.CUSTOMUI
del %userprofile%\Local Settings\Application Data\Microsoft\Office\Excel15.CUSTOMUI
..\bin5\adxregistrator.exe /uninstall="BizInsightXL.dll" /privileges=user
regedit.exe C:\BizInsight\Excel2013_register_OnDemand.reg
```

5. When the .bat file completes, start Excel and continue with the next steps.

Step 8: Configure BizInsight

1. If you used the Content Installer to create an app.config file to use for Centrally Managed settings, you can skip this step.

You will need to know the paths for the BizInsight implementation. Go to the server and start the Content Installer. Click on the Relevant Information link and make a note of the values shown.



If you cannot find the Content Installer on the server, you can get the necessary information from an existing BizInsight workstation, if one exists. Open Excel on a workstation where BizInsight is installed, click on the **Application Settings** button on the BizInsight ribbon and copy the values provided for the **Configuration Path**, the **Administration Path**, the **Default Reporting Services Server** and the **Default Reporting Services Folder Name** fields.

Application Settings

☐ Use settings from Configuration Path.

BizInsight Settings

Configuration Path [Configure SQL](#)

...

Folder or network share where the BizInsight.biz and BizInsightDB.biz are stored.

Administration Path

...

Network share where your license file and user files are stored .

Options

<input checked="" type="checkbox"/> Enable Formula Editor Pop-up	<input type="checkbox"/> Persist SQL Authentication
<input checked="" type="checkbox"/> Enable Refresh Timer	Clear Credentials
<input type="checkbox"/> Enable Cache Information Dialog	Local Content Path
<input checked="" type="checkbox"/> Enable XMLFAST	Calculation Settings
<input type="checkbox"/> Enable Startup Messages	Account Definitions
<input type="checkbox"/> Use Advanced Expression Editor	

Reporting Services Default Settings

Default Reporting Services Server

Format: "http://server/reportserver"

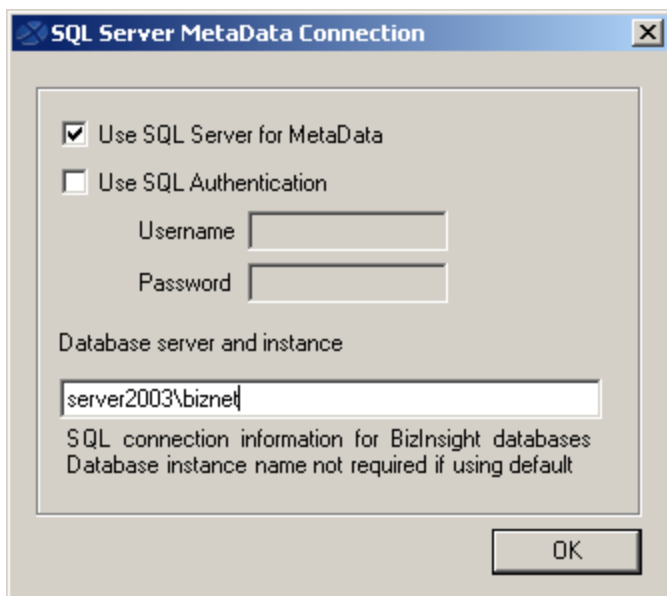
Default Reporting Services Folder Name

Full name of the folder on the reporting services server where the RDLs are deployed.

[OK](#)

Click on the **Configure SQL** button to see if the client workstation is configured for SQL

metadata databases. If this dialog is configured, make a note of the values.



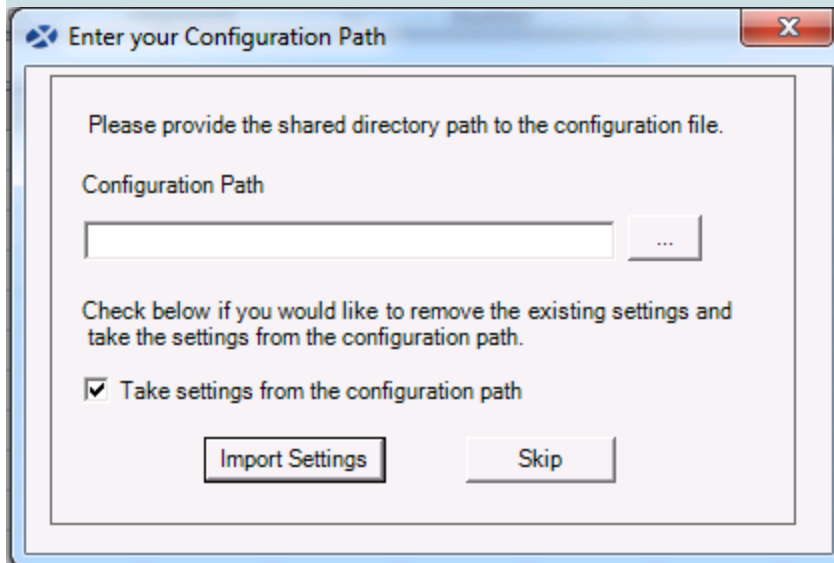
2. While logged in as the BizInsight end user, open Excel.

The next steps depend on whether you chose the Centrally Managed option at the end of the BizInsight installation or chose to manage your settings at the user level. Click [here](#) to jump to the Centrally Managed steps.

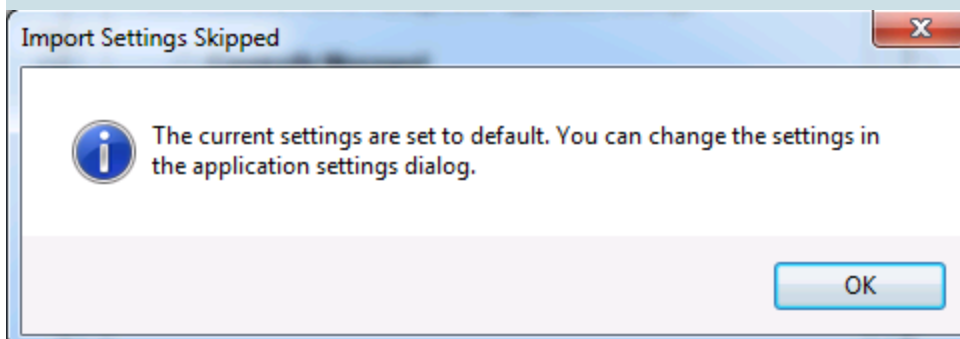
If you installed an older BizInsight version that prompted for these paths during installation, follow the User Managed Settings Steps.

User Managed Settings Steps (blue background)

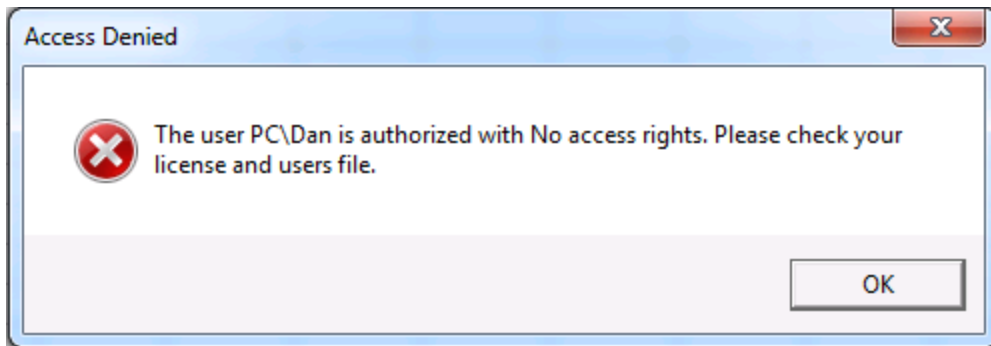
3. If you receive the following dialog, click **Skip**.



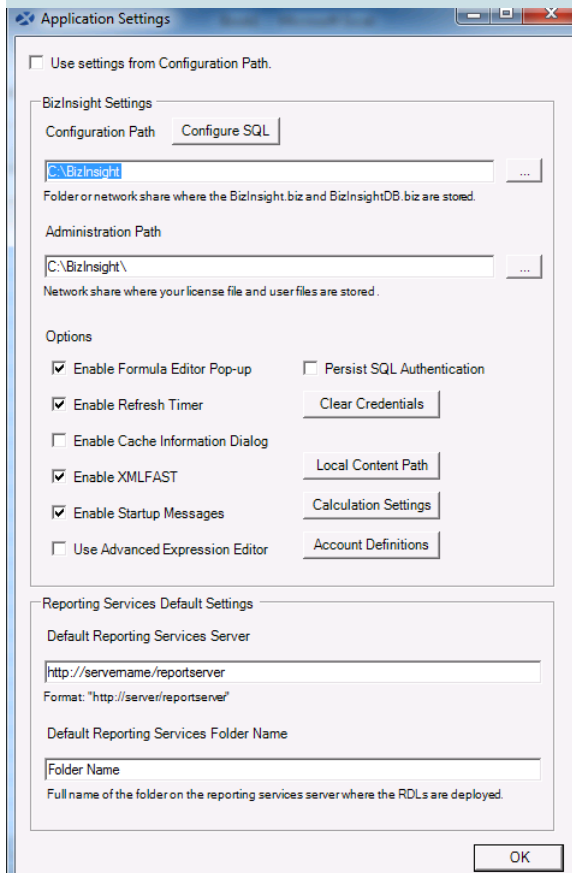
Click **OK** to the next message regarding the use of default settings.



If you receive the following error, go back to the server and grant the user BizInsight security rights, see "Assign BizInsight Security to Users" on page 92.



4. The Application Settings dialog will open. If it does not open, click on the Application Settings button on the BizInsight ribbon.



Perform the following steps:

a. Provide Essential Paths

You must provide values for the **Configuration Path**, the **Administration Path**, the **Default Reporting Services Server** and the **Default Reporting Services Folder Name** fields.

☐ Use settings from Configuration Path.

BizInsight Settings

Configuration Path

C:\BizInsight

Folder or network share where the BizInsight.biz and BizInsightDB.biz are stored.

Administration Path

C:\BizInsight\

Network share where your license file and user files are stored.

Options

☒ Enable Formula Editor Pop-up ☐ Persist SQL Authentication (Session Only)

☒ Enable Refresh Timer ☒ Enable Startup Messages

☐ Enable Cache Information Dialog

☒ Enable XMLFAST

☐ Use Advanced Expression Editor

Reporting Services Default Settings

Default Reporting Services Server

http://servename/reportserver

Format: "http://server/reportserver"

Default Reporting Services Folder Name

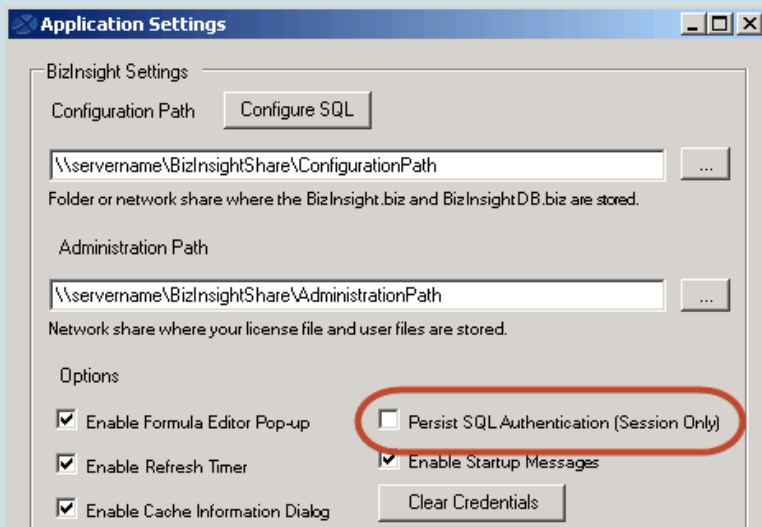
Folder Name

Full name of the folder on the reporting services server where the RDLs are deployed.

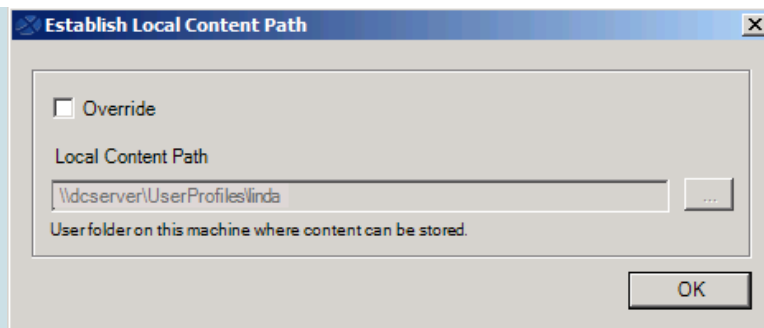
You should have looked up these values at the start of this section.

- b. **SQL Credentials Steps** (skip if not using SQL credentials for data retrieval from the Accounting database)

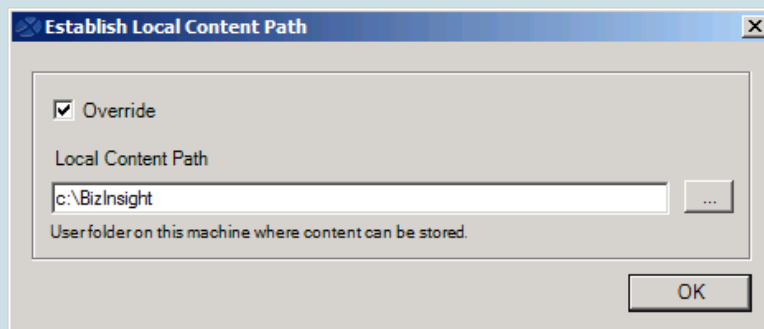
If you configured the Reporting Services data source to use SQL credentials during content deployment, check the **Persist SQL Authentication** checkbox.



- c. Click on the Local Content button. If the default path displayed is not a local directory, click on the Override checkbox and change the path to a directory that resides on the local computer, C:\BizInsight is suggested.



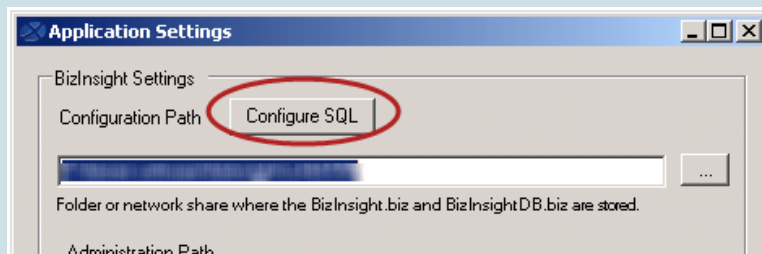
Re-directed profile directory



Override to local directory

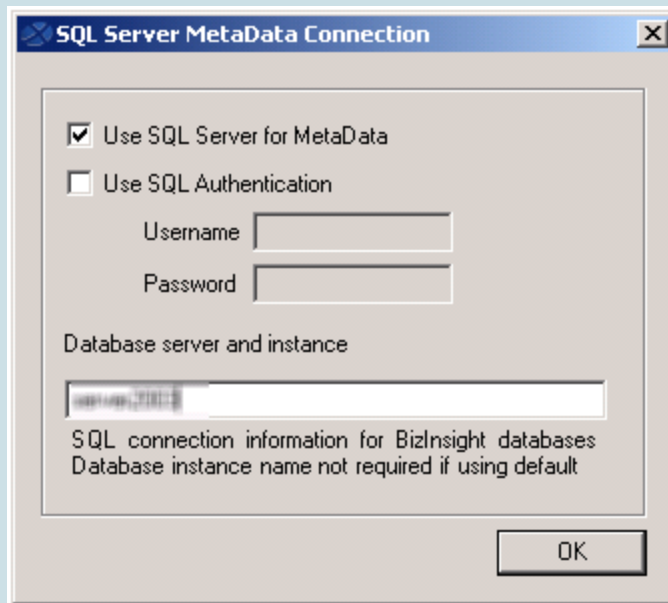
d. **SQL MetaData Databases and Column Security Steps**

If the BizInsight SQL metadata databases (BizInsight and BizInsightDB) were implemented during the server setup, click on the **Configure SQL** button. If the **Application Settings** dialog does not have this button, BizInsight is not the right version. You need to uninstall and install the most current BizInsight version.

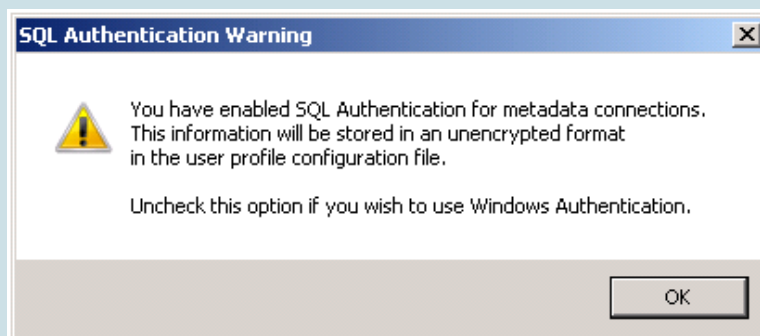


IMPORTANT This step is essential to complete Column Based security configuration. See " BizInsight Column Based Security Overview" on page 86 for more information about this optional security feature.

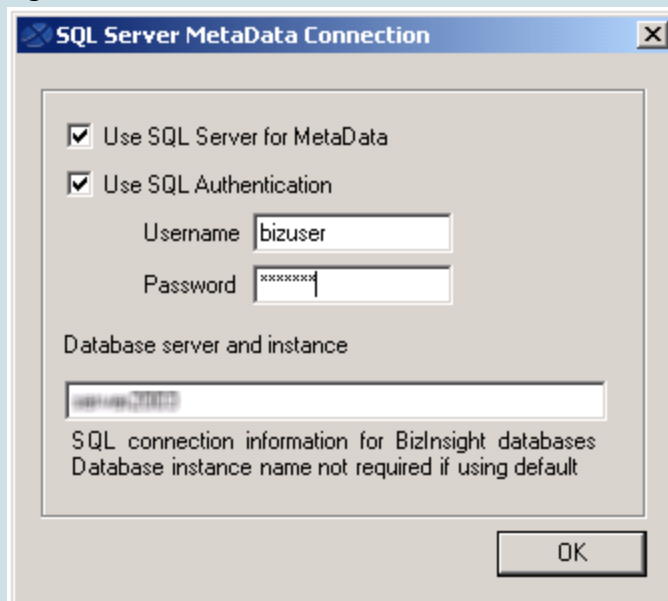
- i. Check the **Use SQL Server for MetaData** checkbox and enter the SQL Server name, and instance name if applicable, where the BizInsight SQL databases (BizInsight and BizInsightDB) are located. The format should be *servername\instancename*.



- ii. If users will be connecting to the SQL metadata databases using SQL authentication, check the **Use SQL Authentication** checkbox. You will get the following Warning message indicating that the credentials provided will be stored in clear text in a configuration file in the user's profile.

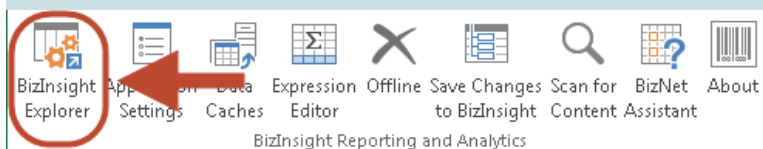


Click **OK** and enter a valid SQL login and password with appropriate rights to the SQL MetaData databases. Click **OK**.



IMPORTANT This dialog allows you to use a different method of connectivity to the BizInsight MetaData databases than for the accounting system database.

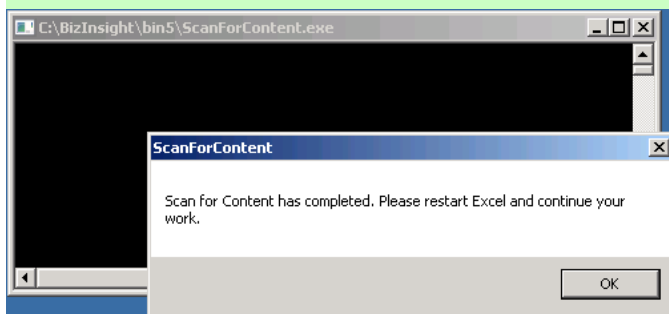
- e. Close the **Application Settings** dialog.
5. Re-start Excel.
6. Click on the BizInsight tab and then click on the BizInsight Explorer button to load the Navigation Pane.



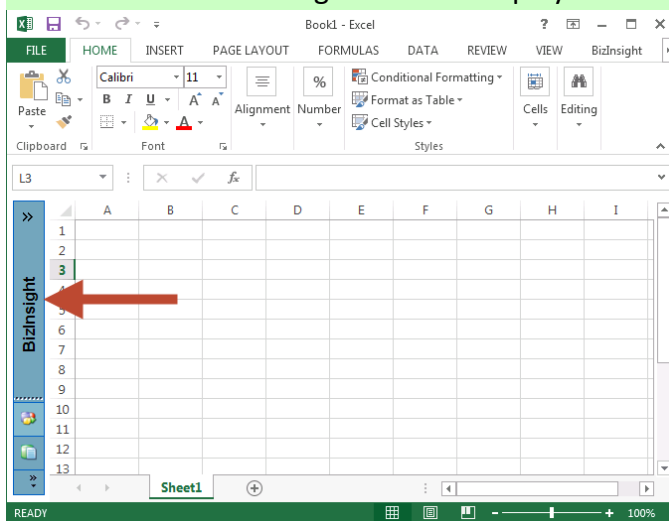
7. Skip to the next white background step.

Centrally Managed User Settings (green background)

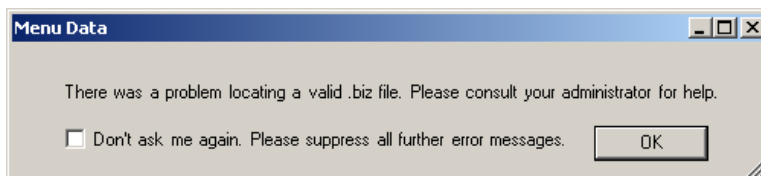
8. If you are using Centrally Managed settings, you will see Scan for Content run when you first open Excel. Click **OK** and restart Excel.



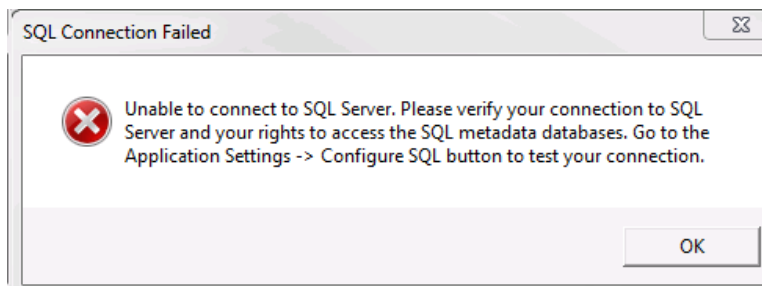
9. You should see the Navigation Pane display on the left side in Excel.



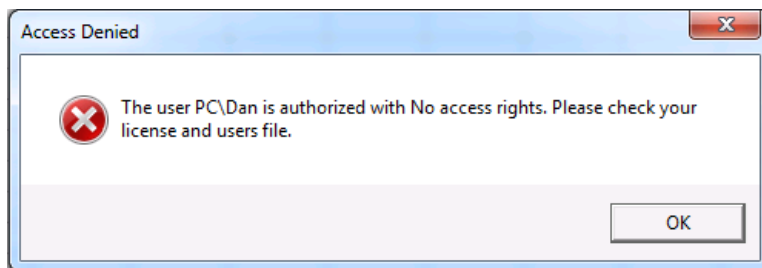
10. If you receive the following error, go back to your server and make sure all of the configuration changes have been made for XMLFast (see "CheckTCP/IP, SQL Browser and Firewall Exceptions" on page 60) and make sure the end user has the db_datareader and db_datawriter permissions to the SQL metadata databases (BizInsight and BizInsightDB).



Click **OK** to this message as well as the one that follows:



If you receive the following error, go back to the server and grant the user BizInsight security rights, see "Assign BizInsight Security to Users" on page 92.



You are now ready to test the installation. Proceed to "Verify the BizInsight Installation".

Step 9: Verify the BizInsight Installation

Locate an existing BizInsight report to use to verify the installation. Open the report, right-click anywhere in the report and choose **BizNet Refresh**.



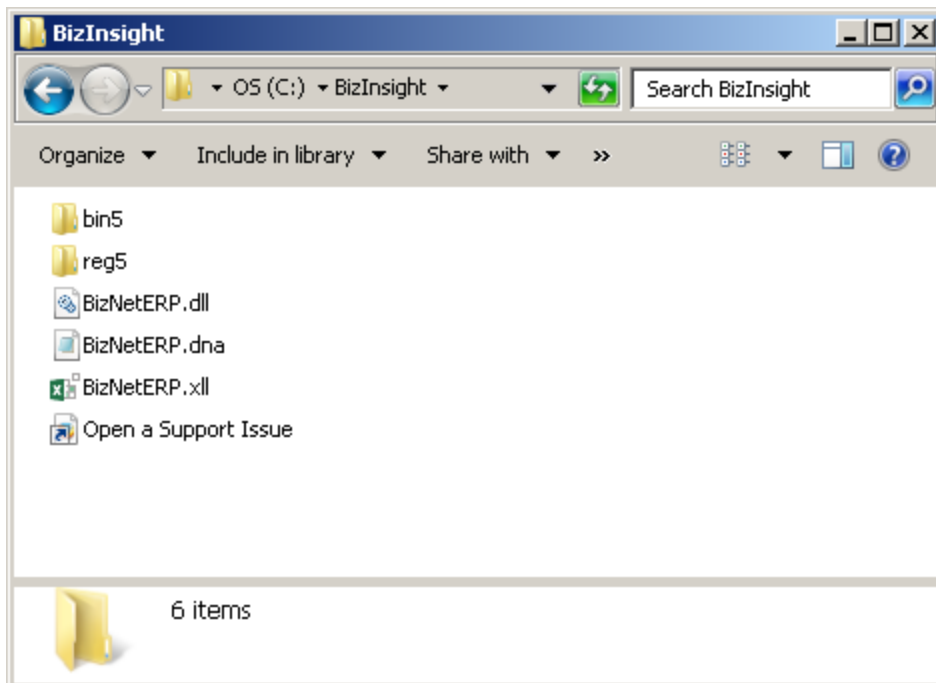
Appendices

Manually Installing BizContent Add-ins	49
CheckTCP/IP, SQL Browser and Firewall Exceptions	60
BizInsight Column Based Security Overview	86
Assign BizInsight Security to Users	92

Manually Installing BizContent Add-ins

If you are using a BizInsight version that is older than , you will need to register the BizContent add-ins manually in Excel. BizNet Software recommends upgrading to the latest BizInsight version but if that is not possible, perform the following steps:

1. Browse to the BizInsight shared directory and copy the content add-in files (.dll, .xll and .dna) to the directory to which you installed the BizInsight client. If you are using separate config and admin folders, the client add-in files will be in the config folder.



The remaining steps vary based on the Office version installed:

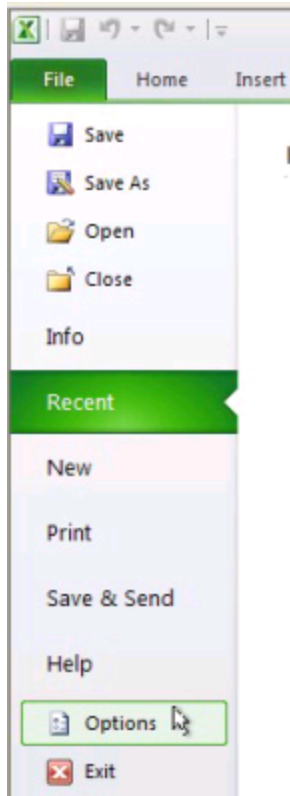
[Office 2010/2013 steps](#)

[Excel 2007 steps](#)

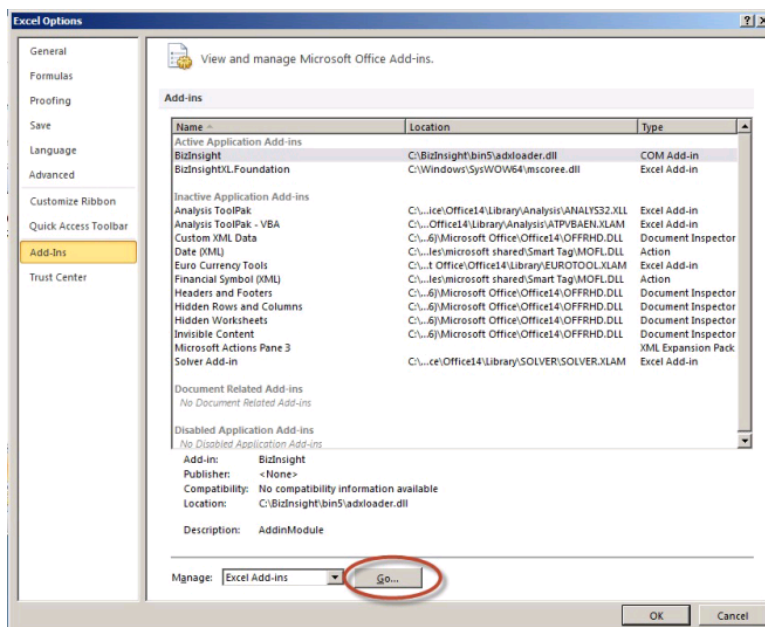
[Excel 2003 steps](#)

Excel 2010/2013

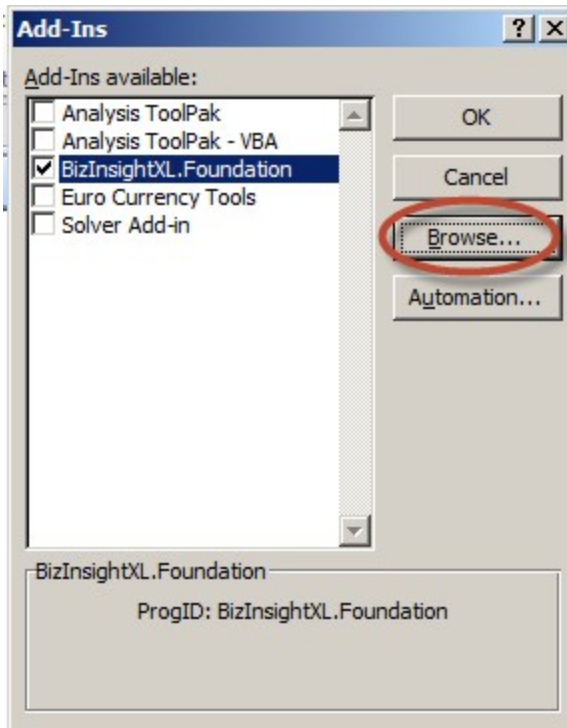
1. Click on **File > Options**.



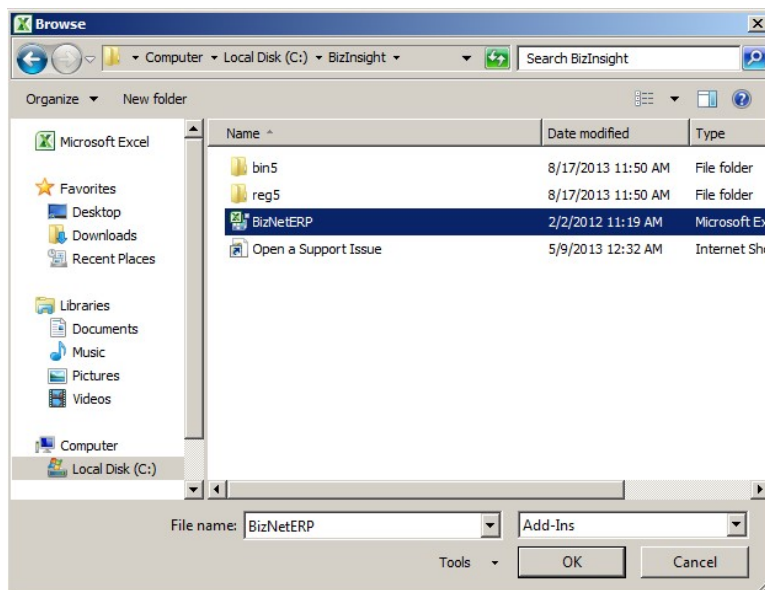
- Click on **Add-ins** in the left pane and then click on **Go** at the bottom on the right pane.



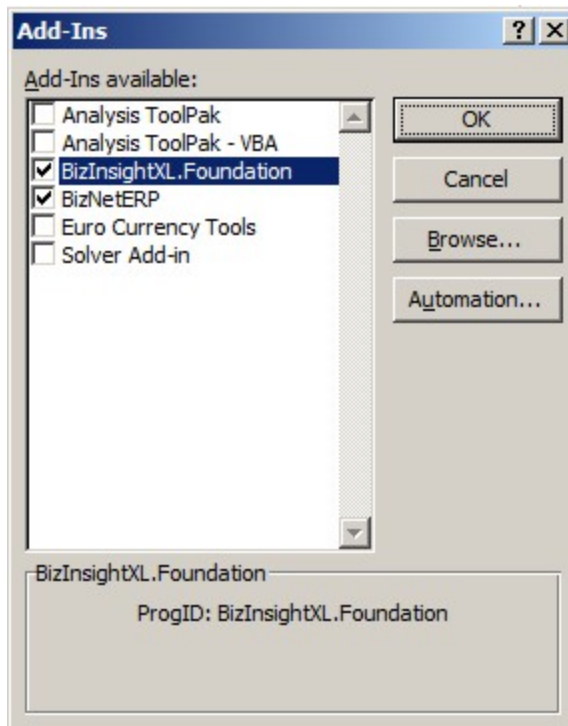
2. In the Add-ins dialog, click on the **Browse** button.



3. Browse to the directory to which you installed BizInsight and select the .xll file in that directory. Then click **OK**.



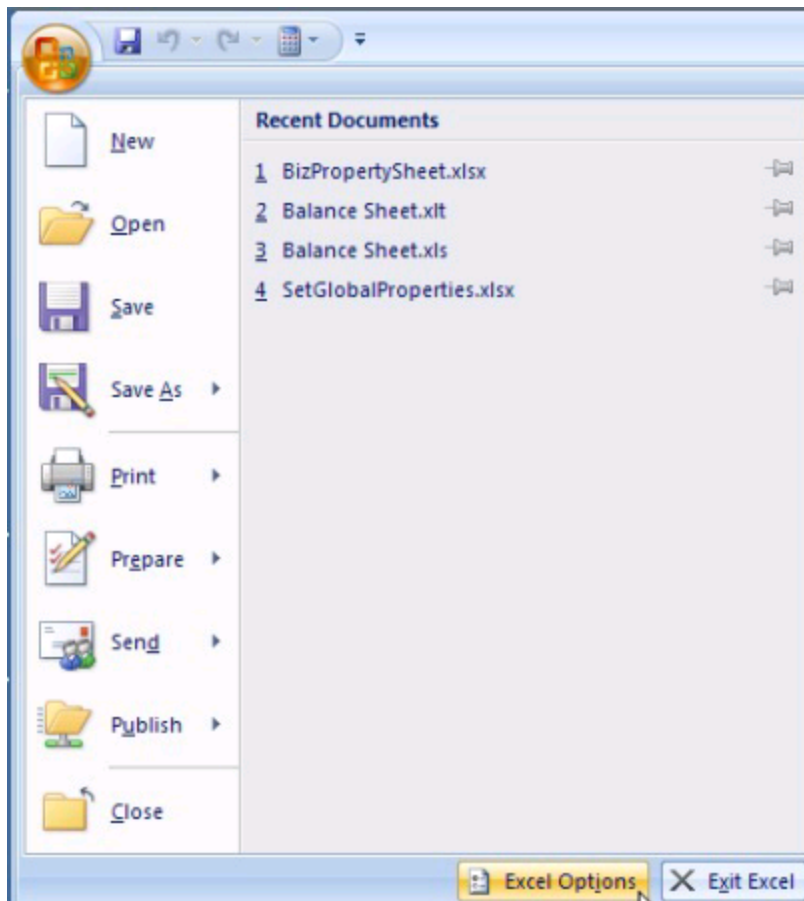
The Add-ins dialog should now look like the following:



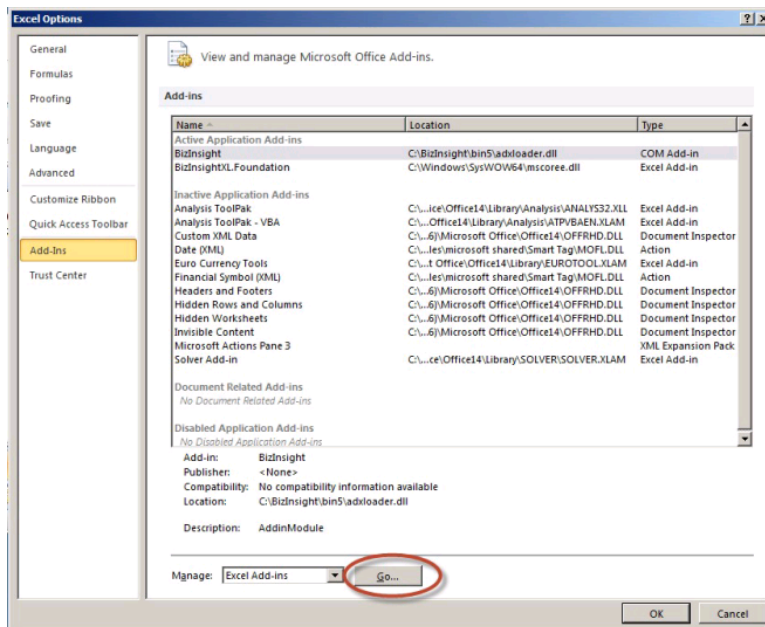
4. Click **OK**.

Excel 2007

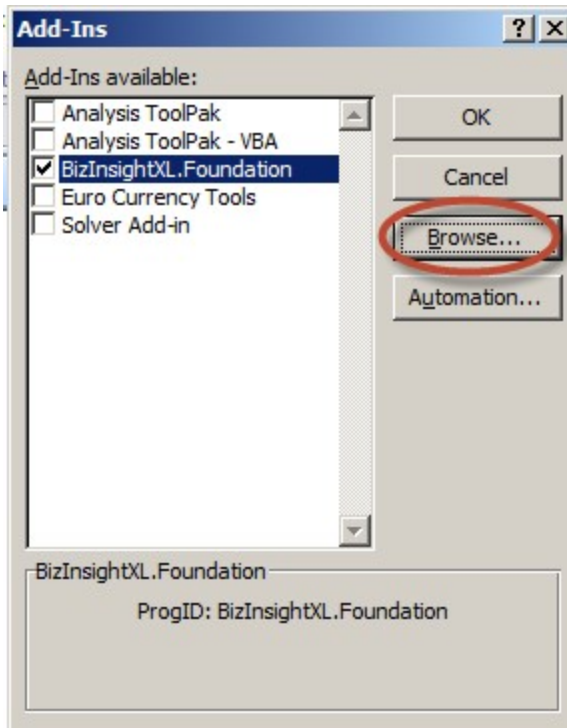
1. Click on the **Office** button and then click on the **Excel Options** button.



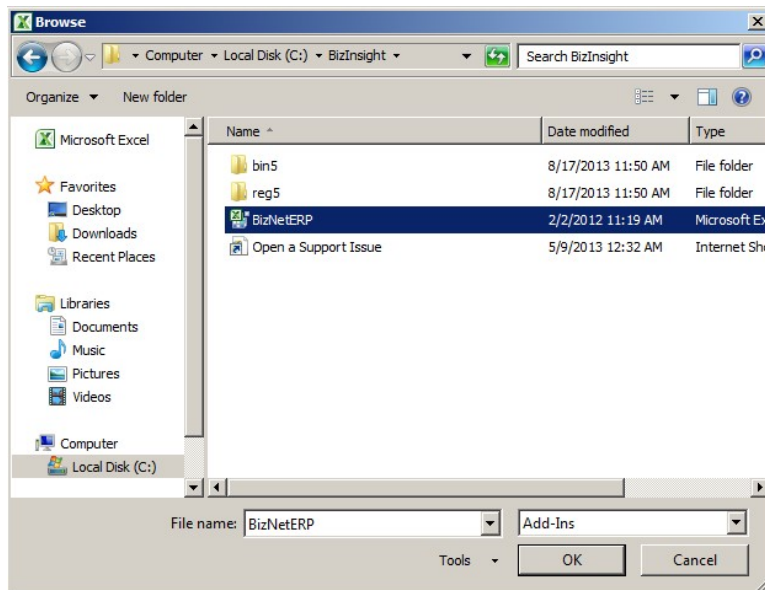
2. Click on **Add-ins** in the left pane and then click on **Go** at the bottom on the right pane.



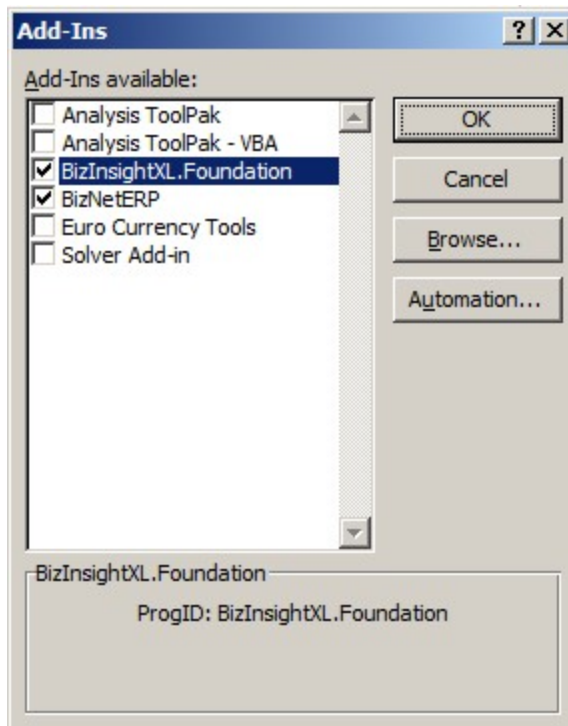
3. In the Add-ins dialog, click on the **Browse** button.



4. Browse to the directory to which you installed BizInsight and select the .xll file in that directory. Then click **OK**.



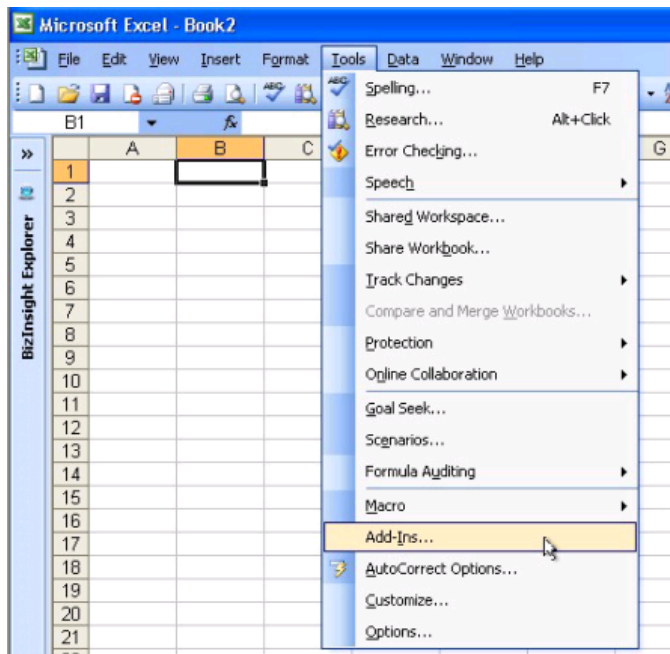
The Add-ins dialog should now look like the following:



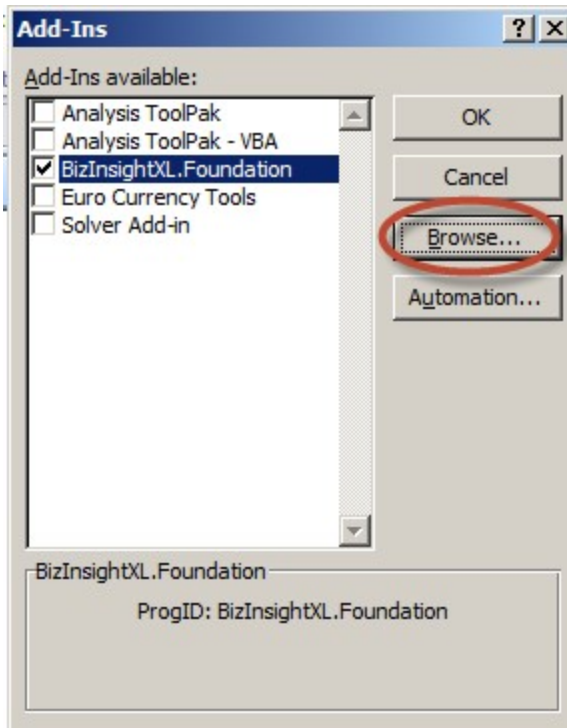
5. Click **OK**.

Excel 2003

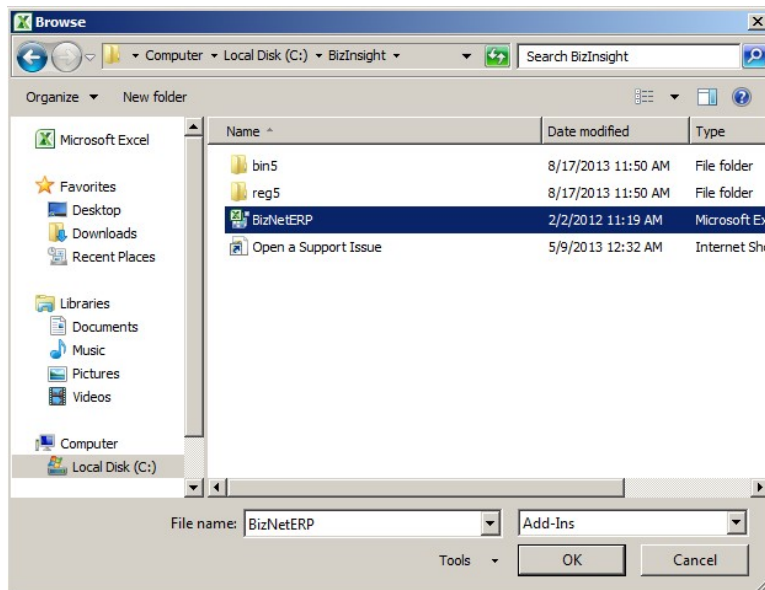
1. Click on **Tools > Add-Ins**



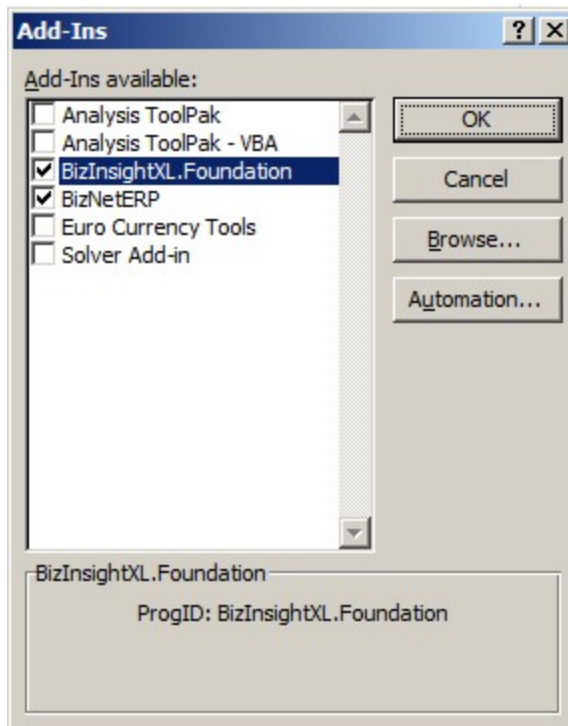
2. In the Add-ins dialog, click on the **Browse** button.



3. Browse to the directory to which you installed BizInsight and select the .xll file in that directory. Then click **OK**.



The Add-ins dialog should now look like the following:



4. Click **OK**.

Check TCP/IP, SQL Browser and Firewall Exceptions

The XMLFast feature added in an earlier BizInsight build requires the following server configuration changes:

- The TCP/IP protocol must be enabled for SQL Server and the SQL Browser Service must be running. see "Enable TCP/IP" below.
- Server firewall exceptions must be added for TCP Port 1433, UDP Port 1434 and a program exception for sqlservr.exe. see "Add Windows Firewall Exceptions" on page 70

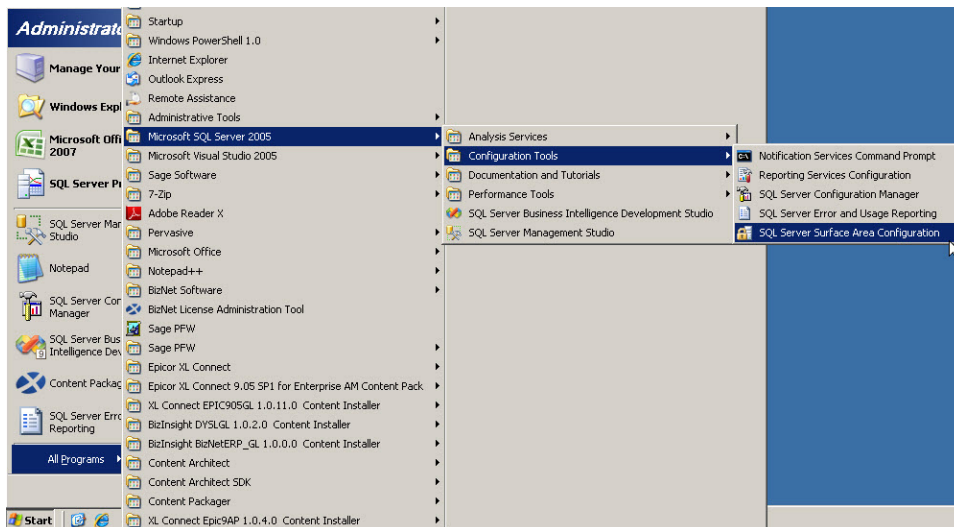
Customers are strongly encouraged to make these changes in order for the XMLFast feature to work. While the XMLFast feature can be turned off on the client workstation in Application Settings, doing so will result in significantly slower data retrieval times.

Enable TCP/IP

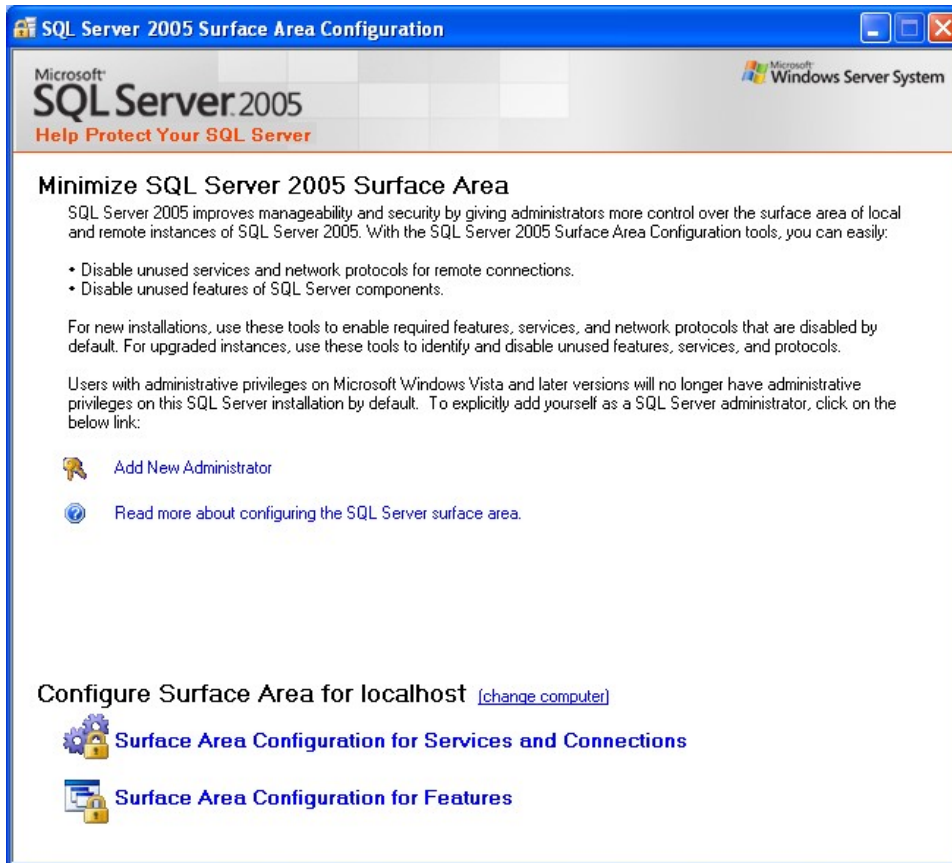
To enable TCP/IP, the steps vary depending on your SQL Server version. The steps for SQL Server 2005 are as follows. For SQL Server 2008 or higher, see "SQL Server 2008" on page 65.

SQL Server 2005

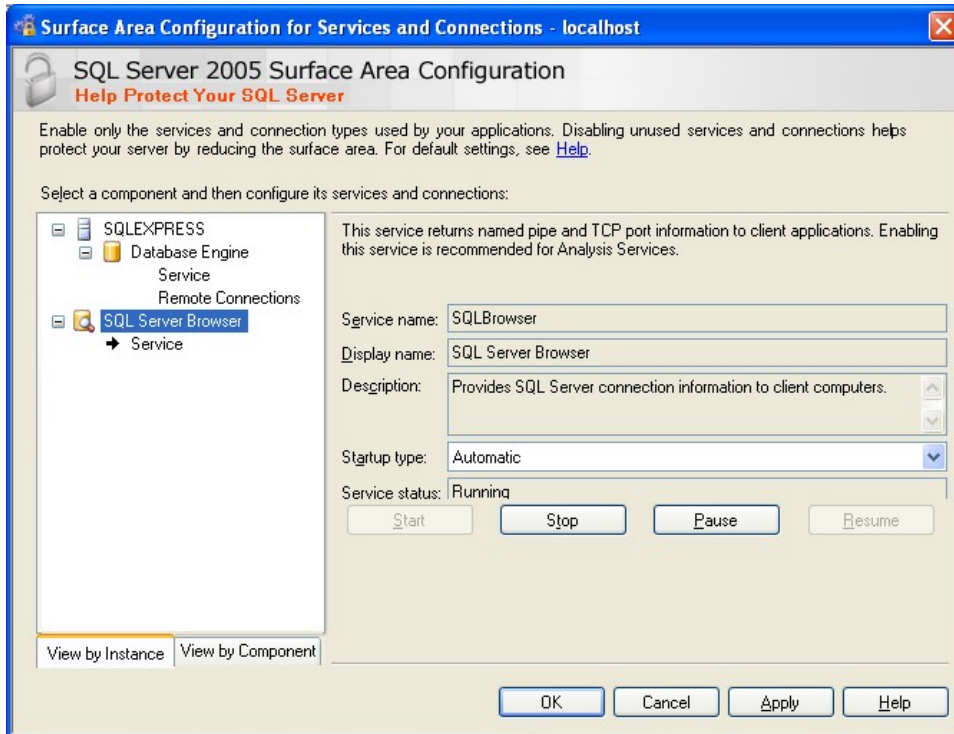
1. Click on **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Surface Area Configuration**.



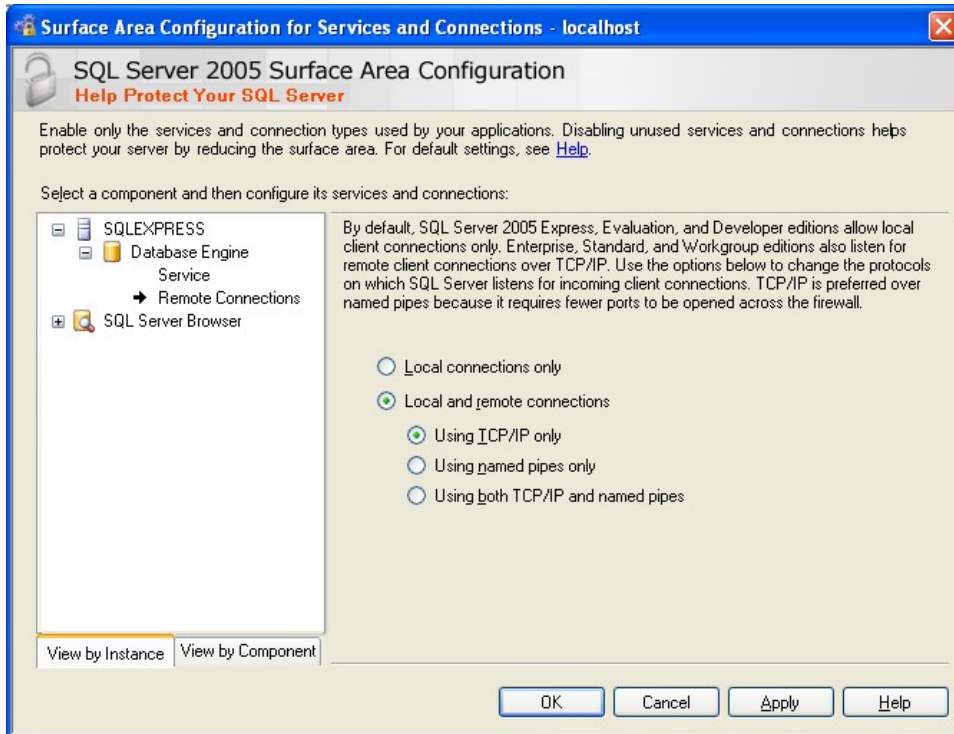
2. Click on **Surface Area Configuration for Services and Connections**.



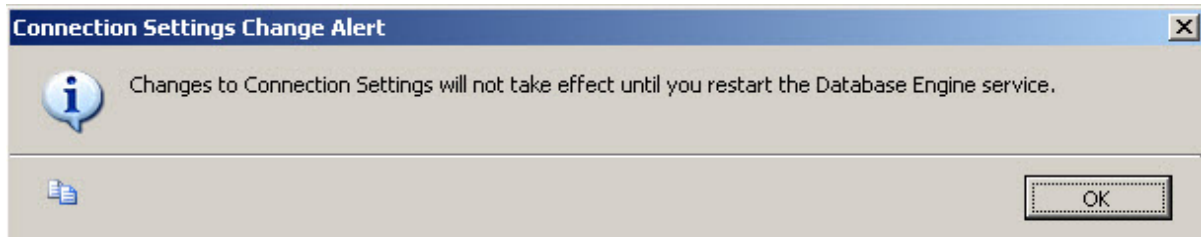
3. In the left pane, click on **SQL Server Browser**. When the right pane has refreshed with the options for the SQL Server Browser, make sure that **Startup Type** is set to "Automatic" and click on **Start** if the service is not started.



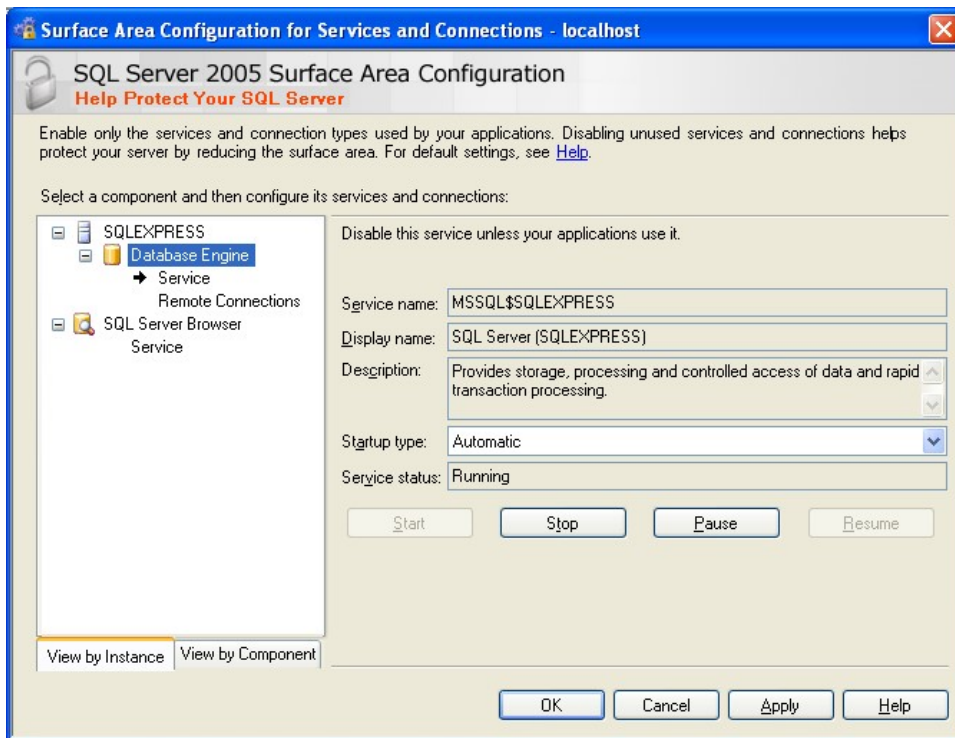
- Under Database Engine, click on **Remote Connections**. Select the **Local and Remote Connections** radio button to enable remote users to access this SQL Server instance. Click **Apply**.



- An alert dialog will be displayed indicating that the changes will not take effect until the Database Engine service is stopped and restarted. Click **OK**.

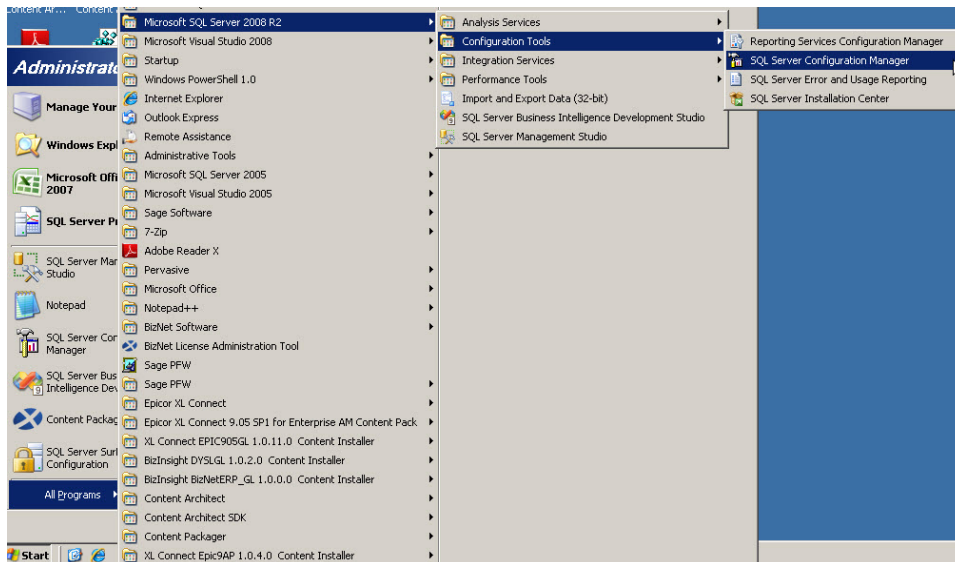


- In the left pane, expand **Database Engine** and click on **Service**. In the right pane, click on **Stop** and then click on **Start** when that button becomes enabled. Once the service is restarted, click **OK** to exit the Surface Area Configuration tool.

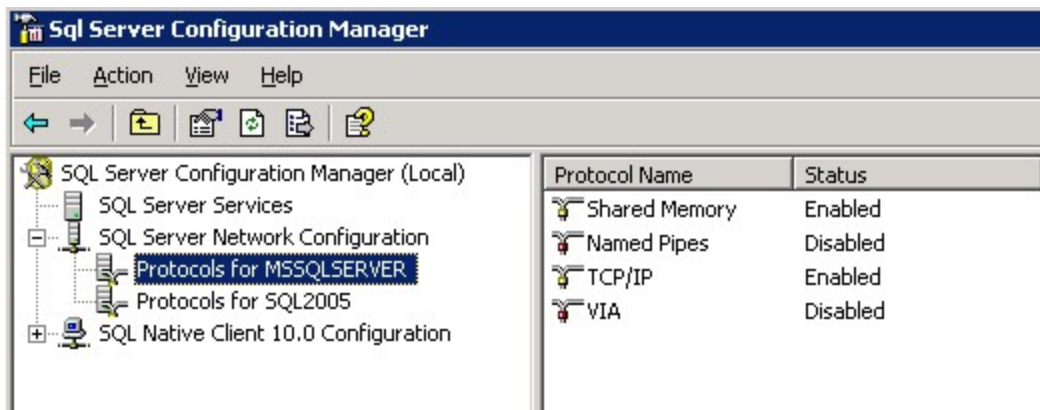


SQL Server 2008

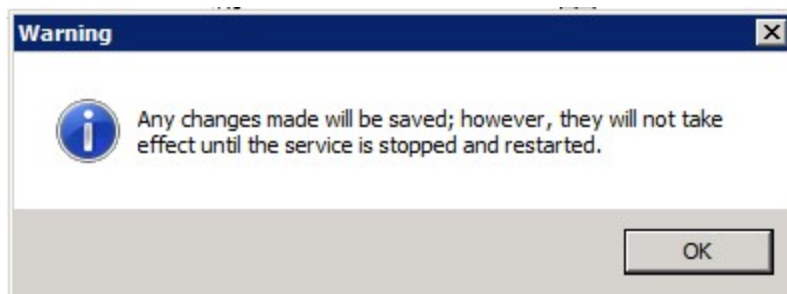
1. Click on **Start > All Programs > Microsoft SQL Server 2008 (2008 R2) > Configuration Tools > SQL Server Configuration Manager**.



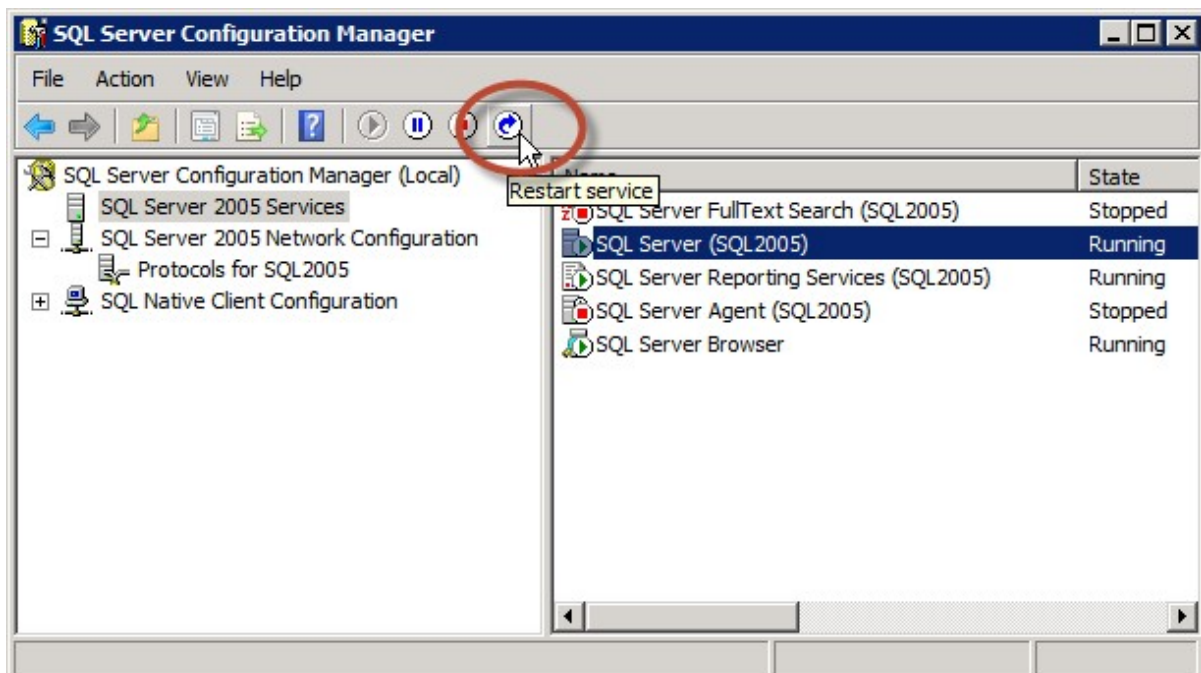
2. Expand **SQL Server Network Configuration** and select the **Protocols for InstanceName** that corresponds to the SQL Server instance that hosts the accounting system database.



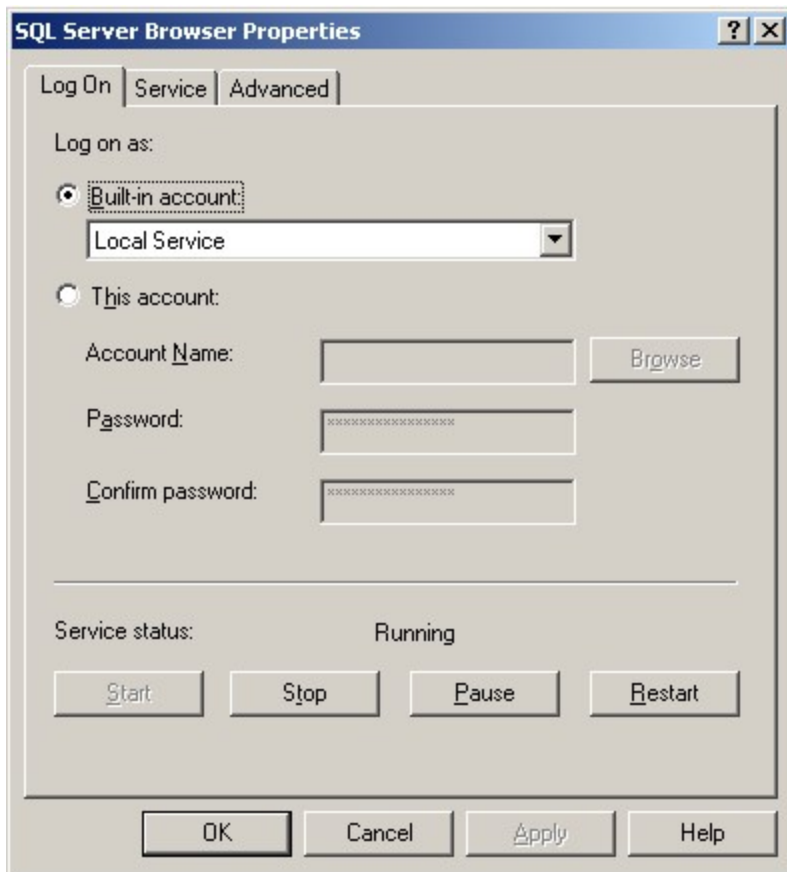
3. Verify that the **TCP/IP** Protocol is "Enabled". If it is not enabled, double-click on the protocol and change its properties to enabled. You will receive a warning that the service will need to be stopped and restarted:



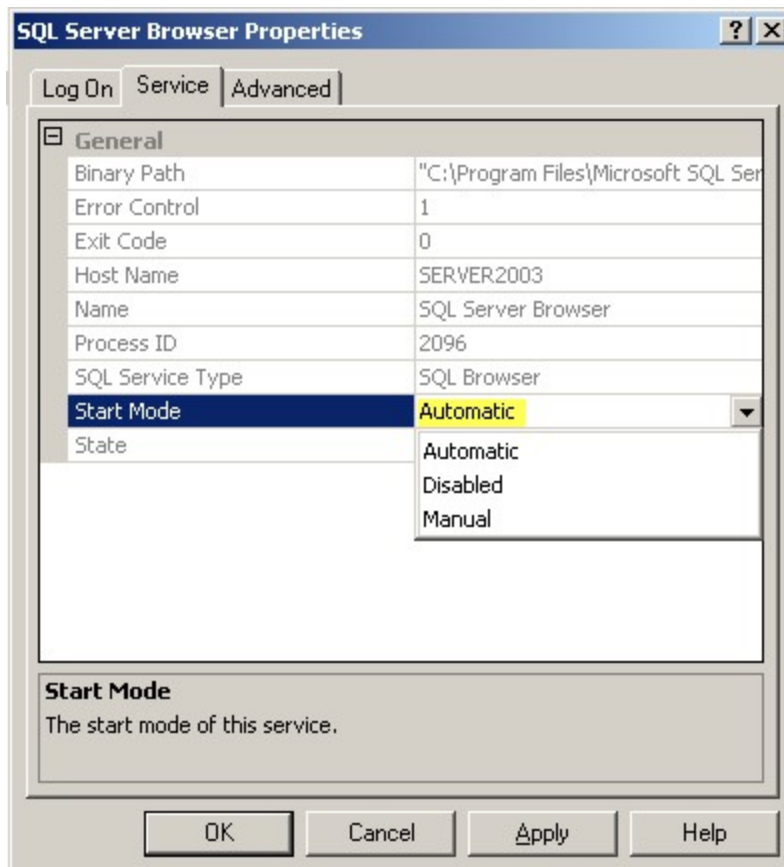
4. Go to the **SQL Server Services** section. Select the SQL Server service and click on the restart the service button.



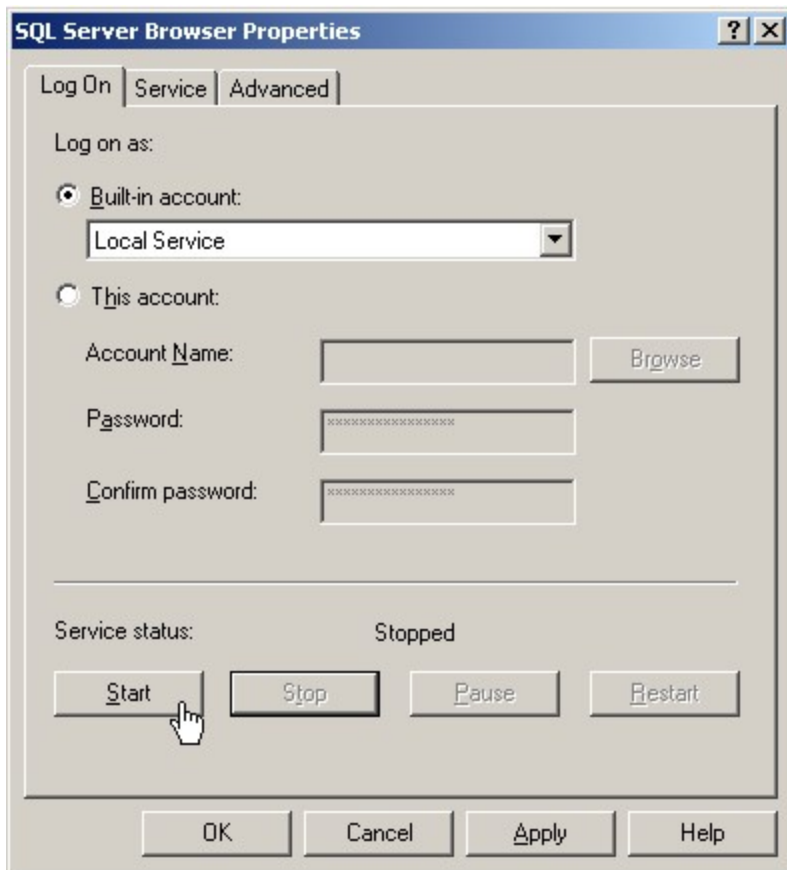
5. In the SQL Server Services section, verify that the SQL Server Browser service is started. If it is not, double-click on the service to open the service properties.



- Click on the **Service** tab and make sure the **Start Mode** is set to "Automatic".



7. On the **Log On** tab, click on the **Start** button to start the service

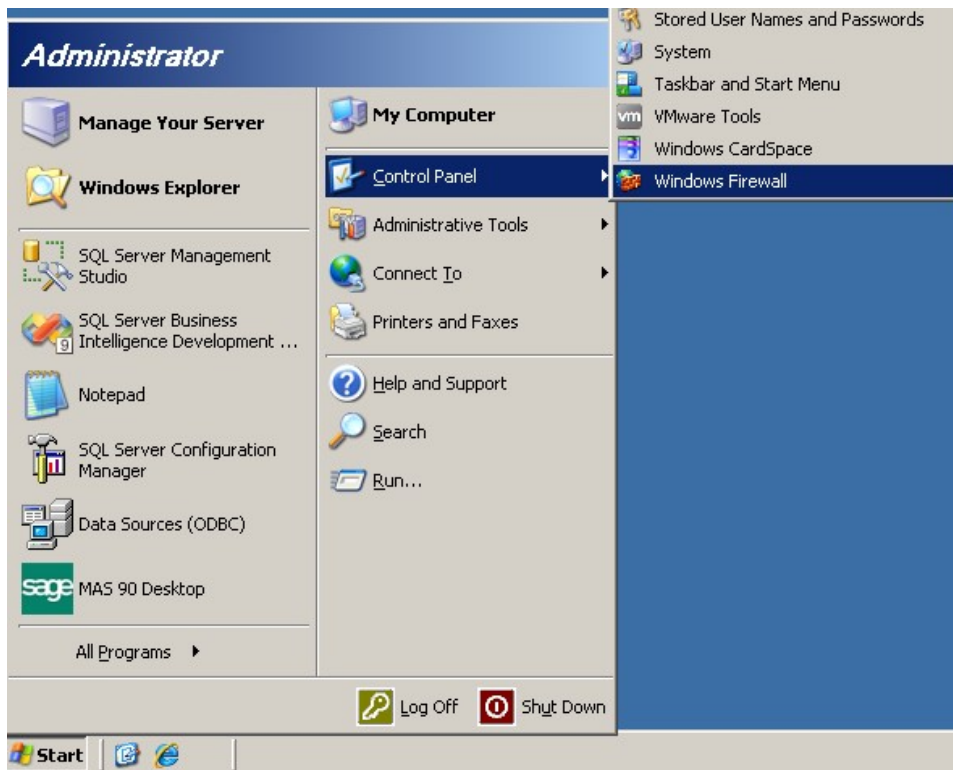


Add Windows Firewall Exceptions

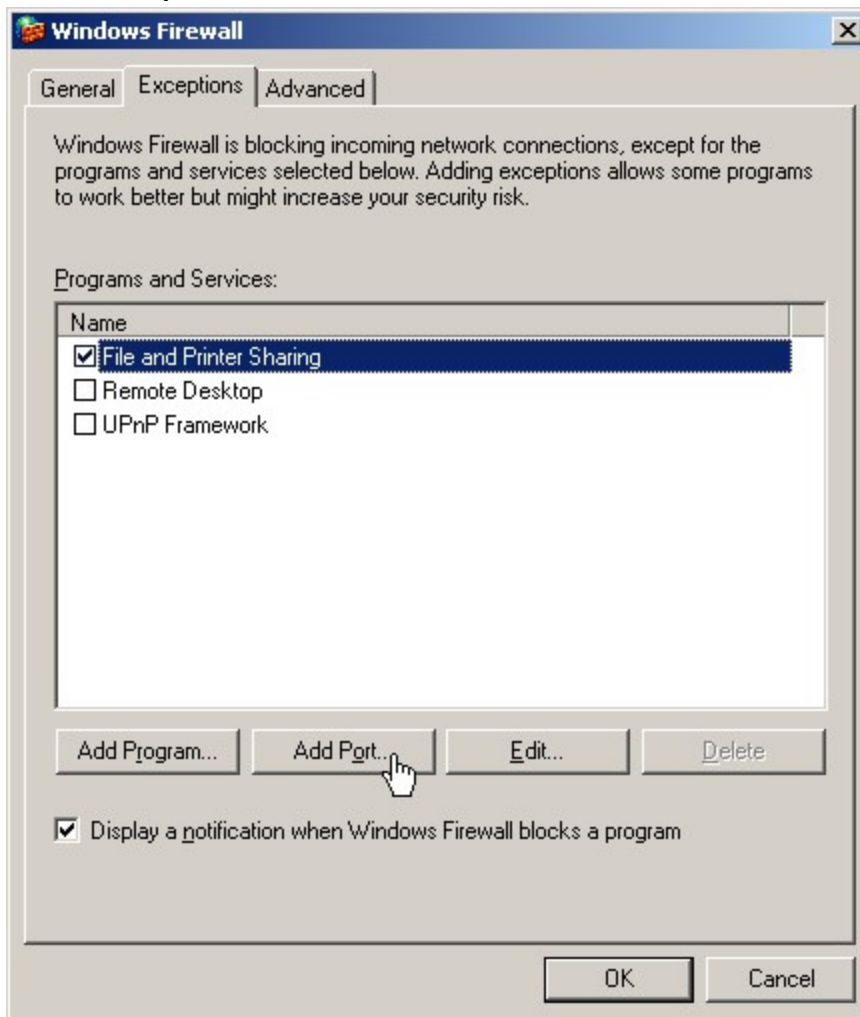
This step may not need to be performed if the Windows Firewall is turned off on the server.

Server 2003 (click [here](#) to go to the Server 2008 instructions)

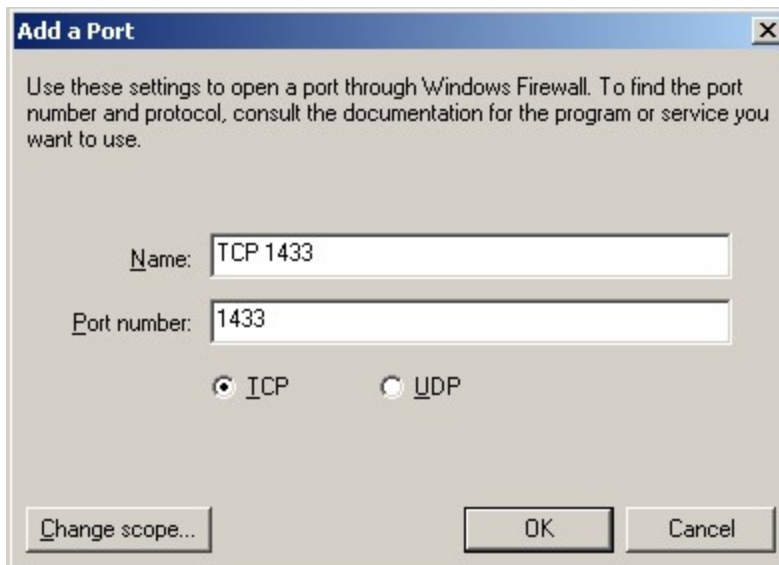
1. Click on **Start > Control Panel > Windows Firewall**



2. On the **Exceptions** tab, click the **Add Port** button.

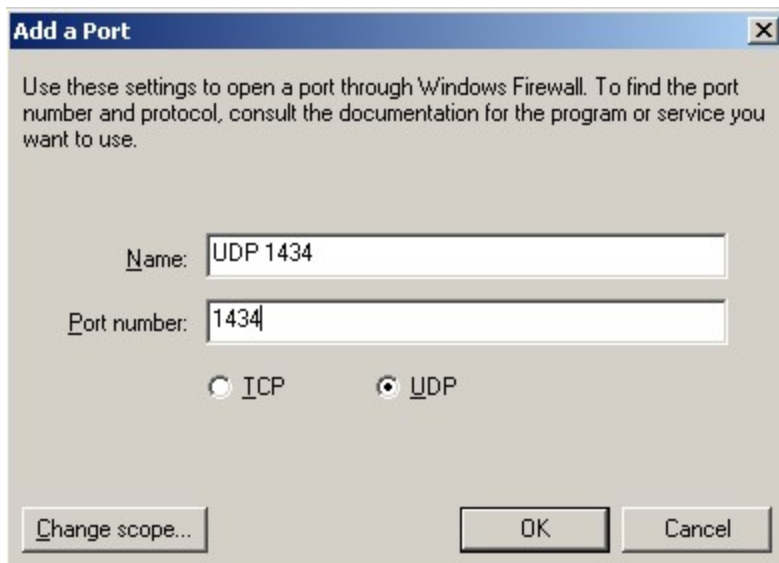


3. In the **Add a Port** dialog, enter a name for the exception entry and type "1433" for the port number. Click **OK**.



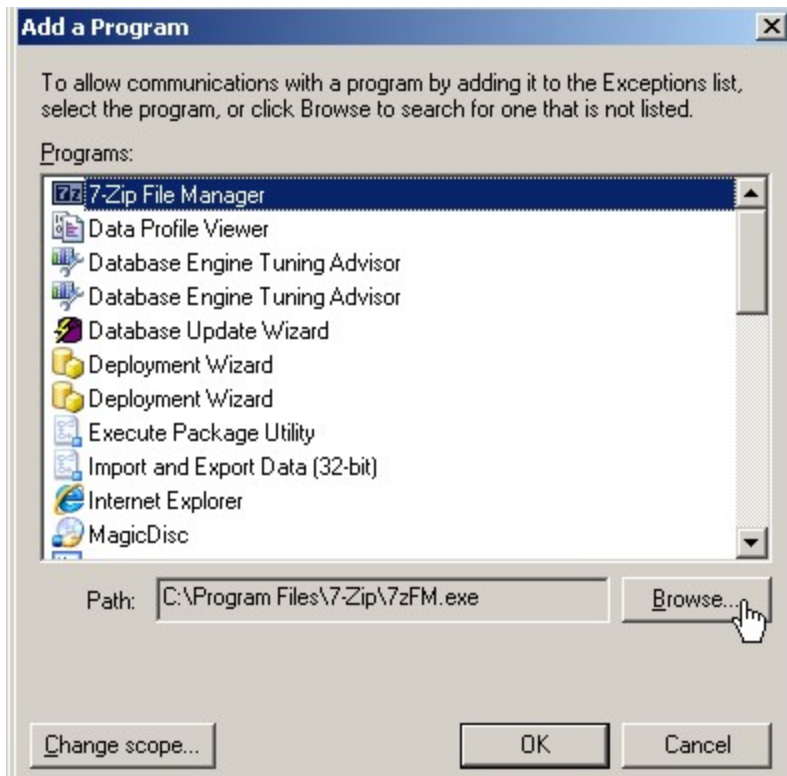
The screenshot shows the 'Add a Port' dialog box. The title bar is blue with the text 'Add a Port' and a close button. Below the title bar is a message: 'Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.' There are two text input fields: 'Name:' with the text 'TCP 1433' and 'Port number:' with the text '1433'. Below these fields are two radio buttons: 'TCP' (selected) and 'UDP'. At the bottom are three buttons: 'Change scope...', 'OK', and 'Cancel'.

4. Add a second port exception for UDP 1434.

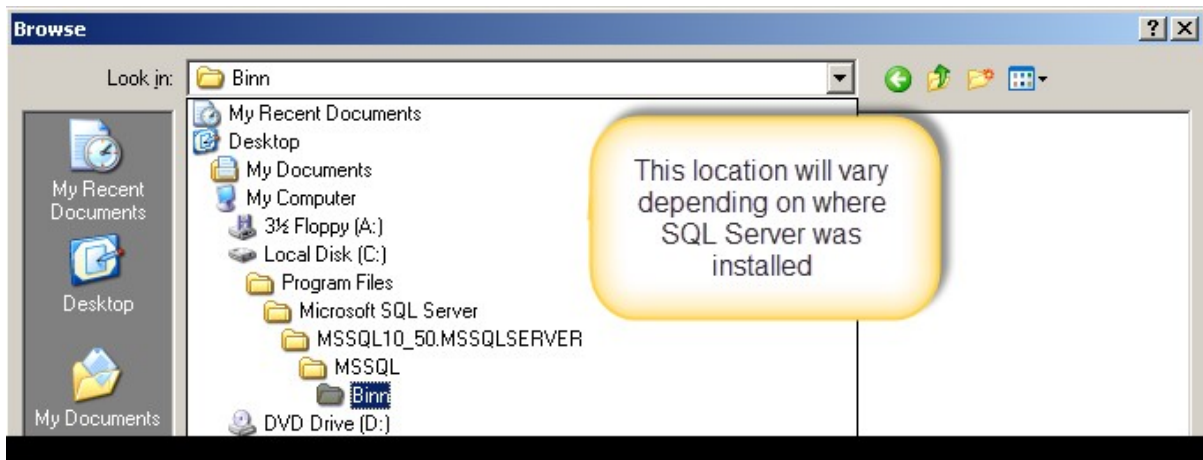


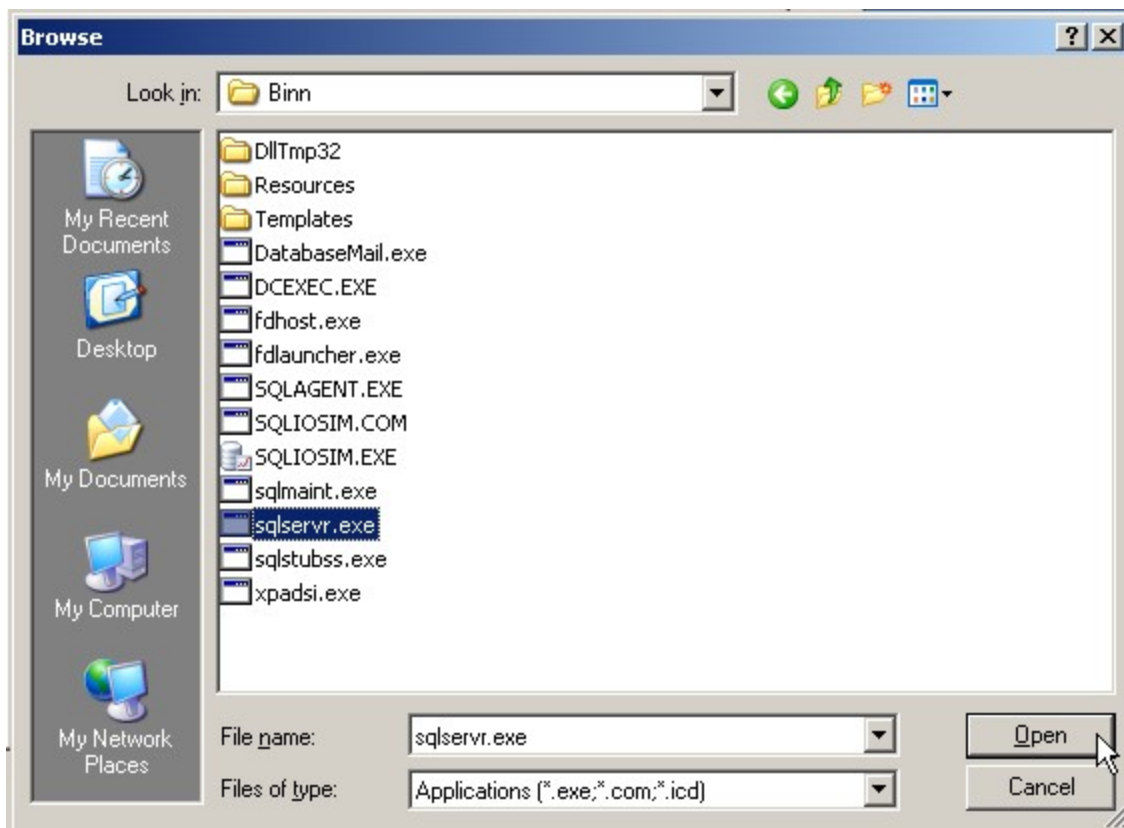
The screenshot shows the 'Add a Port' dialog box. The title bar is blue with the text 'Add a Port' and a close button. Below the title bar is a message: 'Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.' There are two text input fields: 'Name:' with the text 'UDP 1434' and 'Port number:' with the text '1434'. Below these fields are two radio buttons: 'TCP' and 'UDP' (selected). At the bottom are three buttons: 'Change scope...', 'OK', and 'Cancel'.

5. Click the **Add Program** button then click the Browse button



6. Browse to the SQL Server installation's Binn directory and select **sqlservr.exe**.

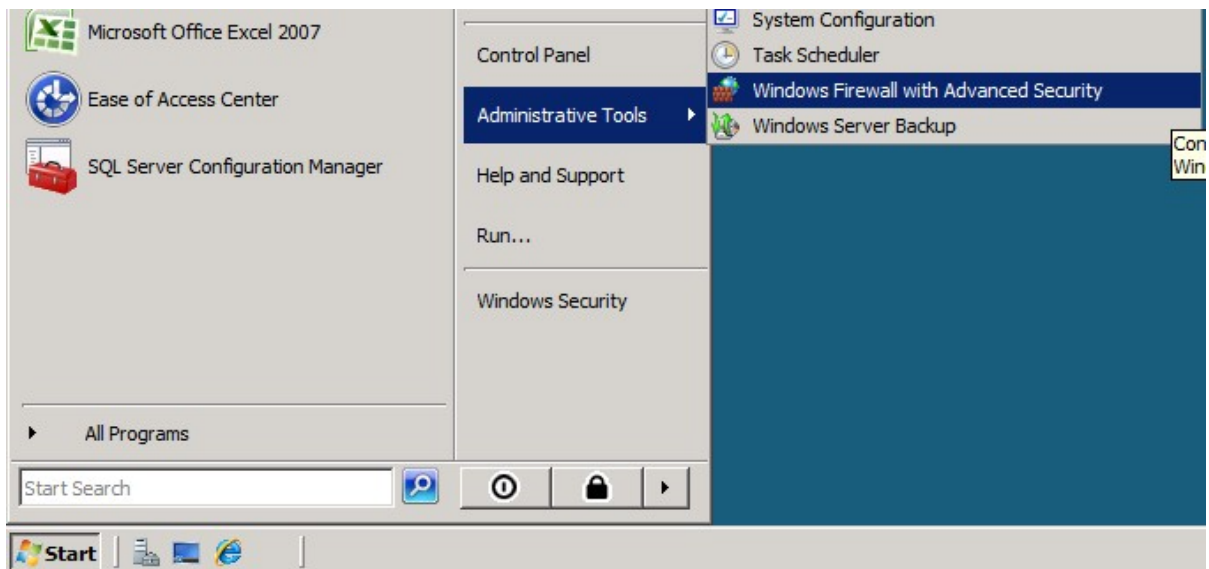




7. Close the Firewall dialog after making these additions.

Server 2008

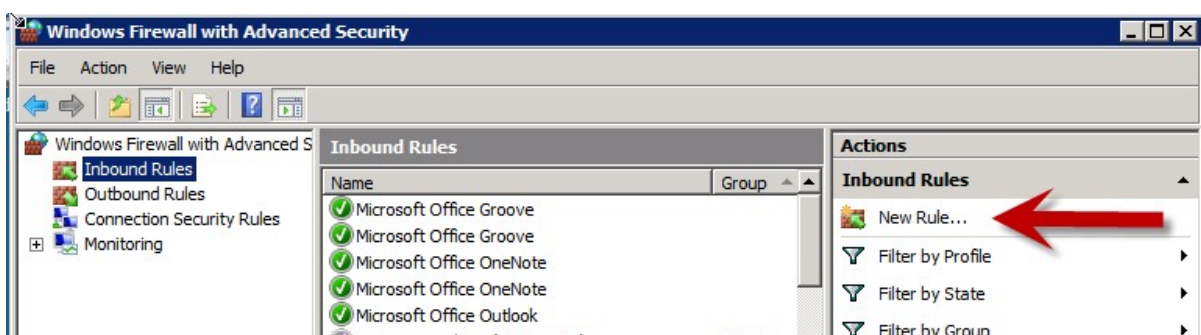
1. Click on **Start > Administrative Tools > Windows Firewall with Advanced Security**



2. Click on **Inbound Rules**.



3. Click on **New Rule...**



4. Choose the **Port** radio button and click **Next**.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Rule Type' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. Below the title bar, the 'Rule Type' section is active, with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps' pane lists five steps: 'Rule Type' (selected with a green dot), 'Protocol and Ports' (green dot), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main area asks 'What type of rule would you like to create?' and lists four options with radio buttons: 'Program' (Rule that controls connections for a program.), 'Port' (Rule that controls connections for a TCP or UDP port.), 'Predefined:' (Rule that controls connections for a Windows experience., with a dropdown menu showing 'BITS Peercaching'), and 'Custom' (Custom rule.). A link 'Learn more about rule types' is at the bottom left. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☒ **Port**
Rule that controls connections for a TCP or UDP port.

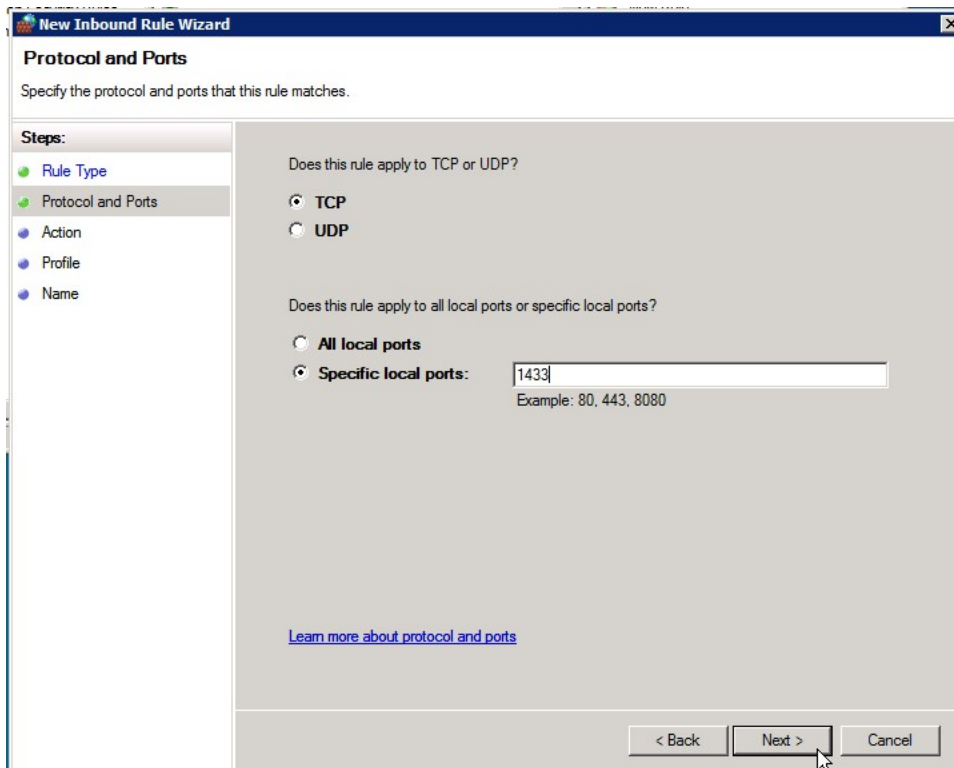
☐ **Predefined:**
BITS Peercaching
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

[Learn more about rule types](#)

< Back Next > Cancel

5. Leave the **TCP** option selected and type in port 1433. Click **Next**.



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. Below the title bar, the section 'Protocol and Ports' is displayed with the instruction 'Specify the protocol and ports that this rule matches.' On the left side, there is a 'Steps:' pane with four items: 'Rule Type' (selected with a green dot), 'Protocol and Ports' (selected with a green dot), 'Action' (unselected with a blue dot), 'Profile' (unselected with a blue dot), and 'Name' (unselected with a blue dot). The main area of the wizard contains two questions. The first question is 'Does this rule apply to TCP or UDP?' with two radio button options: 'TCP' (selected) and 'UDP' (unselected). The second question is 'Does this rule apply to all local ports or specific local ports?' with two radio button options: 'All local ports' (unselected) and 'Specific local ports:' (selected). Below the 'Specific local ports:' option, there is a text input field containing the value '1433'. Below the input field, there is a small text label that reads 'Example: 80, 443, 8080'. At the bottom of the wizard, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

New Inbound Rule Wizard

Protocol and Ports
Specify the protocol and ports that this rule matches.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP

☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

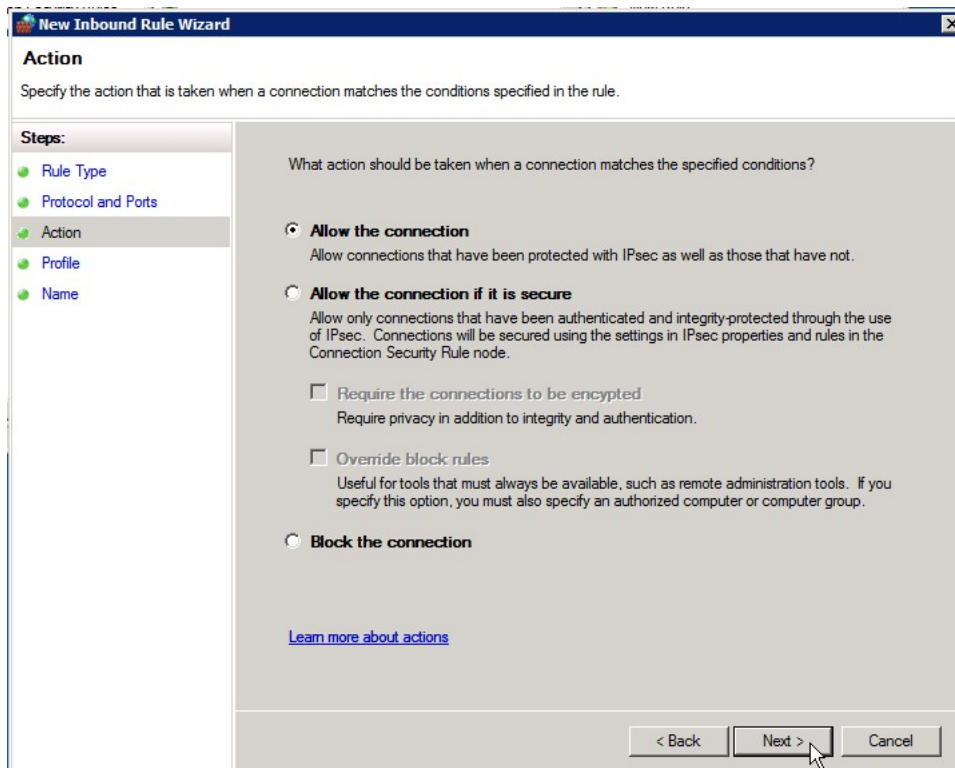
☒ Specific local ports:

Example: 80, 443, 8080

[Learn more about protocol and ports](#)

< Back Next > Cancel

6. Leave the **Allow the connection** radio button selected and click **Next**.



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. Below the title bar, the word 'Action' is displayed in bold. A subtitle reads: 'Specify the action that is taken when a connection matches the conditions specified in the rule.' On the left side, there is a 'Steps:' panel with a list of steps: 'Rule Type', 'Protocol and Ports', 'Action' (which is highlighted with a green dot and a grey background), 'Profile', and 'Name'. The main area of the wizard is titled 'What action should be taken when a connection matches the specified conditions?'. It contains three radio button options: 1. 'Allow the connection' (selected): 'Allow connections that have been protected with IPsec as well as those that have not.' 2. 'Allow the connection if it is secure': 'Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' This option has two unchecked checkboxes: 'Require the connections to be encrypted' (with the subtext 'Require privacy in addition to integrity and authentication.') and 'Override block rules' (with the subtext 'Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.'). 3. 'Block the connection'. At the bottom left of the main area is a blue hyperlink: 'Learn more about actions'. At the bottom right are three buttons: '< Back', 'Next >' (which has a mouse cursor pointing at it), and 'Cancel'.

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- **Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
Allow connections that have been protected with IPsec as well as those that have not.

☐ **Allow the connection if it is secure**
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Require the connections to be encrypted**
Require privacy in addition to integrity and authentication.

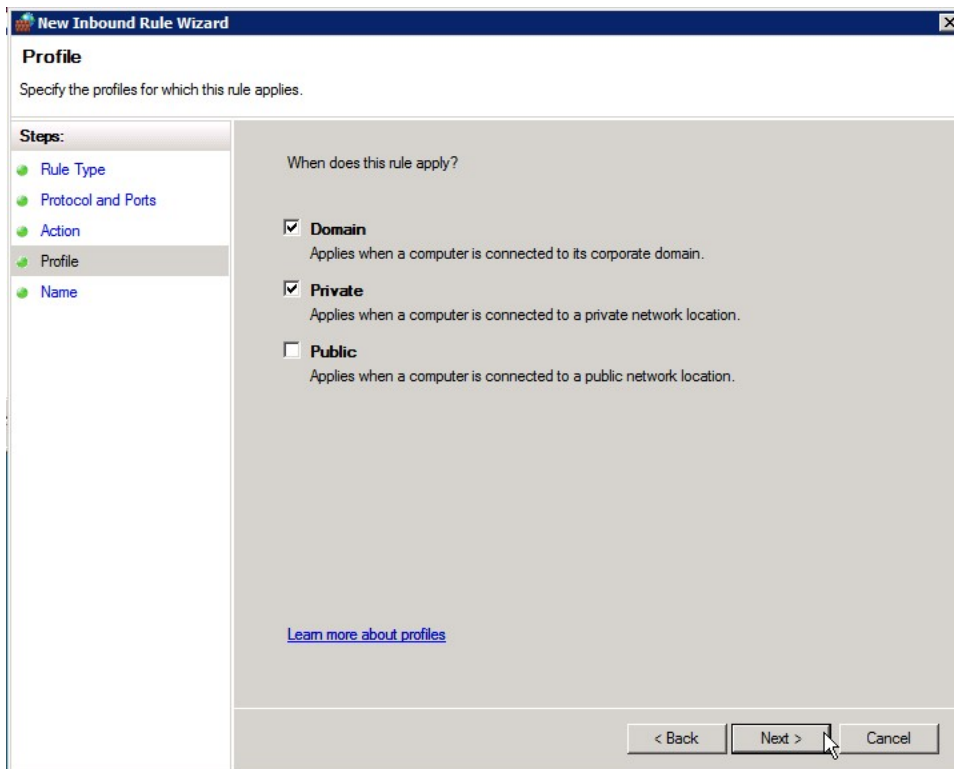
☐ **Override block rules**
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

☐ **Block the connection**

[Learn more about actions](#)

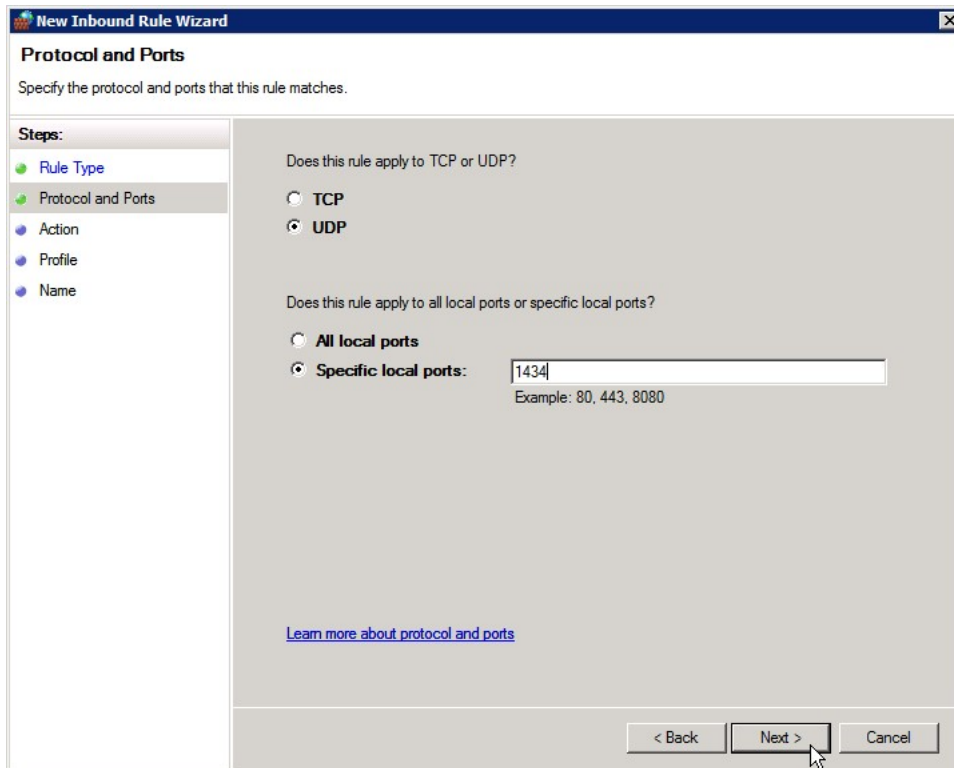
< Back **Next >** Cancel

7. Uncheck the **Public** checkbox (unless users are connecting using a public network location) and click **Next**.



8. Type a name and description for the exception and click **Finish**.

9. Repeat these steps to add a UDP port exception for port 1434.



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. Below the title bar, the section 'Protocol and Ports' is highlighted, with the instruction 'Specify the protocol and ports that this rule matches.' To the left of the main content area is a 'Steps:' sidebar with five items: 'Rule Type' (green dot), 'Protocol and Ports' (green dot and highlighted), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main content area contains two questions. The first question is 'Does this rule apply to TCP or UDP?' with two radio button options: 'TCP' and 'UDP'. The 'UDP' option is selected. The second question is 'Does this rule apply to all local ports or specific local ports?' with two radio button options: 'All local ports' and 'Specific local ports:'. The 'Specific local ports:' option is selected, and next to it is a text input field containing the value '1434'. Below the input field is a small text example: 'Example: 80, 443, 8080'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button. A link labeled 'Learn more about protocol and ports' is located at the bottom left of the main content area.

New Inbound Rule Wizard

Protocol and Ports
Specify the protocol and ports that this rule matches.

Steps:

- Rule Type
- Protocol and Ports**
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☐ TCP

☒ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

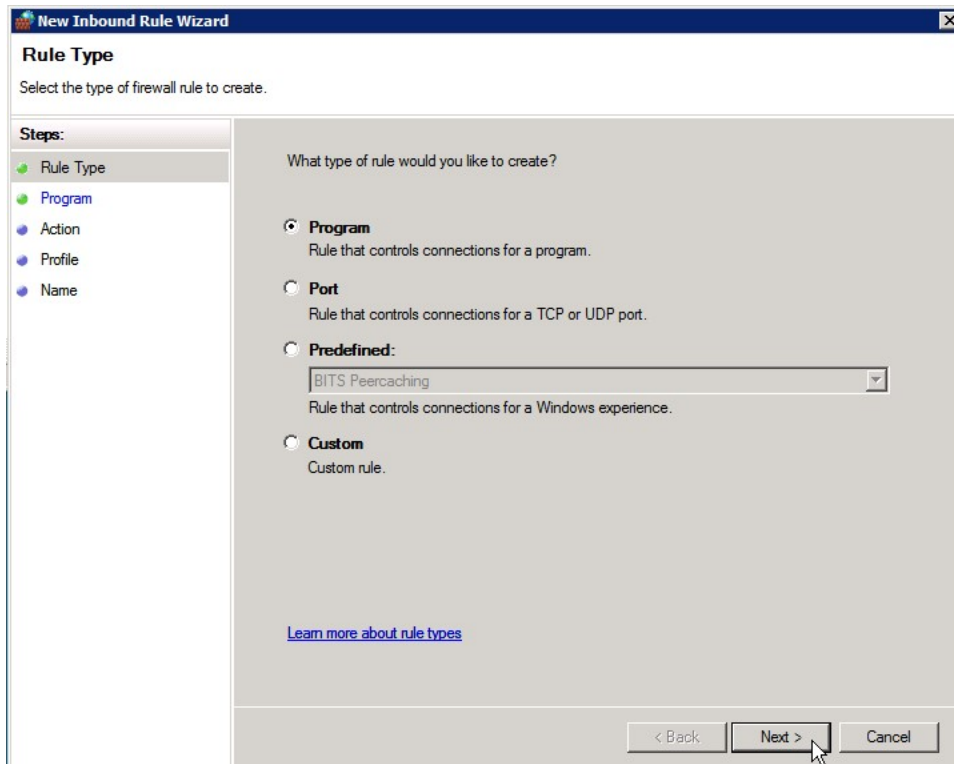
☒ Specific local ports:

Example: 80, 443, 8080

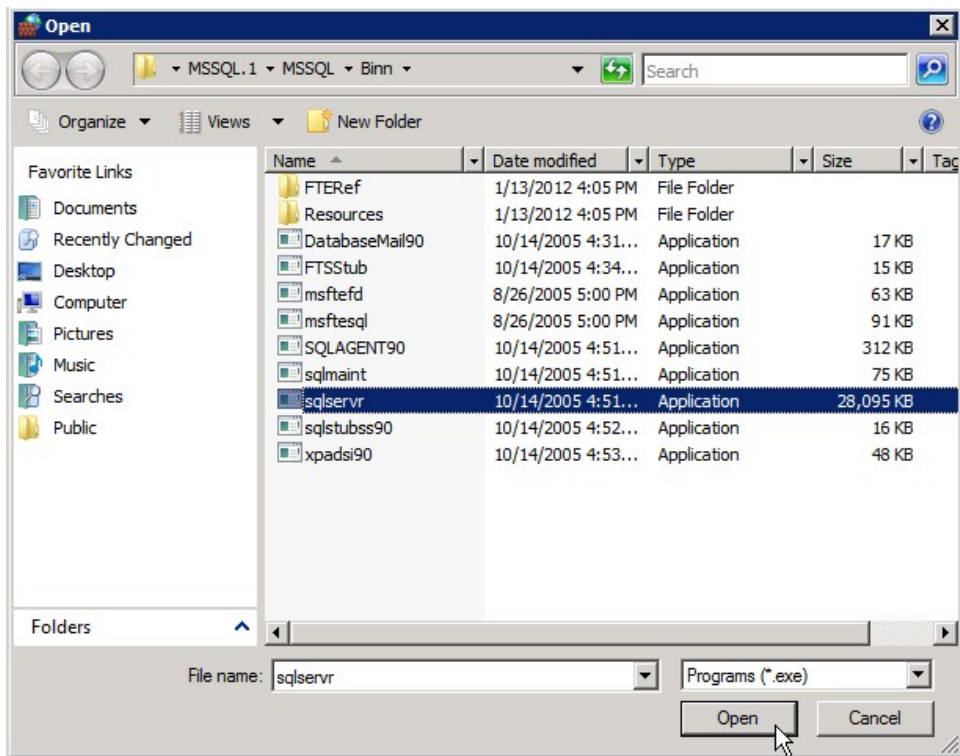
[Learn more about protocol and ports](#)

< Back Next > Cancel

10. Add a third new inbound rule for a program exception.



11. Click on the **Browse** button and browse to the SQL Server installation's Binn directory and select **sqlservr.exe**. Then click **Next**.



New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program**
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

☐ **All programs**
Rule applies to all connections on the computer that match other rule properties.

☒ **This program path:**

Example: c:\path\program.exe
 %ProgramFiles%\browser\browser.exe

This path will vary depending on where SQL Server was installed.

[Learn more about specifying programs](#)

< Back Next > Cancel

12. Leave **Allow the connection** selected and click **Next**.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. Below the title bar, the 'Action' section is highlighted. The main area of the wizard contains the following text and options:

Action
Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- **Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
Allow connections that have been protected with IPsec as well as those that have not.

☐ **Allow the connection if it is secure**
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Require the connections to be encrypted**
Require privacy in addition to integrity and authentication.

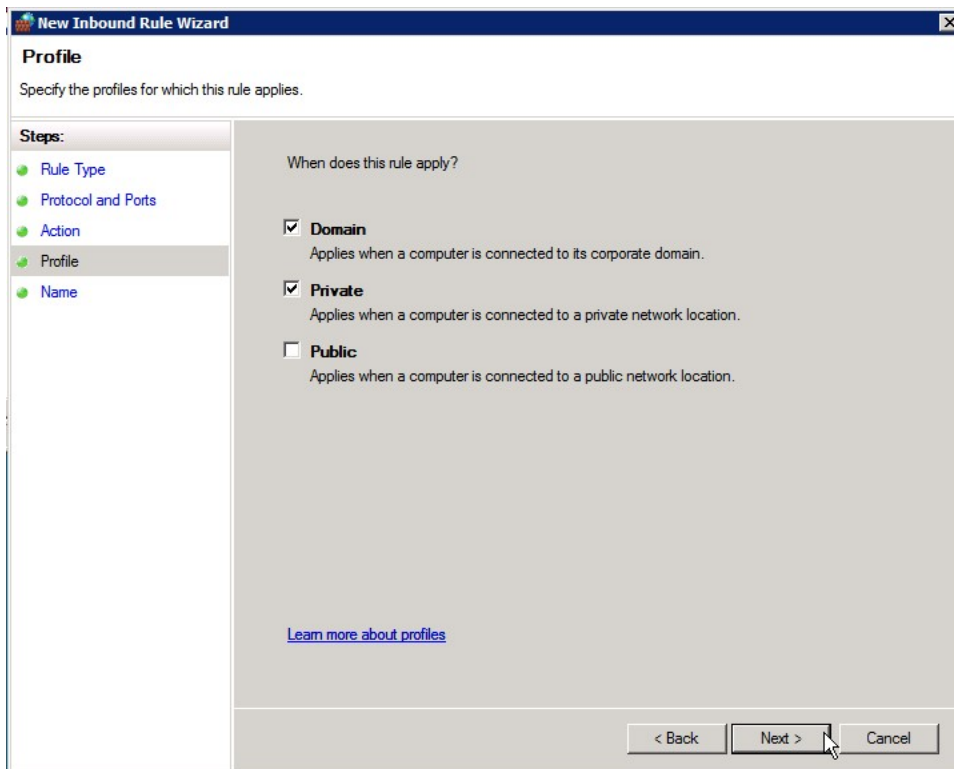
☐ **Override block rules**
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

☐ **Block the connection**

[Learn more about actions](#)

At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

13. Uncheck the **Public** checkbox (unless users are connecting using a public network) and click **Next**.



14. Type a name and description for the exception and click **Finish**.

BizInsight Column Based Security Overview

Disclaimer:

The following information is for general purposes only. The information is provided by BizNet Software and while we strive to keep the information up to date and accurate, we make no representations or warranties of any kind, express or implied, about the accuracy or reliability with respect to our internal research contained in this documentation. Any reliance you place on such information is therefore strictly at your own risk.

In no event will BizNet Software, Inc. or BizNet Software, Inc. be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of the documentation.

In any ERP system, the balance between making data accessible to end users while denying access to those who should not have access is a difficult challenge. ERP security only at the application layer is not a truly secured system; the communication between the application and the data is exposed to users who are not authorized to access confidential information. BizNet Software has incorporated four layers of security into the BizInsight product. These security levels are as follows:

1. BizInsight License User Types Security
2. DataSet Security – applies to RDL security on the Report Server.
3. MetaData Security – applies to SQL Database and Shared Directory folder.
4. Column Security – applies to all functionality on content packs. (Functions, Drill-downs, and Analysis Sets)

Of the above four security levels, two are specifically provided with the BizInsight product: BizInsight License User Types Security and Column Security. The other two items, DataSet Security and MetaData security, utilize the native security model provided with Reporting Services, SQL Server, and Windows NTFS security.

BizInsight uses Reporting Services to store the queries and datasets used for connectivity to the accounting system. Reporting Services provides its own security and BizInsight objects can be

independently secured using the delivered Reporting Services security model. Users must be granted access to the BizInsight objects published to Reporting Services in order to utilize them.

BizInsight uses SQL databases (BizInsight and BizInsightDB) to store product metadata. BizInsight users must be provided access to these databases using native SQL Server security. In addition, the BizInsight shared directory is also a metadata repository and sufficient Windows NTFS security.

BizInsight License User Types Security

This security level ensures that only licensed users are able to use the BizInsight product. In addition, BizInsight licensing is broken out into different user types: . The different user types have decreasing capabilities with the Designer user having the most capabilities. See the User Guide for more information regarding the different user types and their capabilities.

Column Security

Column security is based on a security policy that specifies the rules and conditions under which a user can access a column value from a table. The column access restriction is based on individual user permissions. When defining the column to apply the restriction, the column must exist across all datasets from which BizInsight is retrieving data. In most business policies, restricting access by the "Company" column is the most frequently used security logic; however, BizInsight provides the flexibility to utilize other columns.

The column security design uses an optimistic method in restricting user access: IT administrators will need to provide the values to deny. Values not listed are inferred to be allowed. For example, if a user is permitted to access 97 out of 100 unique values, 3 restricted values will need to be defined when defining column security for that user. The remaining 97 values not defined in the security table will be able to be accessed by that user. All possible threats, vulnerabilities, and attacks and choosing the security design to implement are based on threat mitigation as first and performance second.

When column security is enabled and user restrictions are defined, access to the data will be restricted for the particular user. On the client machine, the user restriction policy applies to all content modules and functionality. Any access to functions, drill-down, and analysis set is denied if the restricted value is inserted in the feature. In the scenario of multiple parameters being passed to a function, if one of the parameter values is restricted, the security will deny access completely even though the user may have access to the non-restricted values.

Security vs Performance

Design choices for securing a system affect performance, scalability and usability. The more secure a system becomes, the more companies must compromise in terms of performance and usability. In selecting the best balance between security and performance, the optimistic security design has proven to be the ideal option. The below research and development results are based on BizNet Software internal testing and illustrate the impact security has on performance. Results will vary depending on network connection, environmental setup, and Microsoft Office bitness.

Scenario: Excel 2010 64-bit BizData Iterations - 80,688 Dedicated Server and Client Machine	First Refresh (sec)	Second Refresh (sec)	Offline Mode	Number of Restricted Values
Baseline: Security OFF on SQL Database	114.57	113.18	69.07	N/A
Security ON with no restricted users	111.4	109.38	75.18	0
Security ON and restricted values apply to the current user	118.81	114.61	74.16	1
Security ON and restricted values apply to the current user	124.54	119.9	80.14	6*
Security ON and restricted values apply to the current user	132.14	126.58	86.39	12*
Security ON and restricted values apply to other users	114.97	120.16	69.28	N/A
Security ON and restricted values apply to all users	124.64	119.29	79.16	N/A

* Multiple restricted columns is not currently supported

Key Results:

1. When Security mode is activated with no restricted values in the security table, little to no significant reporting performance loss.
2. When Security mode is activated with restricted values in the security table, there is about a 10% loss in reporting performance.

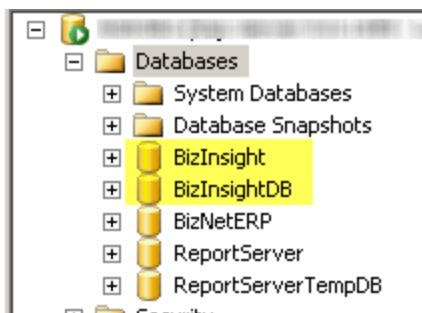
3. When Security mode is activated with double the amount of restricted values in the security table, there is about a double percentage loss in reporting performance.

Column Security Limitations

- Only a single column can be restricted. Multiple column security is not supported.
- The column must exist across all content packs.
- The column must exist as a server side parameter on RDLs. Security on optional parameters is not supported.
- The column name should be uniform across all RDLs.
- Connected to an single ERP. Multiple ERP systems are not supported.
- Security is based on an 'Exclusion Method'. IT administrators must insert values to restrict access.

Requirements to Use Column Security

- BizInsight 5.0.35.0 and later is installed on all client machines.
- Existing BizInsight and BizInsightDB databases created using a Content Installer and were created directly in SQL Server (not converted using the Access to SQL conversion tool).



- Reporting Services versions 2005*, 2008, 2008 R2, 2012 or 2014

IMPORTANT Reporting Services 2005 requires additional files to be installed. IT administrators must install the prerequisite files in a particular order. Following is a link to a Microsoft article with links to the necessary download files.

<http://www.microsoft.com/en-us/download/details.aspx?id=16978>

a. Install Microsoft® System CLR Types for SQL Server® 2008 R2

The SQL Server System CLR Types package contains the components implementing the geometry, geography, and hierarchy id types in SQL Server 2008 R2. This component can be installed separately from the server to allow client applications to use these types outside of the server.

b. Install Microsoft® SQL Server® 2008 R2 Shared Management Objects

The SQL Server Management Objects (SMO) is a .NET Framework object model that enables software developers to create client-side applications to manage and administer SQL Server objects and services. This object model will work with SQL Server 2000, SQL Server 2005, SQL Server 2008 and SQL Server 2008 R2.

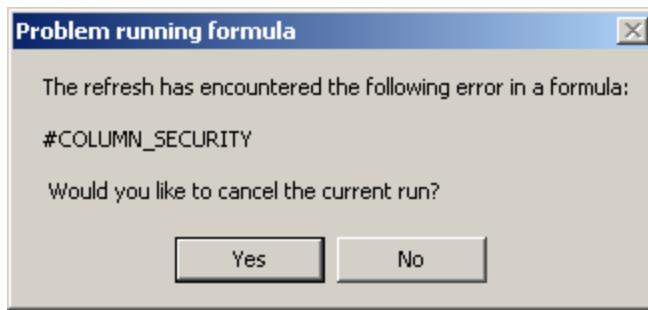
Column Security User Experience

When a user tries to access data to which they have been denied access, the cell will display #VALUE.

	A	B	C
1			
2		Not Restricted	Restricted
3	Company	Epic01	Epic03
4	Year	2009	2011
5	Period	12	4
6	Book	TARGET	TARGET
7			
8			
9	4*	-535800.78	#VALUE!
10			

To confirm that the error is due to Column Security, check the event log by clicking on the **About** button on the BizInsight ribbon and then clicking on **Support Tools > View Events**. A #COLUMN_SECURITY error will be logged there if the #VALUE is due to restricted access.

If the user refreshes a report that tries to retrieve data for a company to which they have no access, an error message will be displayed indicating they have requested restricted data:



Analysis sets that try to retrieve restricted data will return #COLUMN_SECURITY:

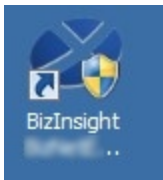
Refer to the Installation Guide for instructions on implementing Column Based Security.

Assign BizInsight Security to Users

Each BizInsight user's Windows account name must be added to a .users file in the admin shared directory in order for that user to perform any BizInsight action. You will use the License Administration Tool to perform these steps.

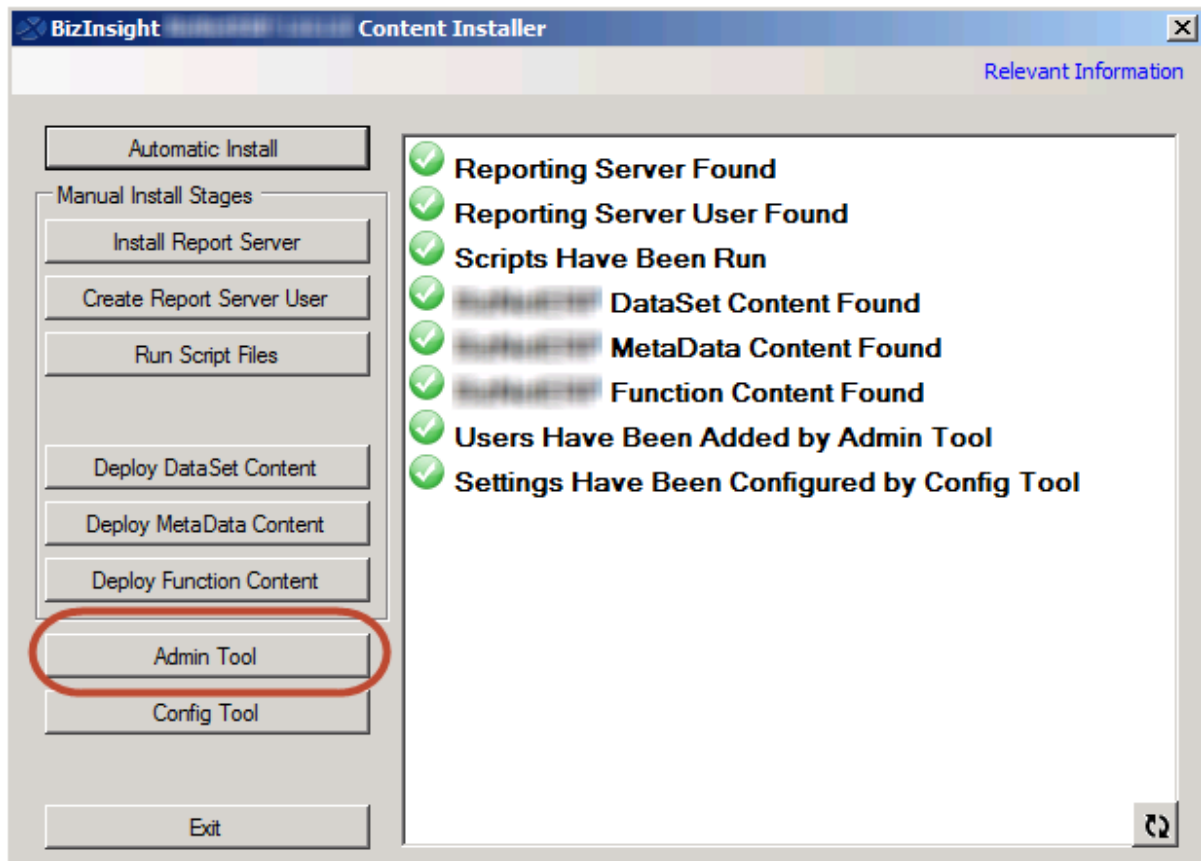
To assign BizInsight security to your users, do the following:

1. On the server, double-click any content installer desktop icon. If the content installers were installed without desktop icons, browse to the installation directory and double-click the file named "BizNet Content Installer.exe". If the content installer was uninstalled, reinstall it.



If you do not want to reinstall the content installer, see "Manual Steps" on page 98.

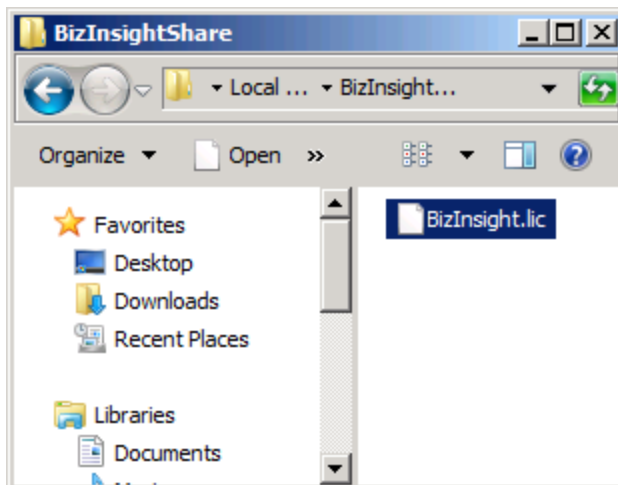
2. Click on the **Admin Tool** button.



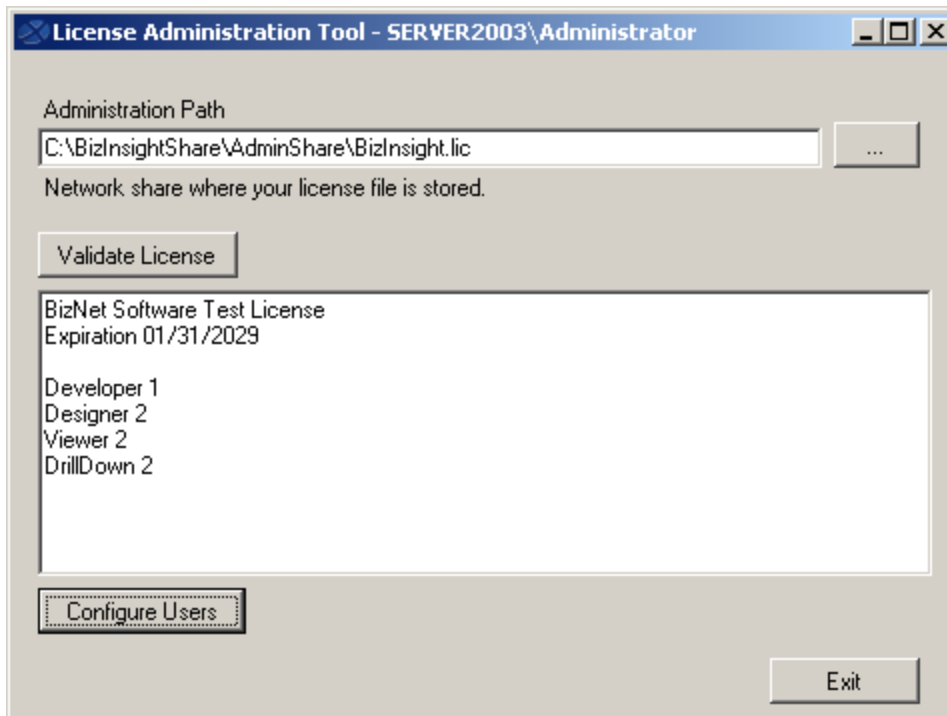
3. Click on the ellipses and browse to the admin share folder of your BizInsight shared directory.



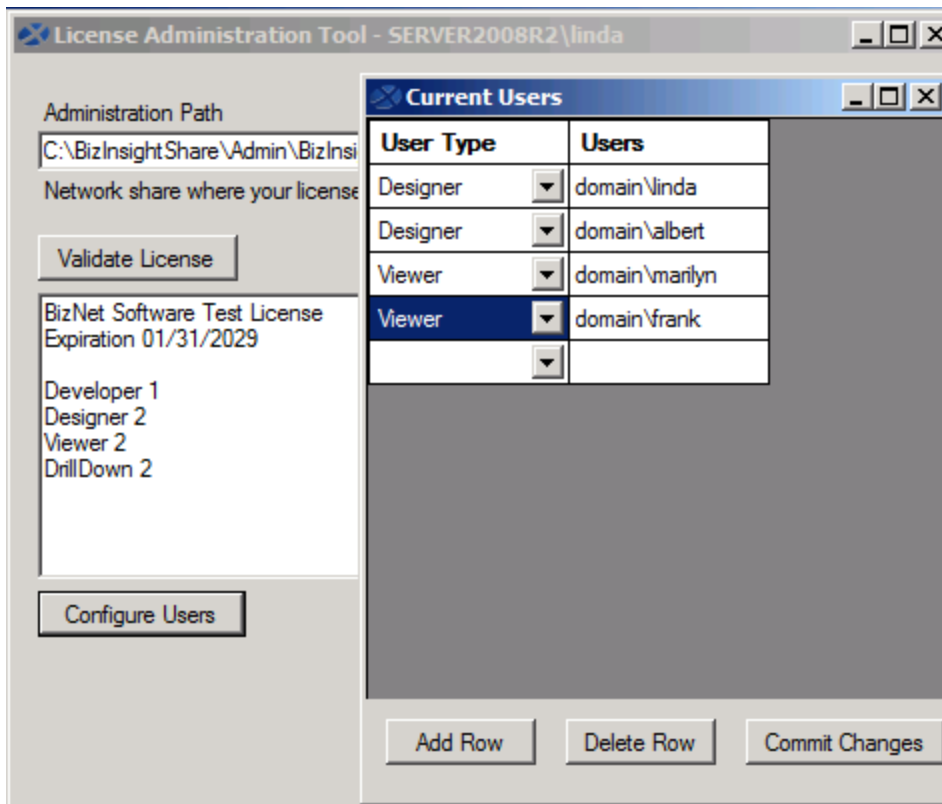
4. Select your BizInsight license file and click Open.



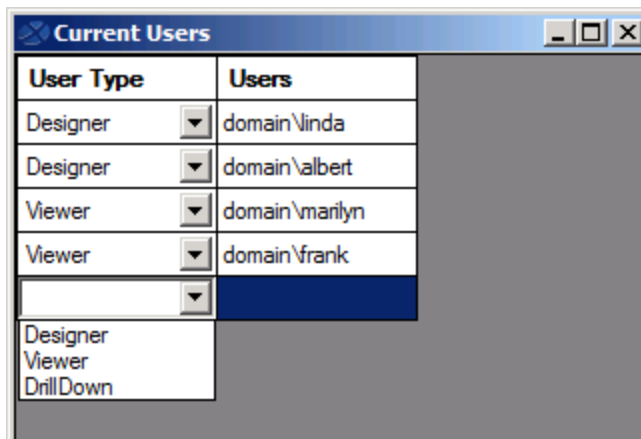
5. Click on the **Validate License** button to check how many licenses you currently have. Your current license count will be displayed.



6. Click on the **Configure Users** button. The **Current Users** dialog will open.

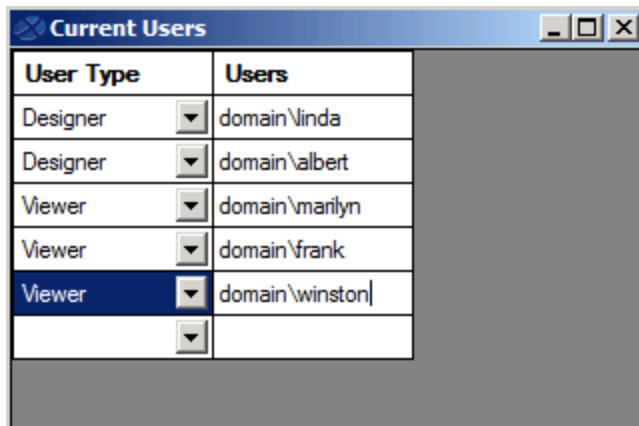


7. You will now add your new BizInsight user and assign them a user type. Click on the **User Type** drop down and select the desired user type. If you want your user to be a Designer, choose Designer from the drop down list.

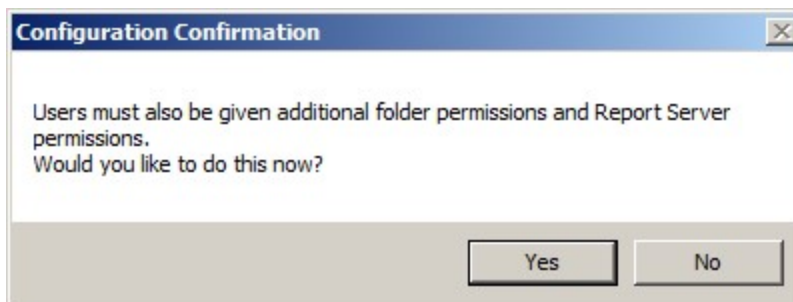


8. Type the user's name in the **Users** field in the format of domain\username.

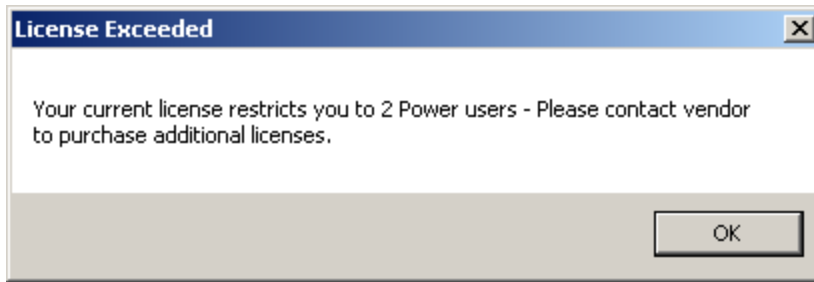
WARNING Do **not** add your own login using the Admin Tool unless you know for sure that you have another login available with sysadmin rights to the SQL Server instance. Early versions of the content installer (pre version 1.6) will remove existing permissions for users, including those with sysadmin rights. If uncertain, skip this step and confirm sysadmin access will not be lost then return to complete the Admin Tool step.



9. Click on the **Commit Changes** button when finished. You will be presented with a message asking if you want to grant the user additional security permissions. Click **Yes**.

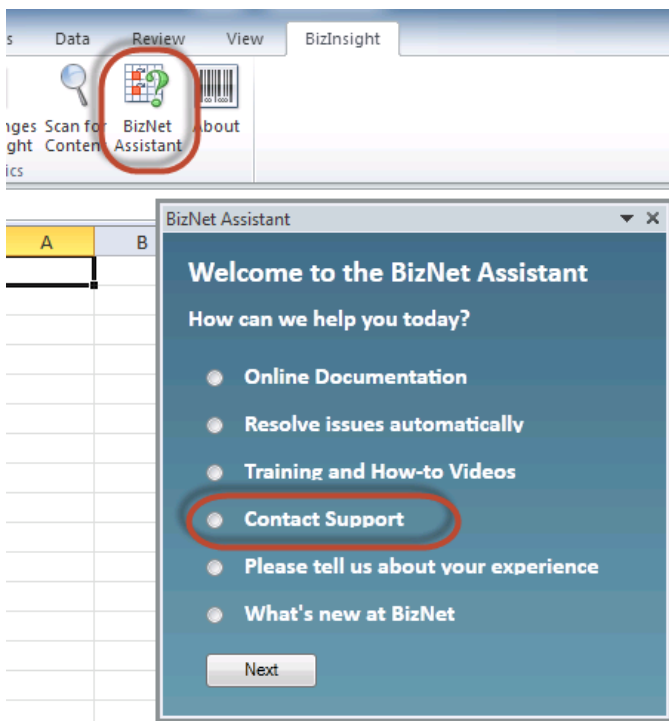


If you have entered more names for a particular user type than you have licenses, you will get an error similar to the following.



You will be returned to the **Current Users** dialog where you can remove a row so that you comply with the number of licenses your company purchased. Select the row to remove and click the **Delete Row** button.

To purchase additional licenses, use the BizNet Assistant button to open a support ticket indicating that you need to purchase additional licenses.



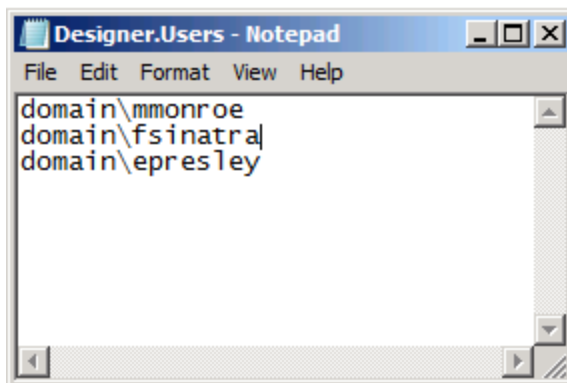
When you receive your new license, move your old license from the Administration Path shared directory and save the new license there. Do not rename the old license and leave it in the Administration Path; it must be removed from the directory in order for the new license count to take effect.

Manual Steps

1. In the Admin shared directory, open the .users file with Notepad that corresponds with the BizInsight permissions the user should have. For example, if the user should have Designer permissions, you would open the Designer.users file.

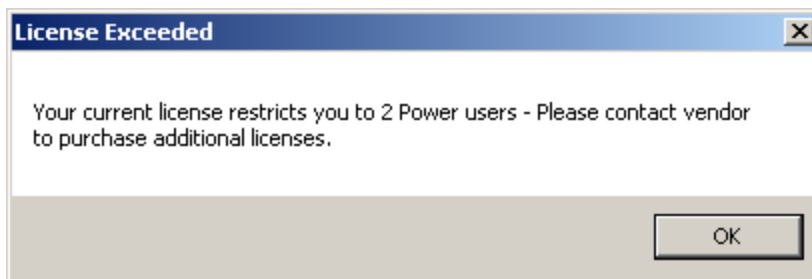
Tip If you are not sure where to find the Admin shared directory, go to an existing user's workstation, open Excel and click on the **Application Settings** button on the BizInsight ribbon and copy the path provided for the Administration Path.

2. In the .users file, add the Windows account name of the BizInsight user. For more information on the different user types, refer to the User Types section of the User Guide.



3. Save and close the file.

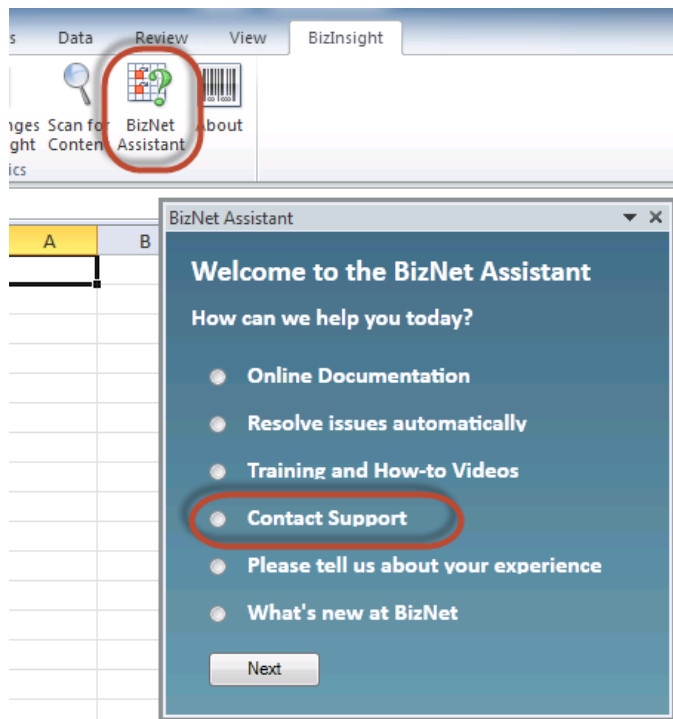
IMPORTANT As you add Windows account names to the .users files, add only as many as you have licenses. If you add more Windows account names than you have licenses or you have an extra line return in the file, users will get an error message similar to the following when they open Excel after BizInsight is installed.



If you are not sure how many licenses you have, open the .lic file that is in the Admin

shared directory with Notepad and check how many licenses are shown for the user type you are adding.

To purchase additional licenses, use the BizNet Assistant button to open a support ticket indicating that you need to purchase additional licenses.



When you receive your new license, move your old license from the Administration Path shared directory and save the new license there. Do not rename the old license and leave it in the Administration Path; it must be removed from the directory in order for the new license count to take effect.