Creating a Patch Management Dashboard with IT Analytics
Hands-On Lab

Description	This lab provides a hands-on overview of the IT Analytics Solution. Students will learn how to browse cubes and configure Pivot Tables and Charts using a number of common usage scenarios. In addition, students will learn advanced report creation by using the Report Builder to create and publish their own SQL Server Reporting Services report.

At the end of this lab, you should be able to	Understand the features and benefits of IT Analytics and be able to create your own reports and dashboards.
	▪ Understand the basics of an OLAP cube and how to browse them for data mining.
	▪ Configure reports and charts using Pivot Tables and Pivot Charts.
	▪ Configure a Key Performance Indicator.
	▪ Create and publish a SQL Server Reporting Services chart using Report Builder.

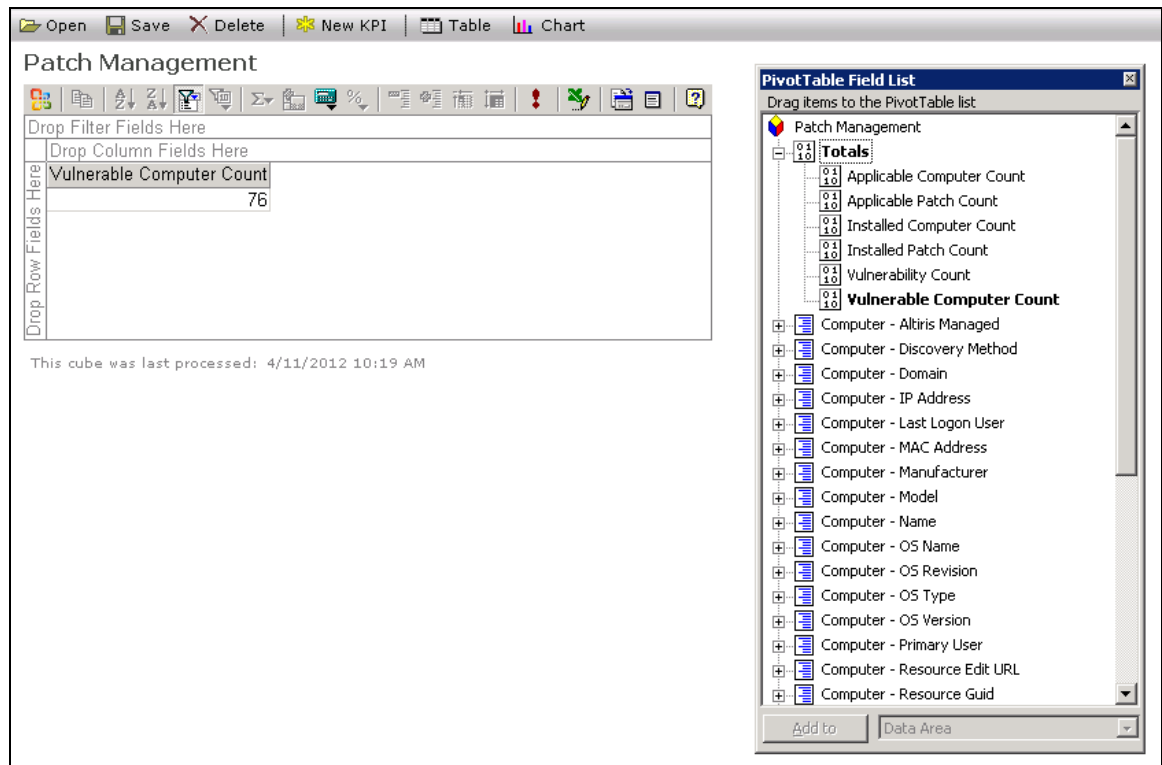|	
Notes	▪ A brief presentation will introduce this lab session and discuss key concepts.
	▪ The lab will be directed and provide you with step-by-step walkthroughs of key features.
	▪ Feel free to follow the lab using the instructions on the following pages. You can optionally perform this lab at your own pace.
	▪ Be sure to ask your instructor any questions you may have.
	▪ Thank you for coming to our lab session.

Introduction to IT Analytics

- What is IT Analytics™ Solution?
  - Leverages Business Intelligence to offer:
    - Advanced ad-hoc data-mining
    - Analyze Trends and historical information
    - Graphical dashboards and powerful reporting
  - Expands upon traditional reporting
  - Designed to facilitate analysis of information
  - Leverages OLAP cubes to provide multi-dimensional data exploration
  - Built on Standard Technologies (SQL Server Analysis and Reporting Services)
- What it enables you to do?
  - Continuously improve your IT Operations
  - Answers existing scalability issues
  - Resources & time savings
- Who is it intended for?
  - New and existing Symantec Management Platform (SMP) clients
    - Optimize your Altiris investment
    - Drill through your Symantec CMDB to mine the right information at the right time
    - Make it easy for users to understand your complex environment
    - Identify trends and opportunities faster
    - Accelerate the decision making process
    - Make fully informed decisions about your organization's performance.
    - Continuously measure & continuously improve

Configure Pivot Tables and Pivot Charts

Exercise 1: Configure a PivotTable report

Using the ad-hoc data mining capabilities of IT Analytics we will perform some forensic analysis of the AntiVirus policy settings that have been applied within the Symantec Endpoint Protection Manager.

1. Launch the Altiris Console by double clicking the Symantec Management Console 7.1 shortcut on the desktop.

2. Click the Reports menu item and select All Reports.

3. Expand the Reports folder.

4. Expand the IT Analytics folder.

5. Expand the Cubes folder.

6. Select the Patch Management Cube.

7. Click Ok when prompted.

8. Click anywhere in the PivotTable window to display the Field List. Clicking on this icon 🔲 in the toolbar will also cause the field list to be displayed.

9. Drag and drop the Vulnerable Computer Count measure into the Totals pane:

10. Drag and drop the Software Update - Provider attribute into the Rows pane:

11. Drag and drop the Software Update - Reference attribute –after the Software Update - Provider attribute and expand one of the Software Update Providers to show the Updates available for the Provider:

| Open | Save | Delete | New KPI | Table | Chart |

Patch Management

Drop Filter Fields Here

Software Update - Provider ▾	Software Update - Reference ▾	Vulnerable Computer Count
⊞ 7-Zip		2
⊟ Adobe Systems	APSB09-03	2
	APSB10-21	1
	APSB10-28	2
	APSB11-03	4
	APSB11-06	1
	APSB11-16	5
	APSB11-24	8
	APSB11-27	1
	APSB11-28	36
	APSB11-30	2
	MS06-069	3
	Total	38
⊞ Apple		9
⊞ Microsoft		76
⊞ Mozilla		2
⊞ Research In Motion		1
⊞ Skype Technologies S.A.		5
⊞ Sun Microsystems		16
Grand Total		76

This cube was last processed: 4/11/2012 10:19 AM

PivotTable Field List

Drag items to the PivotTable list

- ⊞ Computer - Manufacturer
- ⊞ Computer - Model
- ⊞ Computer - Name
- ⊞ Computer - OS Name
- ⊞ Computer - OS Revision
- ⊞ Computer - OS Type
- ⊞ Computer - OS Version
- ⊞ Computer - Primary User
- ⊞ Computer - Resource Edit URL
- ⊞ Computer - Resource Guid
- ⊞ Computer - Resource Manager URL
- ⊞ Computer - Serial Number
- ⊞ Computer - Server
- ⊞ Computer - System Type
- ⊞ Filter - Name
- ⊞ Organizational Group - Name
- ⊞ Software Update - Bulletin Enabled
- ⊞ Software Update - Custom Severity
- ⊞ Software Update - File Name
- ⊞ **Software Update - Provider**
- ⊞ Software Update - Reboot Required
- ⊞ **Software Update - Reference**
- ⊞ Software Update - Severity

| Add to | Row Area |

Now that we have built our initial patch management view which showcases the number of vulnerable computers per software update, we will expand upon this view by bringing in more information and adding filtering capabilities.

12. Drag and drop the Software Update - Severity attribute into the Columns pane:

| Open | Save | Delete | New KPI | Table | Chart |

Patch Management

Drop Filter Fields Here

Software Update - Provider ▾	Software Update - Reference ▾	Critical Vulnerable Computer Count	Important Vulnerable Computer Count	Low Vulnerable Computer Count	Moderate Vulnerable Computer Count	Unclassified Vulnerable Computer Count	Grand Total Vulnerable Computer Count
⊞ 7-Zip						2	2
⊟ Adobe Systems	APSB09-03	2					2
	APSB10-21	1					1
	APSB10-28	2					2
	APSB11-03	4					4
	APSB11-06	1					1
	APSB11-16	5					5
	APSB11-24	8					8
	APSB11-27					1	1
	APSB11-28	36					36
	APSB11-30	2					2
	MS06-069	3					3
	Total	37				1	38
⊞ Apple						9	9
⊞ Microsoft		71	69	62	62	76	76
⊞ Mozilla						2	2
⊞ Research In Motion						1	1
⊞ Skype Technologies S.A.						5	5
⊞ Sun Microsystems						16	16
Grand Total		74	69	62	62	76	76

This cube was last processed: 4/11/2012 10:19 AM

a. Resize\Move the Pivot Table Field List box to optimize your view of the Patch Cube data.

13. Right Click on the Critical column and select Filter by Selection.

14. Drag Software Update - Severity from the Columns pane into the filter pane.

Software Update - Provider ▾	Software Update - Reference ▾	Vulnerable Computer Count
⊟ Adobe Systems	APSB09-03	2
	APSB10-21	1
	APSB10-28	2
	APSB11-03	4
	APSB11-06	1
	APSB11-16	5
	APSB11-24	8
	APSB11-28	36
	APSB11-30	2
	MS06-069	3
	Total	37
⊞ Microsoft		71
Grand Total		74

This cube was last processed: 4/11/2012 10:19 AM

15. Drag the Computer – OS Name attribute from the field list directly into the Filter
pane.

| Open | Save | Delete | New KPI | Table | Chart |

Patch Management

Software Update - Severity ▼	Computer - OS Name ▼	
Critical	All	

		Drop Column Fields Here

Software Update - Provider ▼	Software Update - Reference ▼	Vulnerable Computer Count
⊟ Adobe Systems	APSB09-03	2
	APSB10-21	1
	APSB10-28	2
	APSB11-03	4
	APSB11-06	1
	APSB11-16	5
	APSB11-24	8
	APSB11-28	36
	APSB11-30	2
	MS06-069	3
	Total	37
⊞ Microsoft		71
Grand Total		74

This cube was last processed: 4/11/2012 10:19 AM

16. Click on the dropdown arrow for the Computer – OS Name attribute in the Filter page and select only Microsoft Windows XP, Windows 7 Professional and Windows 7 Ultimate and click OK.

17. Drag in the Computer - Name attribute into the Rows pane before the Software Update – Provider attribute to see the critcal software updates that are missing per computer.

18. Finally you can save this report by clicking this icon ![Save] in the toolbar.

19. Select the "Save as new view" radio button and name it appropriately.

20. You may also check the "Available to all users" checkbox in the event that you would like this report to be available to all users. Leaving this unchecked will make this a private view only available to you.

21. Refresh the SMP Console and navigate back to the Patch Management Cube (Reports > IT Analytics > Cubes). This will bring you back to the initial Patch Management screen.

22. To open the view you just saved click this icon 🗁 Open in the toolbar and select the report you just created in the dropdown list. Note that the report is loaded exactly as you left it.

Exercise 2: Configure a Pivot Chart report

Using the Patch Management Cube we will create a Chart that will allow us to see the Installed versus Vulnerable counts of Adobe Patches on Windows Servers.

1. Launch the Altiris Console by double clicking the Symantec Management Console 7.1 shortcut on the desktop.

2. Click the Reports menu item and select All Reports.

3. Expand the Reports folder.

4. Expand the IT Analytics folder.

5. Expand the Cubes folder.

6. Select the Patch Management Cube.

7. .Click this icon [chart icon] in the toolbar.

8. Click inside the Pivot Chart to display the Field List.

9. Click this icon [icon] in the toolbar above the pivot chart.

10. From the Commands and Options dialog window select Bar and then the first chart type.
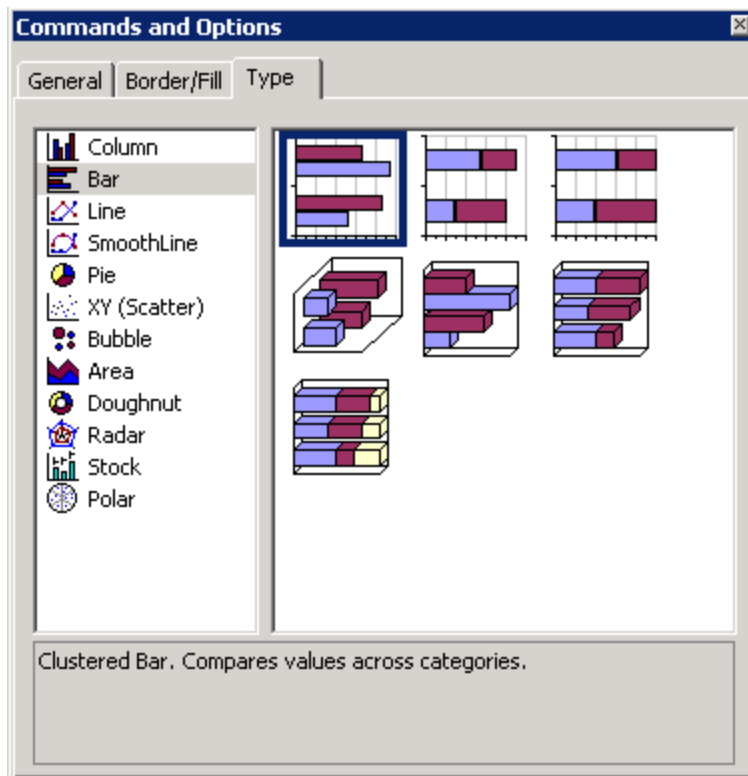
11. Close 'Commands and Options' window using the 'X' on the top right of the pane.

12. Drag and drop the Installed Computer Count and the Vulnerable Computer Count measures into the pivot chart.
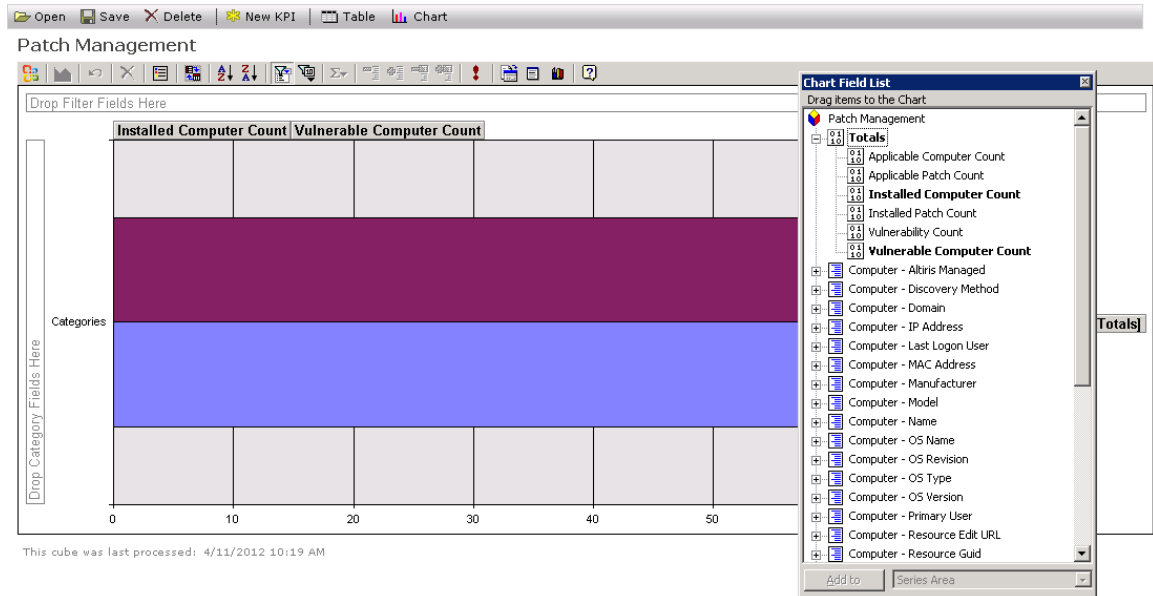
13. Drag and drop the Software Update – Provider attribute from the field list to the filter pane.
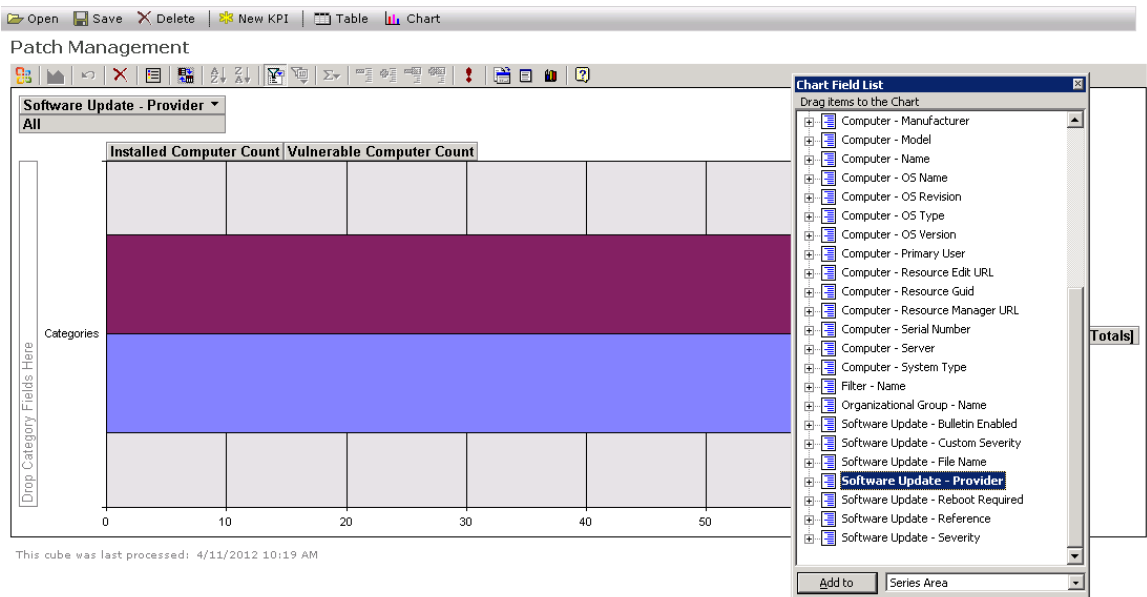
14. Click on the dropdown arrow on the Software Update – Provider attribute in the filter pane and select only Adobe Systems and click OK.
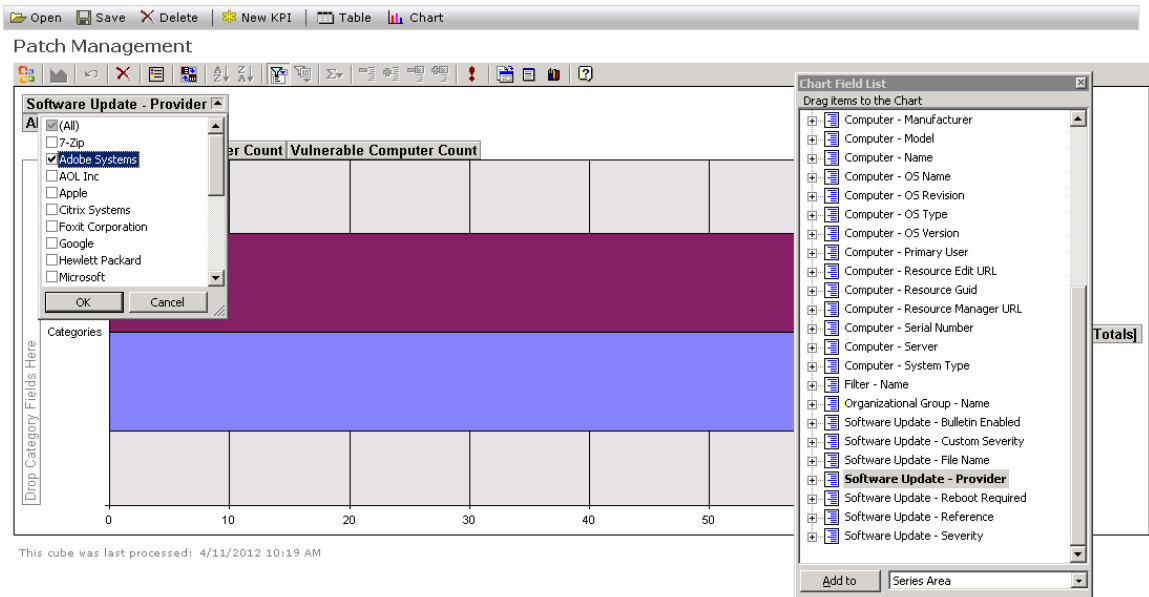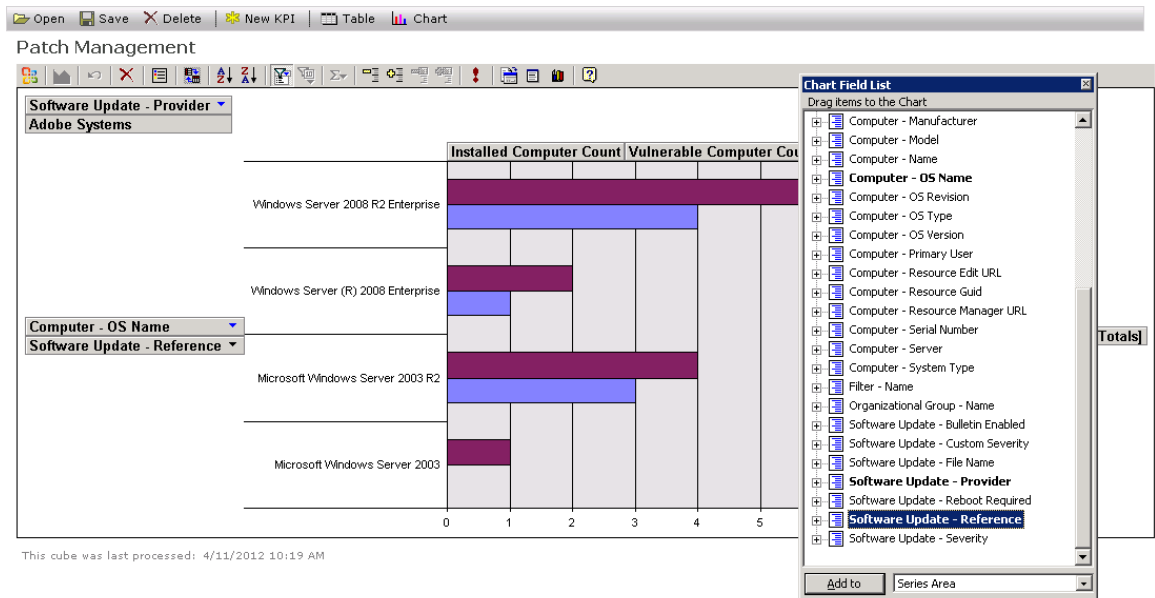

15. Drag and drop the Computer – OS Name attribute into the "Drop Category Fields Here" pane.
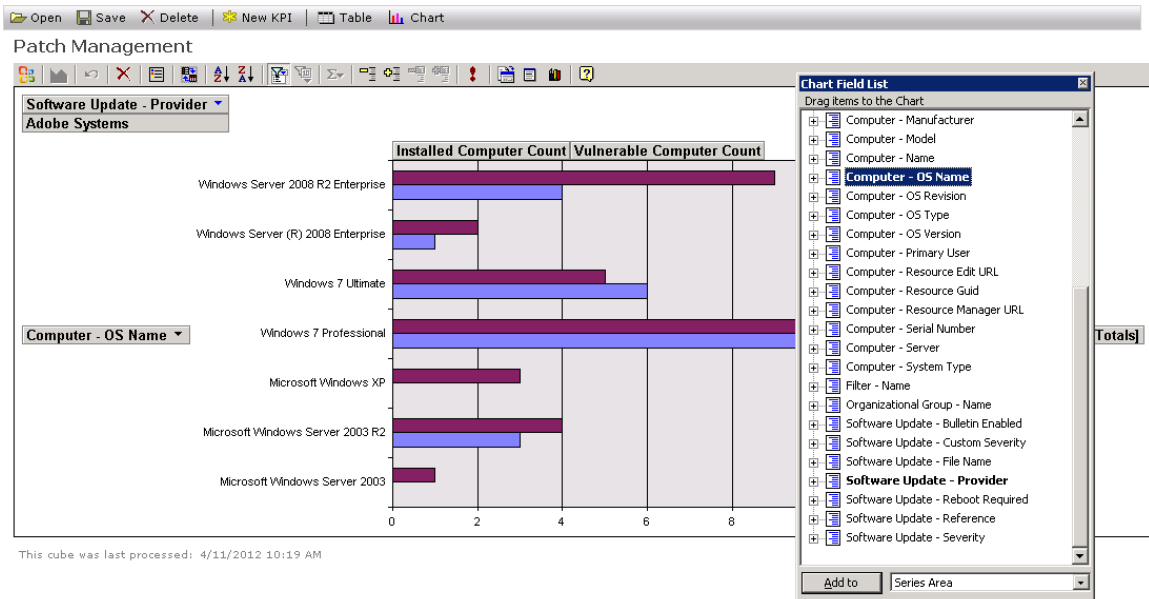
16. Click the dropdown arrow on the Computer – OS Name attribute in the category fields pane and select only Windows Server operating systems (i.e. Windows Server 2003, Windows Server 2008 R2 Enterprise, etc.) and click OK.
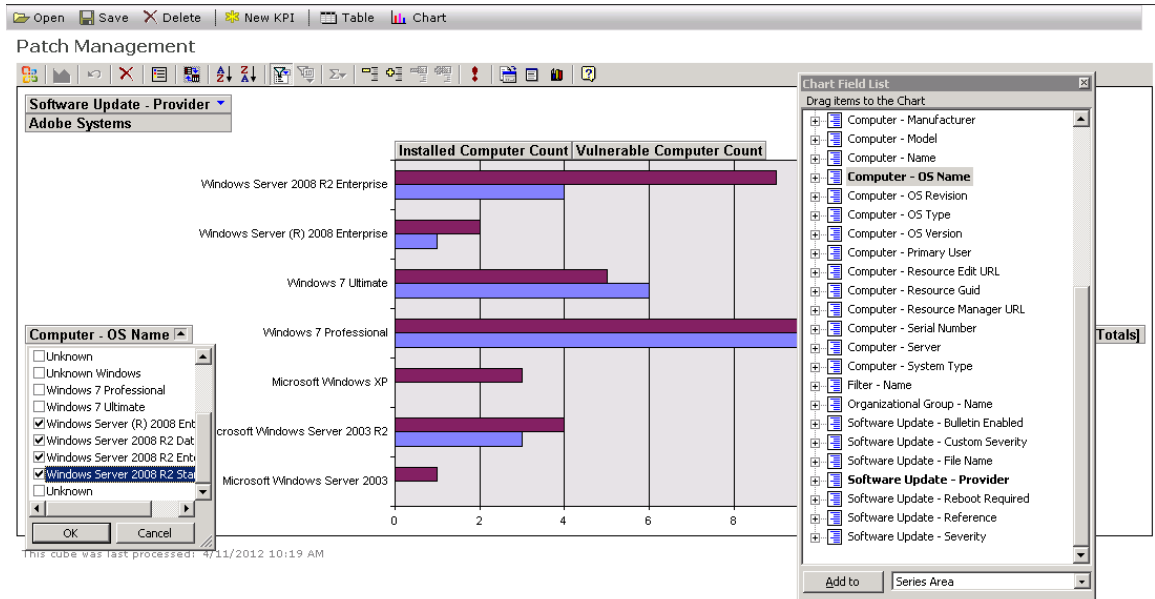
17. Drag and drop the Software Update - Reference attribute directly below the Computer – OS Name attribute in the category fields pane.

18. Right click on the Computer – OS Name attribute and select Expand.
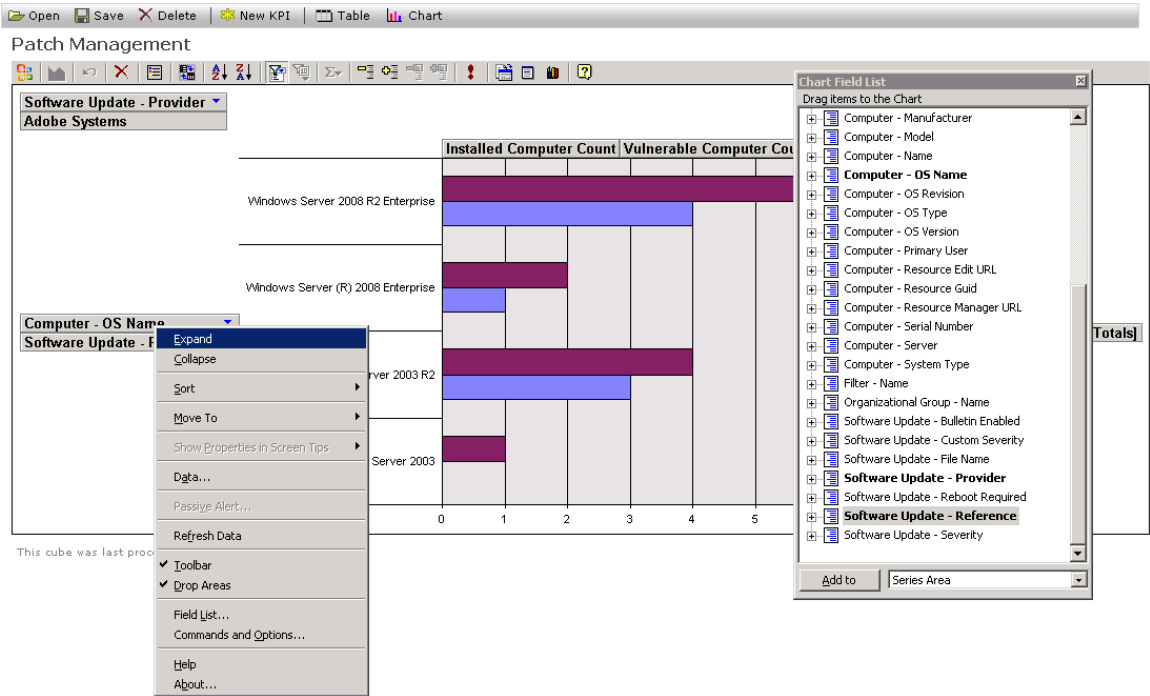
19. You should now see all of the patch references expanded for each of the server operating systems.
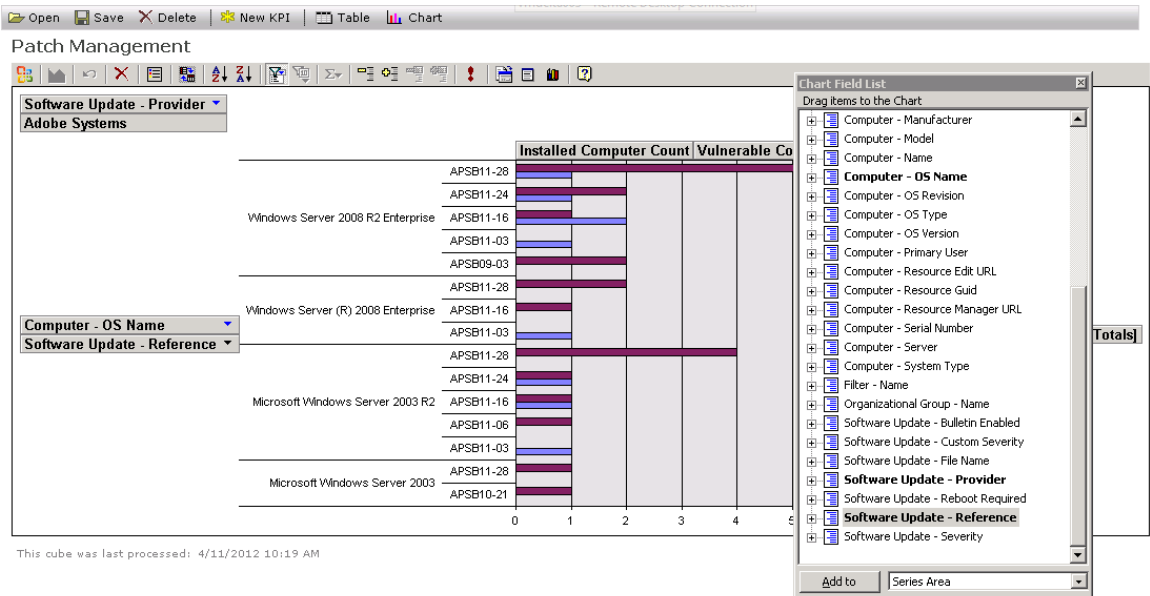
20. Close the field list and click this icon ☷ in the toolbar to expand the Legend.
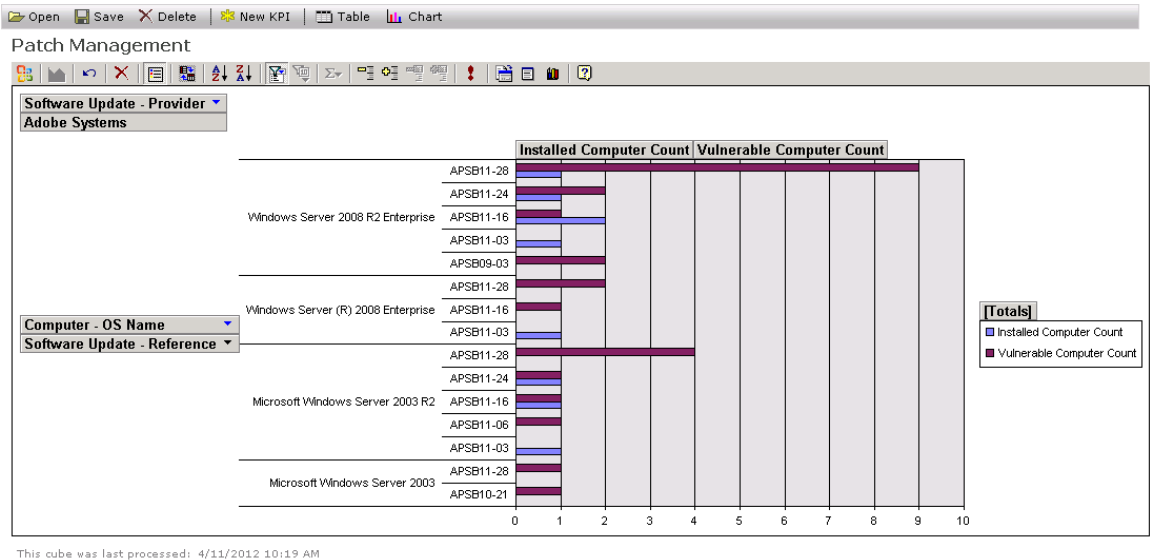
Now that we have the basic structure we are ready to do some formatting to make this chart easier to read.

21. Click this icon 🗔 in the toolbar to launch the Commands and Options window.
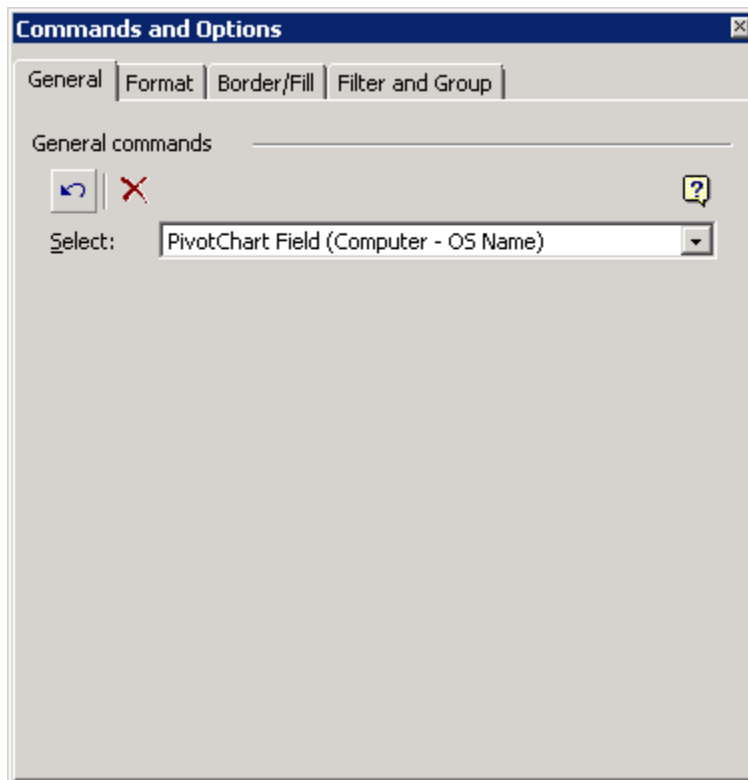
22. In the Commands and Options window select the Chart Workspace value from the dropdown list.

Commands and Options

General | Border/Fill | Data Details | Type | Series Groups | Show/Hide

General commands

Select: Chart Workspace

- Chart Workspace
- PivotChart Fieldset (Software Update - Provider)
- PivotChart Totals
- PivotChart Field (Computer - OS Name)
- PivotChart Total (Installed Computer Count)
- Legend
- Plot Area
- Category Axis 1
- Value Axis 1
- Value Axis 1 Major Gridlines
- Installed Computer Count
- Vulnerable Computer Count

Add

Chart

Overlap:

Gap width:

Wall Thickn

23. Click this icon ![icon] to add a Chart Title.

24. Now switch from Chart Workspace to Title in the dropdown list
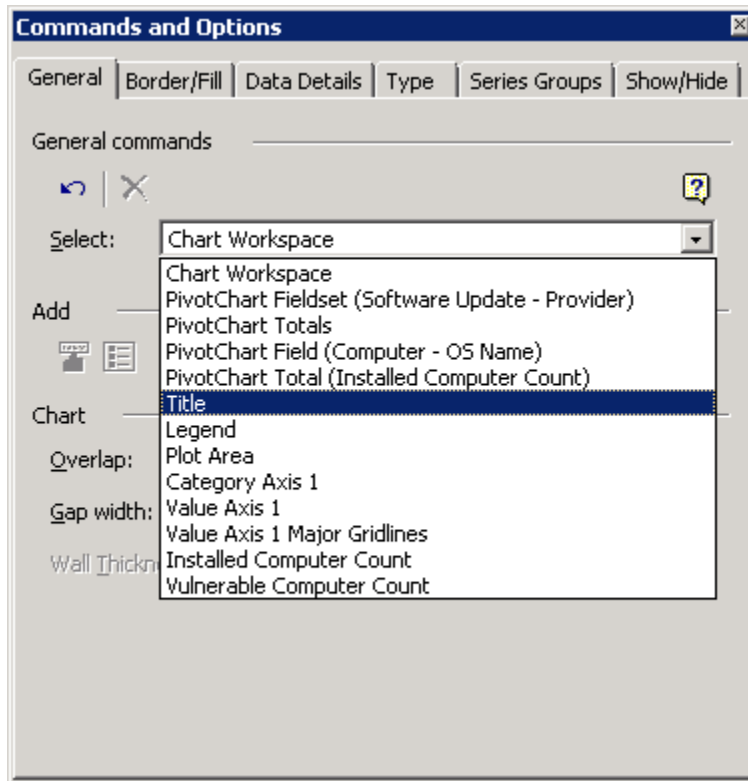
25. Select the Format tab and update the following:

    a. Change the font size from 12 to 14.

    b. Update the Caption text box at the bottom and replace "Chart Workspace Title" to "Adobe Patches – Installed vs. Vulnerable Server Count" or another appropriate title.

26. Click the General tab and switch from Title to Legend from the dropdown list.

Commands and Options

General | Format | Border/Fill

General commands

Select: Title

- Chart Workspace
- PivotChart Fieldset (Software Update - Provider)
- PivotChart Totals
- PivotChart Field (Computer - OS Name)
- PivotChart Total (Installed Computer Count)
- Title
- Legend
- Plot Area
- Category Axis 1
- Value Axis 1
- Value Axis 1 Major Gridlines
- Installed Computer Count
- Vulnerable Computer Count

27. Click the Format tab and change the Position from Right to Bottom.

28. Select the General tab and switch from Legend to Chart Workspace from the dropdown list.
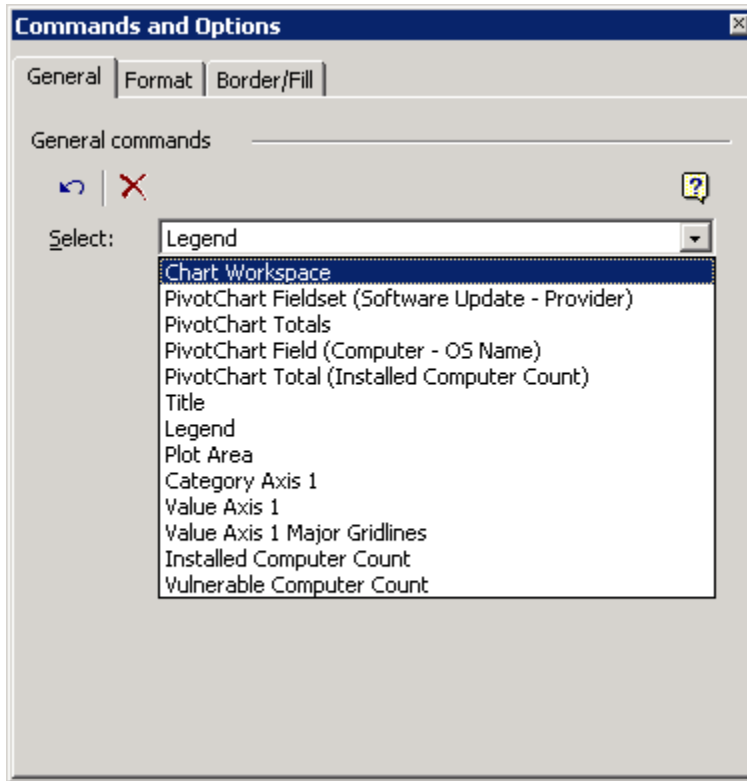
29. Select the Show/Hide tab and uncheck the "Field buttons/drop zones" checkbox.

    a. This will remove the drop panes to make the chart appear cleaner.

30. Close the Commands and Options window.
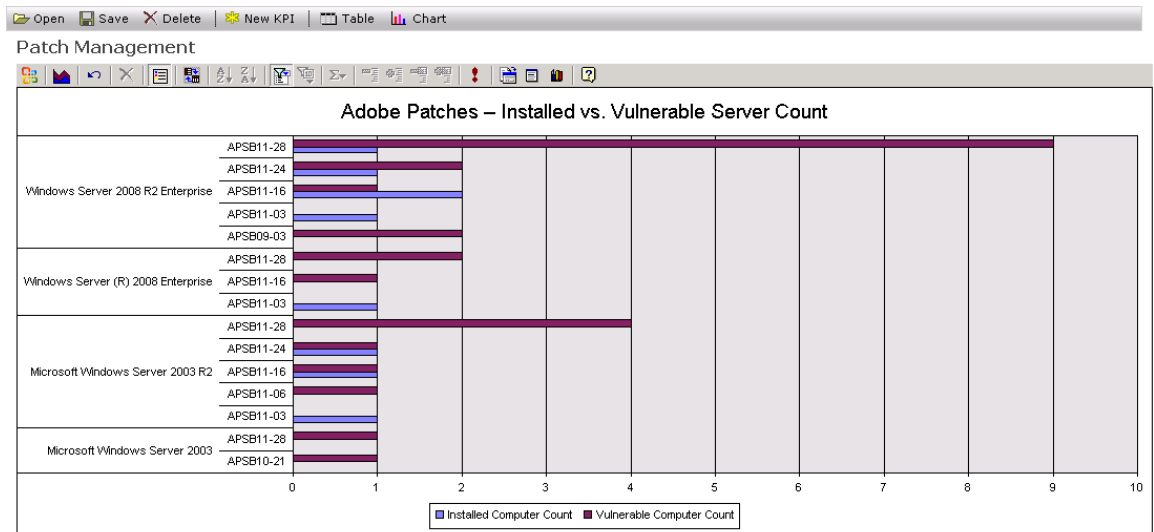
31. Finally click the Save icon ⊟ Save and name this chart appropriately to save it for later use.

Save Cube View -- Webpage Dialog

⦿ Save as new view: es – Installed vs. Vulnerable Server Count

○ Save as existing view: Workstation Critical Vulnerabilities per ▼

☐ Available to all users

Save   Cancel
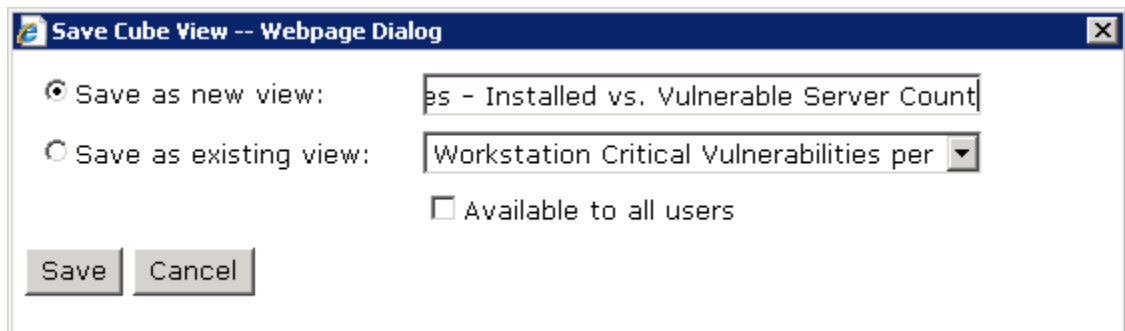
Exercise 3: Configure a Key Performance Indicator

Using the Patch Management Cube we will create a KPI that will allow for the monitoring the Patch Installations versus Patch Applicability for a specific softoware provider bulletin.

1. Select the Patch Management Cube.

2. Drag both the Installed Computer Count and Applicable Count totals into the data pane.

3. Drag and drop the Software Update - Provider attribute into the rows pane.

4. Drag and drop the Software Update - Severity attribute into the filters pane.

5. Select the drop-down menu for the Software Update - Severity filter and select the box for Citical.

6. Drag and drop the Software Update - Reference attribute into the filters pane.

7. Select the Software Update Reference APSB11-28.

8. Right click on the Installed Computer County value Software Update Reference APSB11-28 and the select Use as KPI Value.

9. In the "New Key Performance Indicator pane change the Goal radio button from None to Dynamic. This will allow us to choose another cube value as our Goal to compare our KPI against.

10. Now Right click on the AdobeApplicable Computer Count value in the and select Use as KPI Goal. This will allow us to compare our KPI to the total number of applicable computers.

Open Save Delete | New KPI | Table Chart

Patch Management

New Key Performance Indicator

You have selected the following **KPI Value** definition:

Software Update - Severity	Including -Critical
Software Update - Reference	APSB11-28
Software Update - Provider	Adobe Systems
Measure	Installed Computer Count

Select the type of goal that should be used for this KPI:
○ None ● Dynamic ○ Fixed

To define a dynamic Goal for this KPI, right click on a value from the details area of the view below and choose **Use as KPI Goal**.

Use as KPI Value
Use as KPI Goal
Display Resource List

Copy
Delete

Remove Total

Show Details

Sort Ascending
Sort Descending

Show Only the Top   ▶
Show Only the Bottom   ▶
Show As   ▶

Commands and Options...

PivotTable Field List

Drag items to the PivotTable list

- Computer - OS Revision
- Computer - OS Type
- Computer - OS Version
- Computer - Primary User
- Computer - Resource Edit URL
- Computer - Resource Guid
- Computer - Resource Manager URL
- Computer - Serial Number
- Computer - Server
- Computer - System Type
- Filter - Name
- Organizational Group - Name
- Software Update - Bulletin Enabled
- Software Update - Custom Severity
- Software Update - File Name
- **Software Update - Provider**
- Software Update - Reboot Required
- **Software Update - Reference**
- **Software Update - Severity**

Add to	Row Area

Software Update - Severity ▼
Critical

Drop Column Fields

Software Update - Provider ▼	Software Update - Reference ▼	Applicable Computer	
⊟ Adobe Systems	APSB09-03		
	APSB10-21		
	APSB10-28		1
	APSB11-03		5
	APSB11-06		1
	APSB11-08		1
	APSB11-16		5
	APSB11-24		7
	APSB11-28	37	12
	APSB11-30	2	
	MS06-069	3	
	Total	41	26
⊞ Microsoft		76	73
Grand Total		76	73

11. Click the Create KPI button.

12. In the Key Performance Indicator Window type "Computers with the Abobe Patch APSB11-28 Vulnerability" in the KPI Name textbox.

13. In the Status Expression dropdown box select "Percentage of Goal".

14. In the Status Graphic dropdown box select "Cylinder"

15. Click the Save KPI button.

16. When the screen refreshes click the "Close" button.

17. Click OK on the Windows Message box to reload the page.
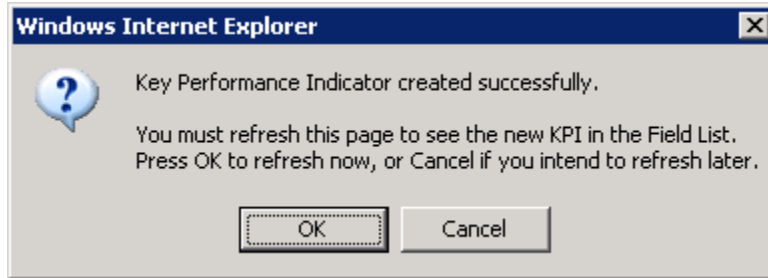
18. Click the Key Performance Indicator item from the left tree navigation.

KPI Name	Cube Name	Value	Goal	Status	Trend	
7Zip Patch Vulerability	Patch Management	22	24			Edit Delete
Application Denials This Month	Application Metering	0	0		→	Edit Delete
Computers with the Abobe Patch APSB11-28 Vulnerability	Patch Management	12	37			Edit Delete
Avg Events per Computer per Day in Last 30 Days	Monitor NT Events	0	10		→	Edit Delete
Avg Hours to Close Incidents	ServiceDesk Incidents	48.3	48			Edit Delete
Avg Percent Bandwidth Utilization in Last 30 Days	Monitor Metrics	0	20		→	Edit Delete
Avg Percent Disk Time in Last 30 Days	Monitor Metrics	0	20		→	Edit Delete
Avg Percent Memory Available in Last 30 Days	Monitor Metrics	0	50		→	Edit Delete
Avg Percent Processor Time in Last 30 Days	Monitor Metrics	0	20		→	Edit Delete
Computers Metered This Month	Application Metering	0	30		→	Edit Delete
Computers Requiring Critical Updates	Patch Management	74	15			Edit Delete
Computers with 7-Zip Patch Vulnerabilities	Patch Management	22	24			Edit Delete
Computers with Critical Alerts in Last 30 Days	Event Console Alerts	0	100		→	Edit Delete
Computers with Error Events in Last 30 Days	Monitor NT Events		100			Edit Delete
Computers with the Abobe Patch APSB11-28 Vulnerability	Patch Management	12	37			Edit Delete
Incidents Opened in Last 30 Days	ServiceDesk Incidents	0	500		→	Edit Delete

Advanced Reporting

This section will dive into advanced report creation using Report Builder to create and publish a SQL Server Reporting Services report.

What is Report Builder

Report Builder is a component of SQL Server Reporting Services that allows ad-hoc reporting functionality enabling end users to build their own reports and charts. Users can then publish these reports into Reporting Services where they can be accessed and viewed.

Exercise 4: Create and publish a report using Report Builder

In this exercise we will create a pie chart that displays the trend of Software Updates.

1. Launch a new web browser and type in http://localhost/reports.
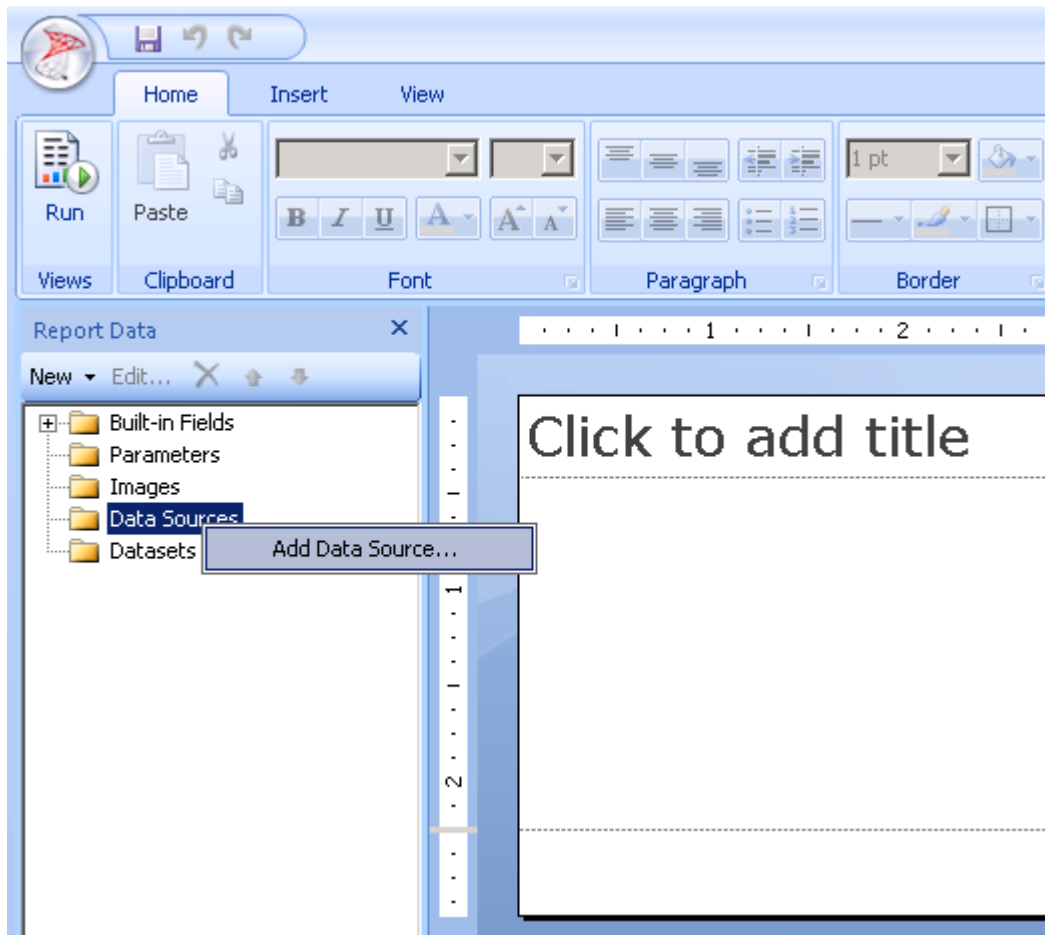2. Click Report Builder.
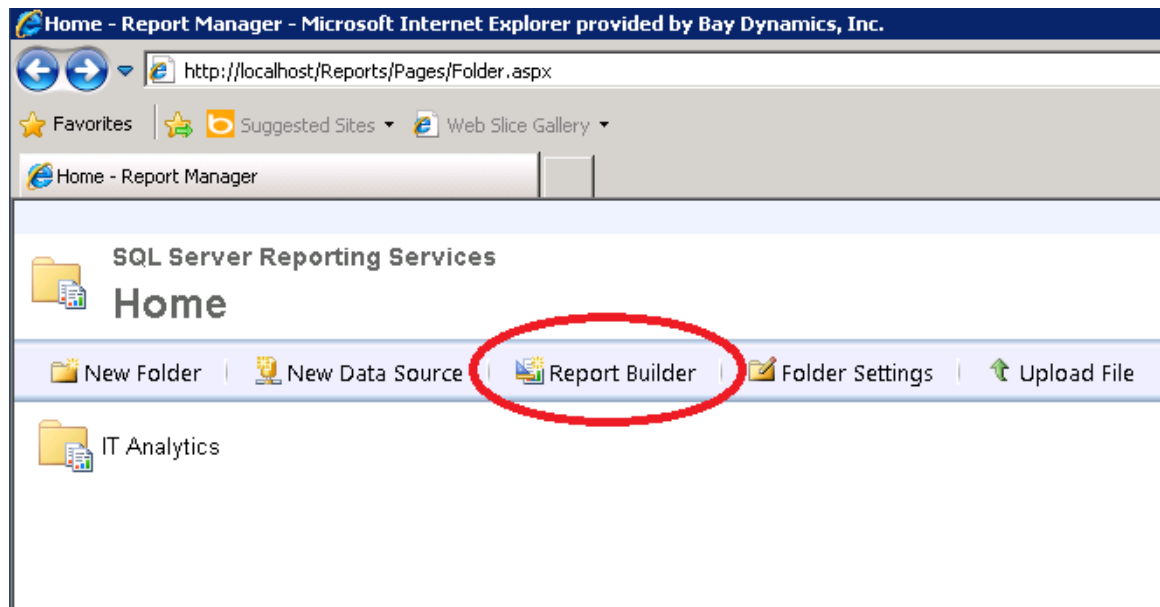
3. When Microsoft Report Building loads, click on the report body and in the Properties pane, expand Size and set the Width to 11in and Height to 8.5in.
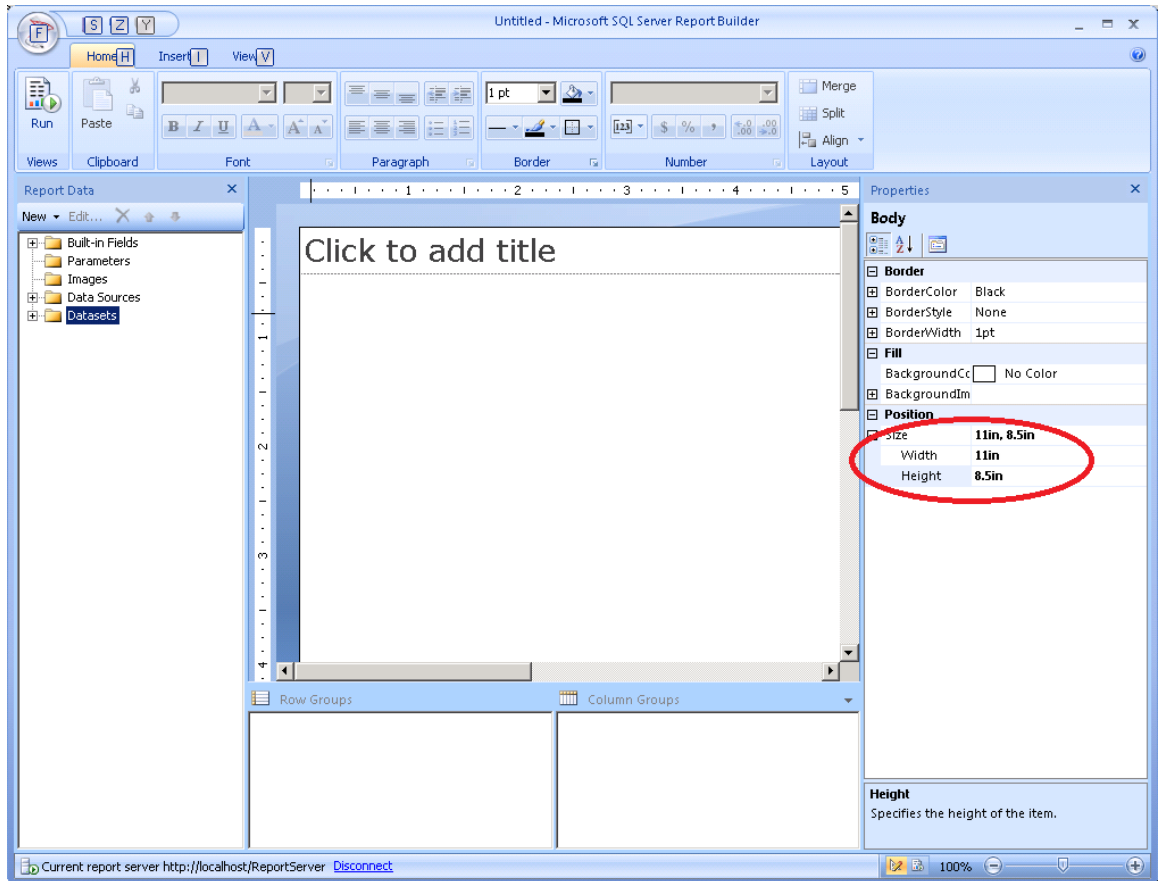
4. Click on the text "Click to add title" and type in Software Update Dashboard.
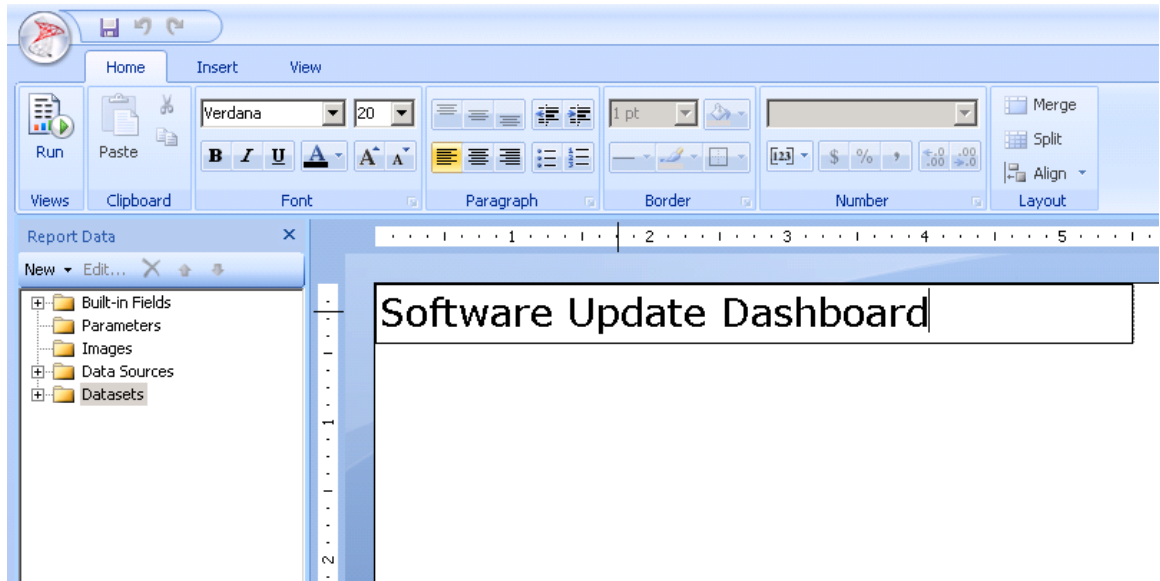
5. In the Report Data pane, right-click on Data Sources and select Add Data Source.

6. Enter ITAnalytics as the data source name and select the "Use a connection embedded in my report" radio button.
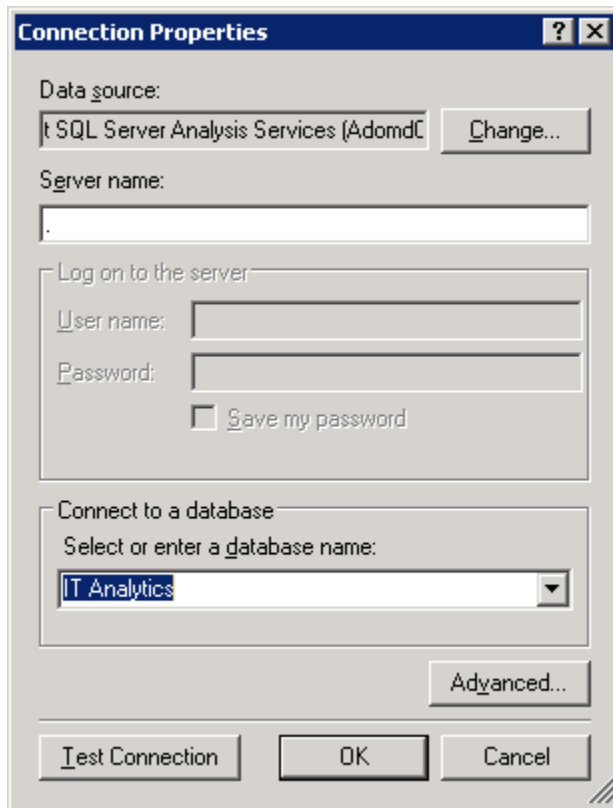
7. Click on the dropdown for "Select connection type" and select Microsoft SQL Server Analysis Services.
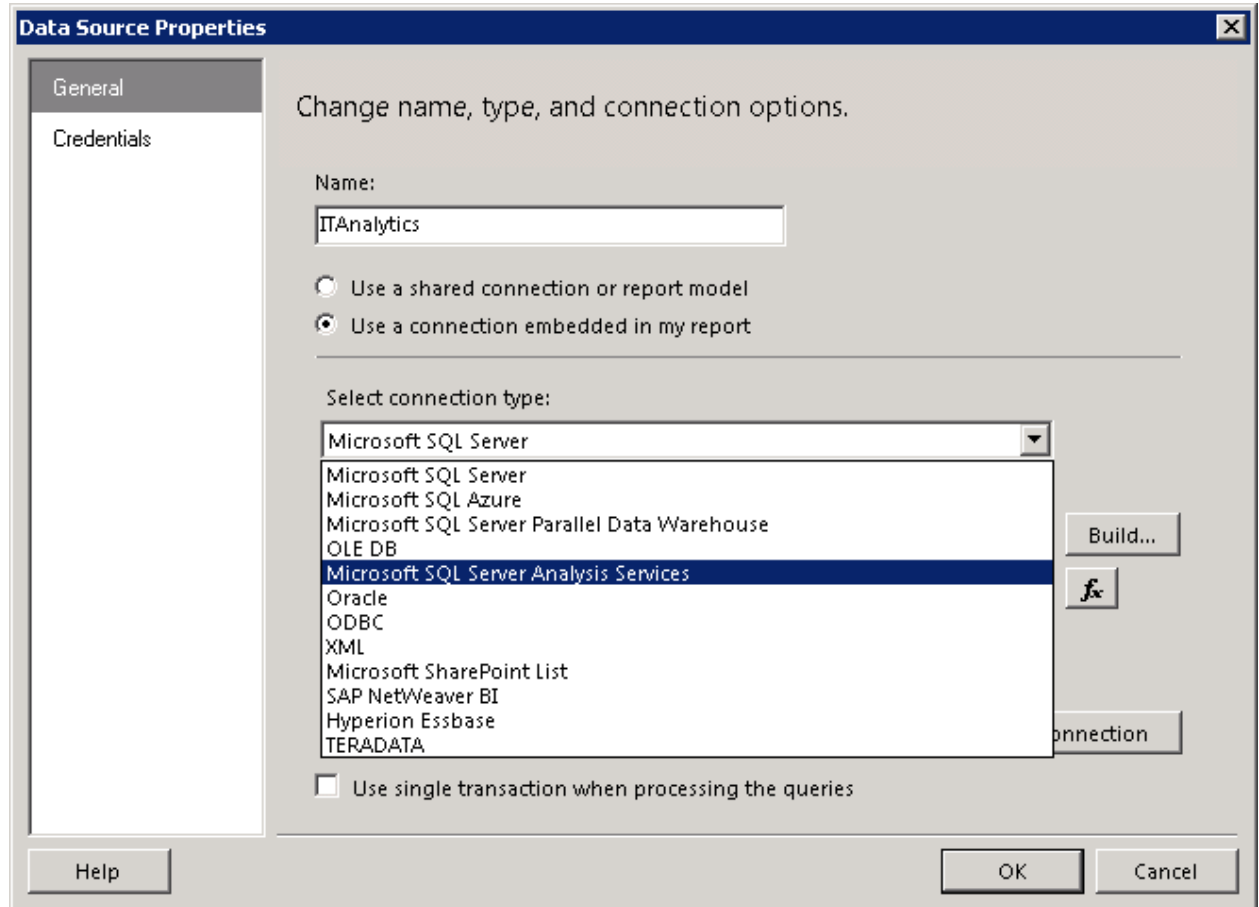
8. Click the build button in the Data Source Properties window.

9. In the Connection Properties window, enter . for the Server name, select IT Analytics as the database and click OK.
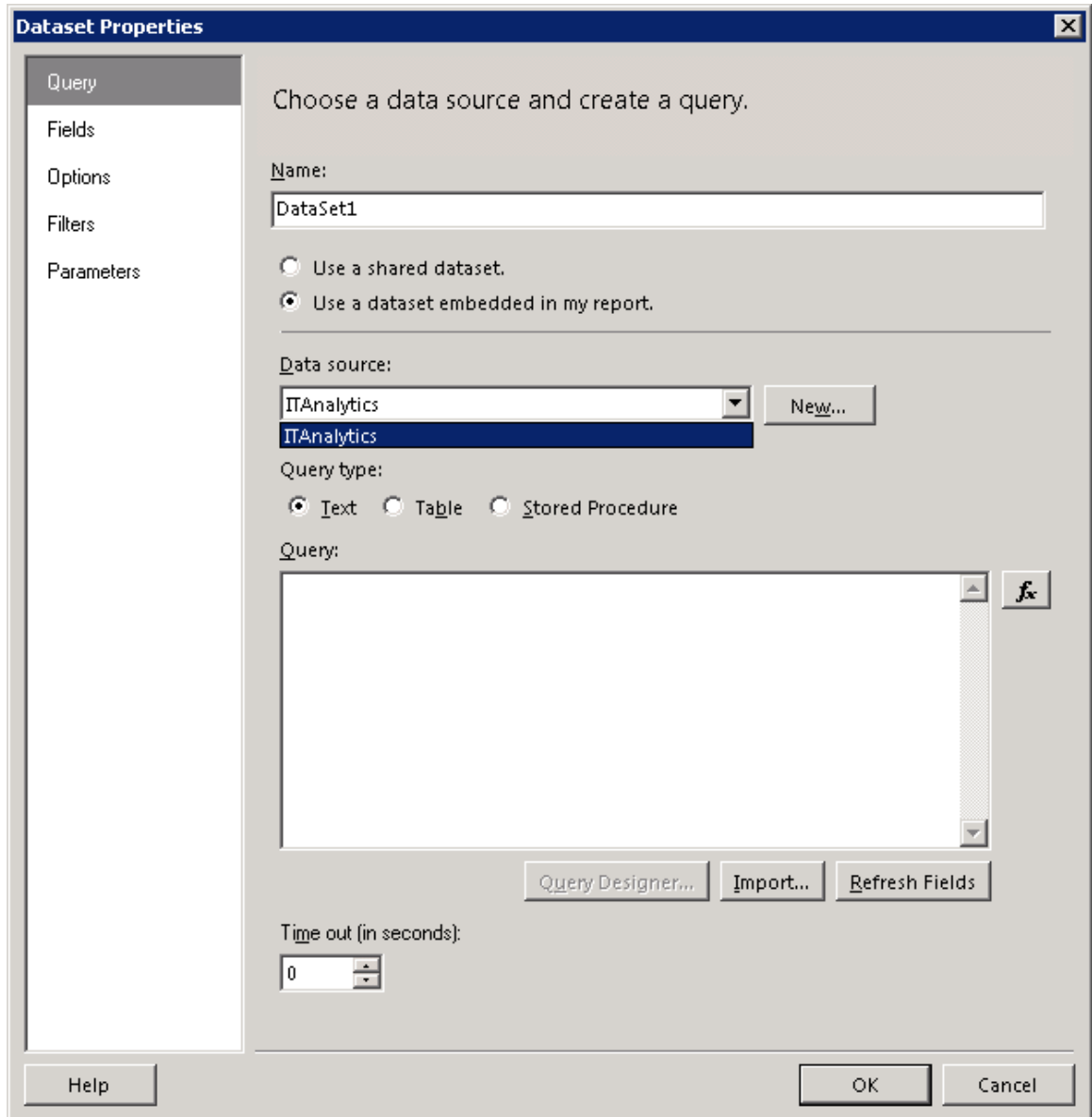

10. Click OK in the Data Source Properties window.
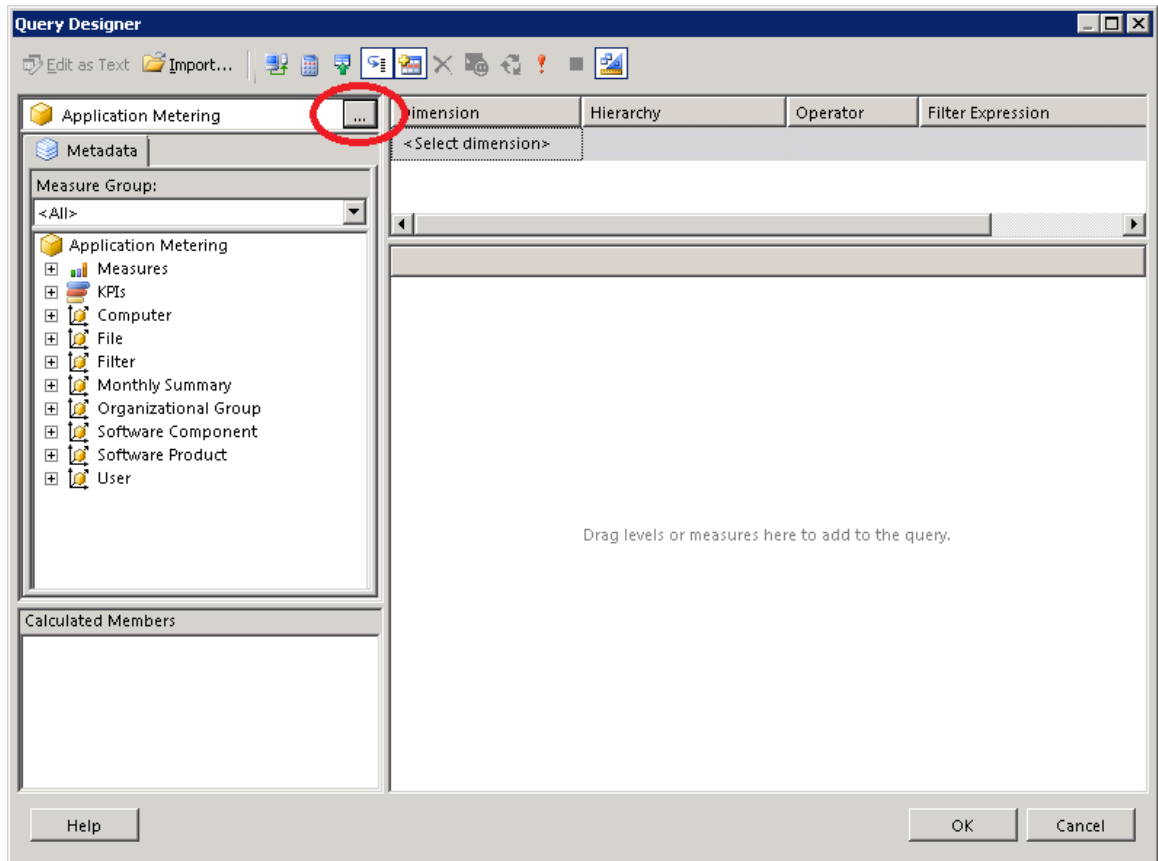
11. Right-click on Datasets and select Add Dataset.
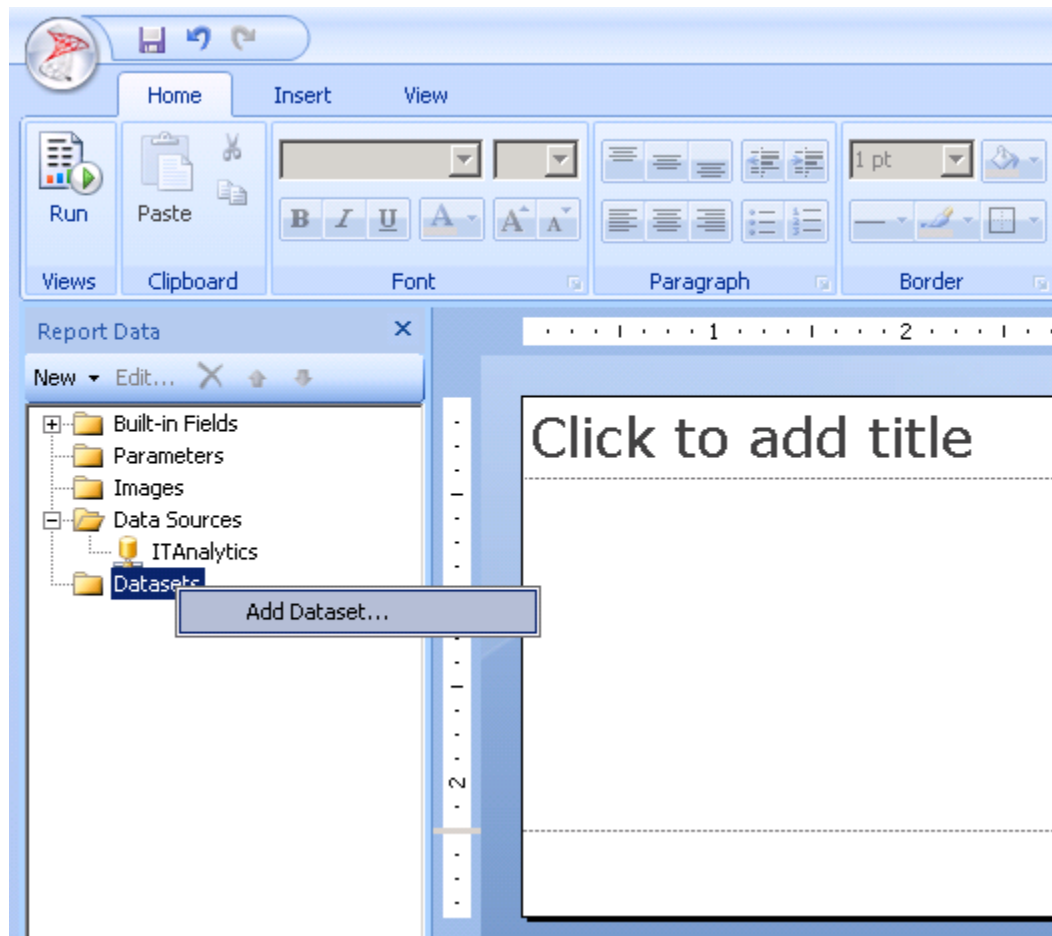
12. In the Dataset Properties window, select the "Use a dataset embedded in my report" radio button, click on the dropdown for Data source and select ITAnalytics.
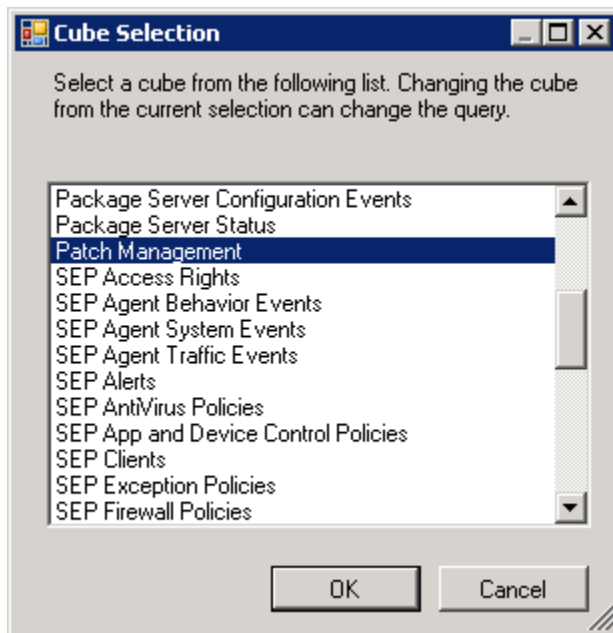

13. Click the Query Designer button in the Dataset Properties window.
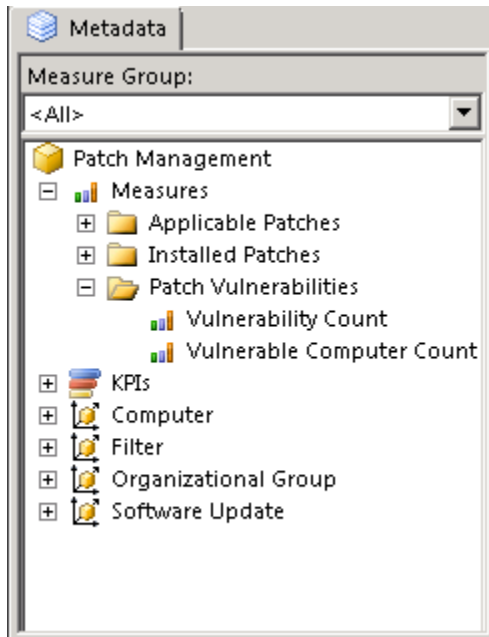
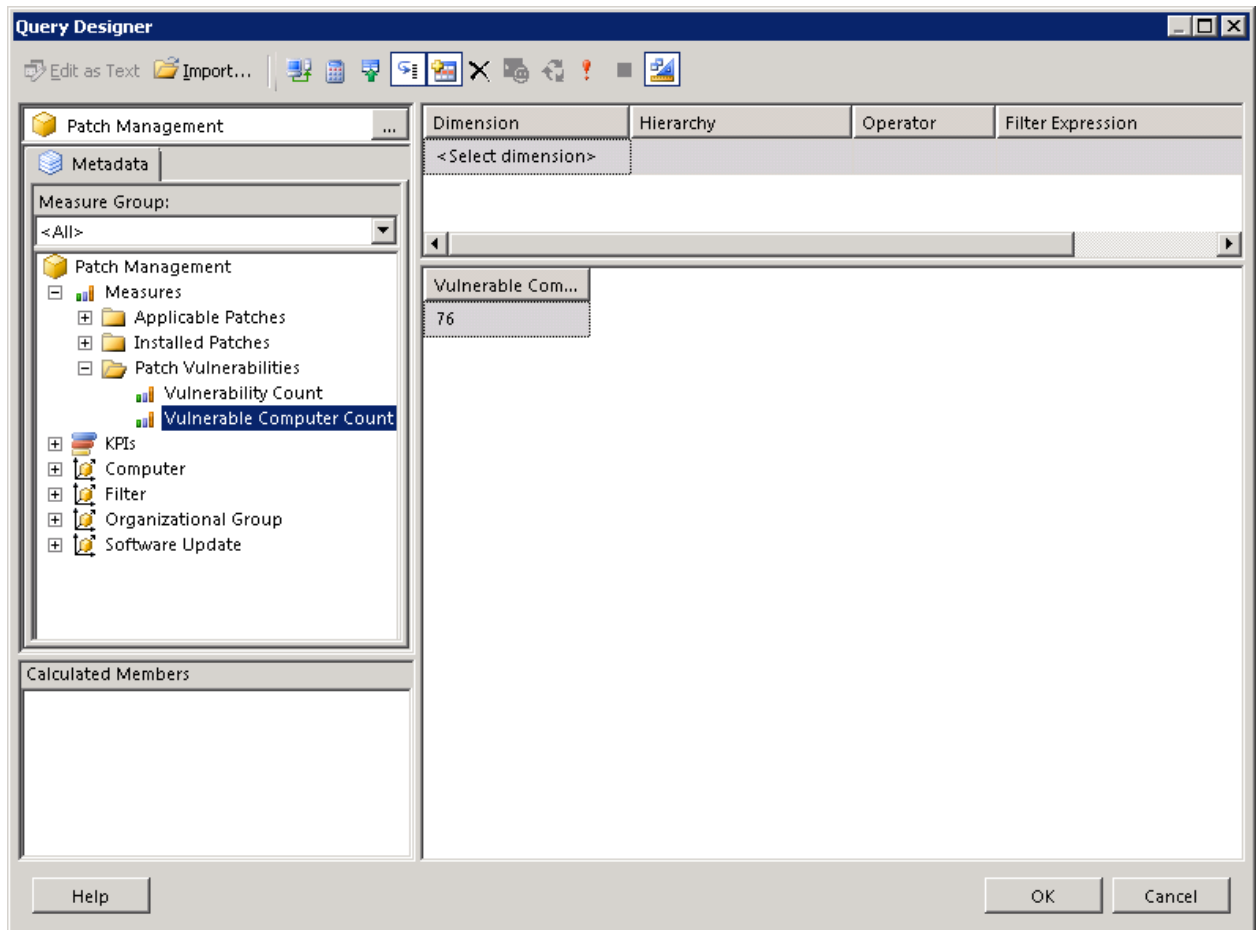14. Click the cube selector on the upper left part of the Query Designer.

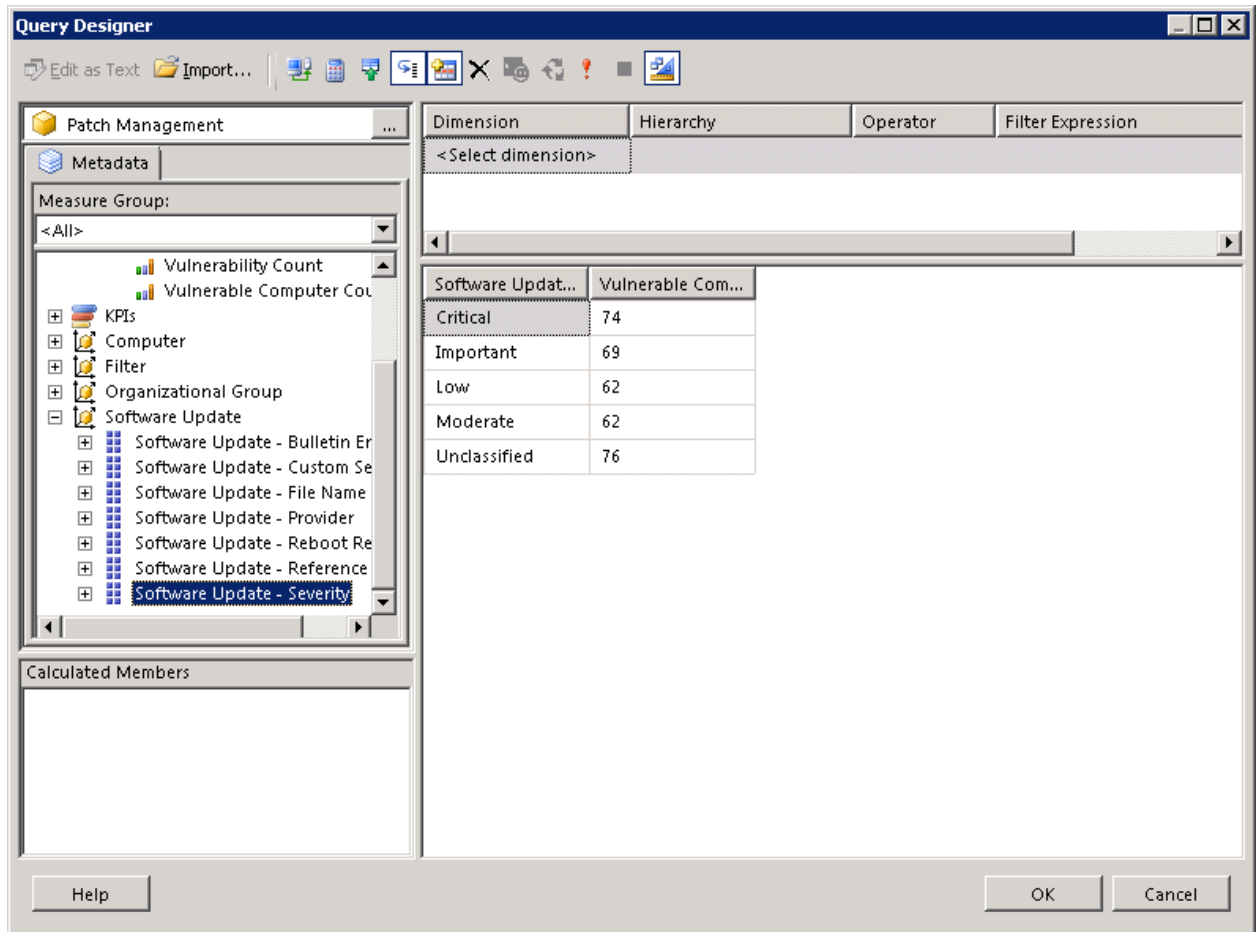15. Select Patch Management from the Cube Selection window.

16. In the Metadata pane of the Query Designer window, expand Measures > Patch Vulnerabilities.

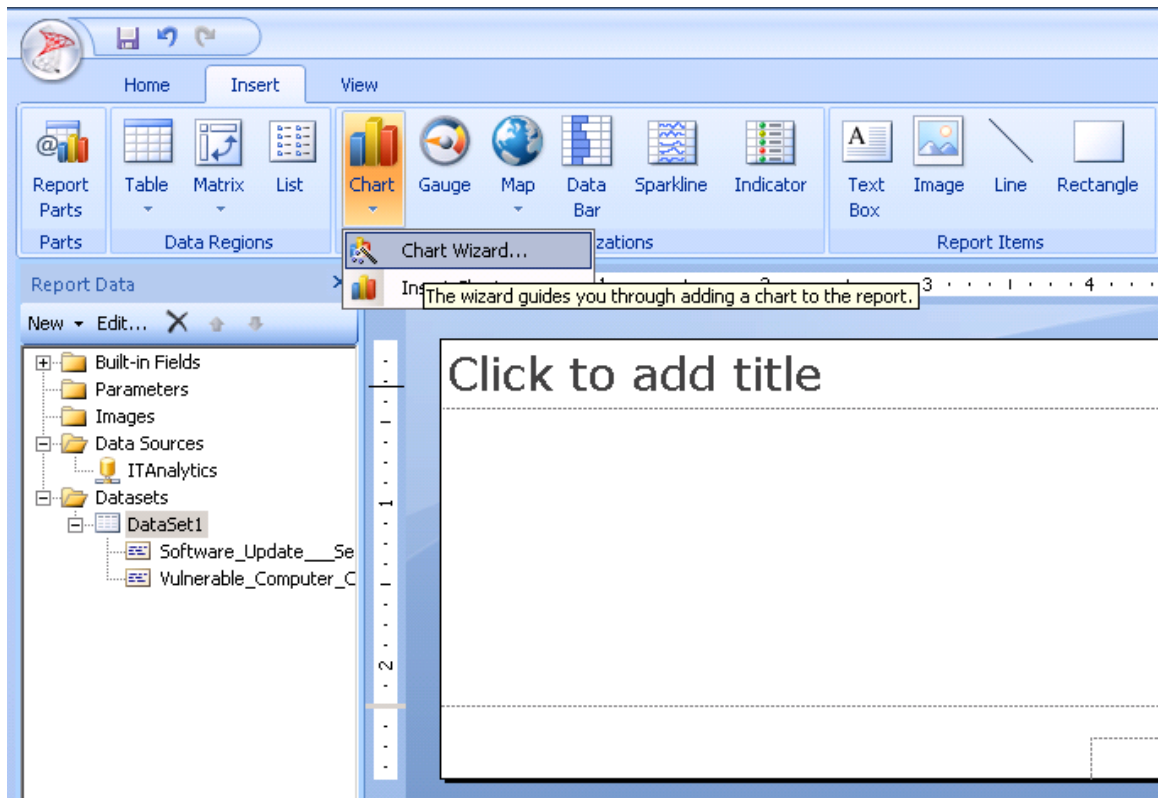17. Drag the Vulnerable Computer Count measure to the query pane.

18. Drag and drop the Software Update – Severity attribute to the query pane.
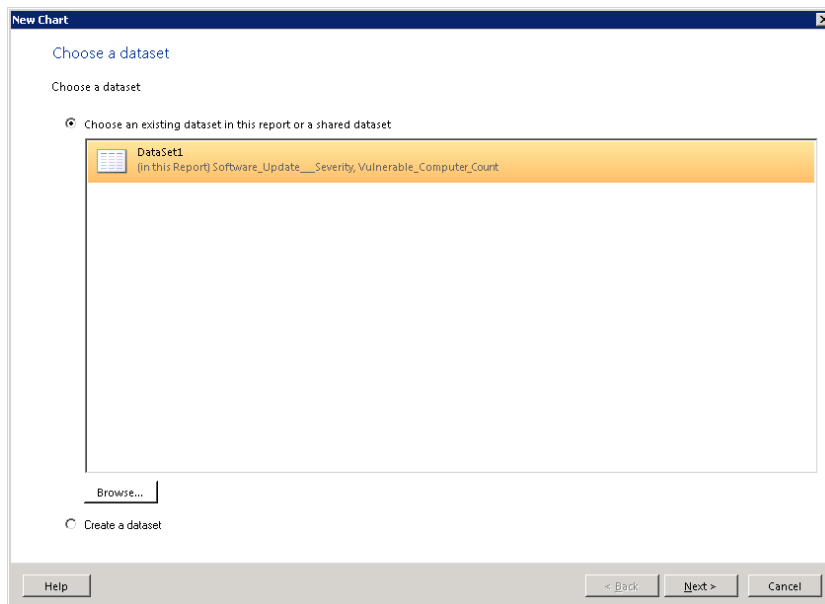

19. Click OK in the Query Designer window and the Dataset Properties window to go back to the main report builder.
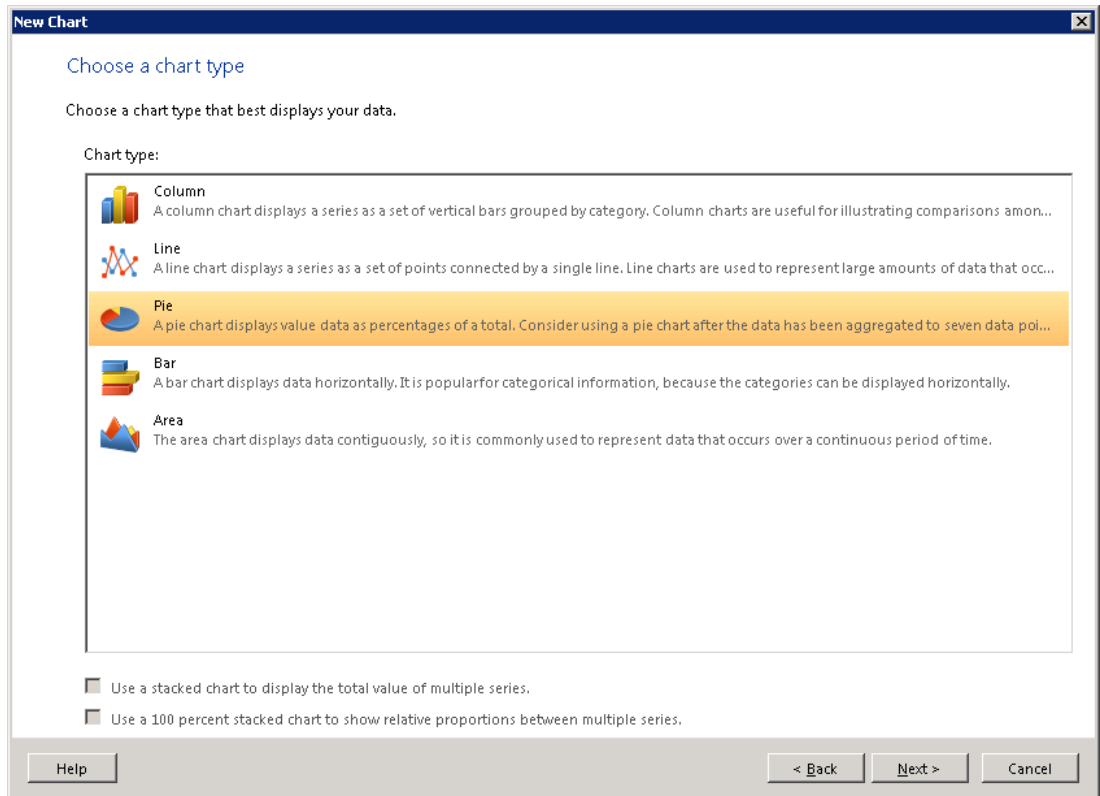
20. Click on Insert in the report builder menu and select Chart and Chart Wizard.
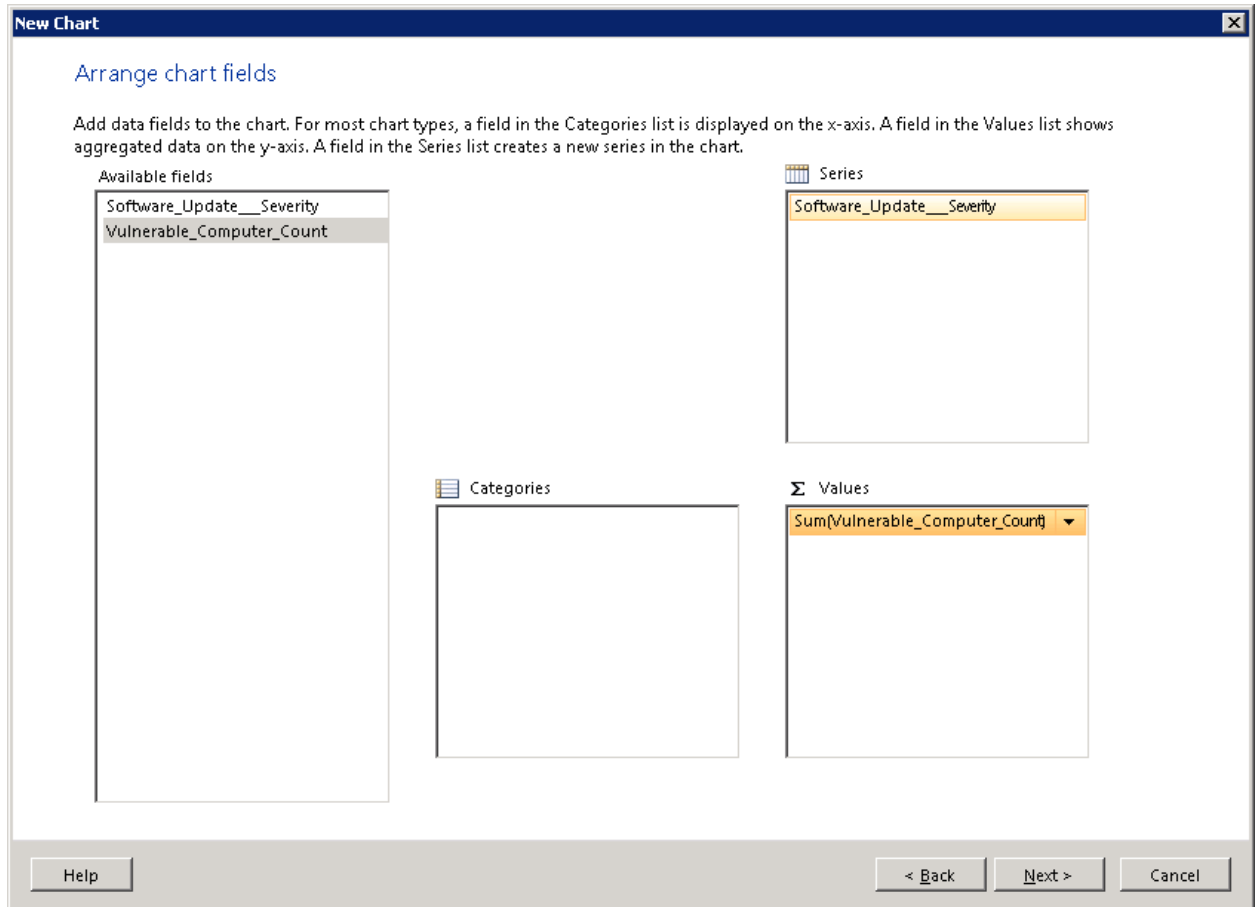

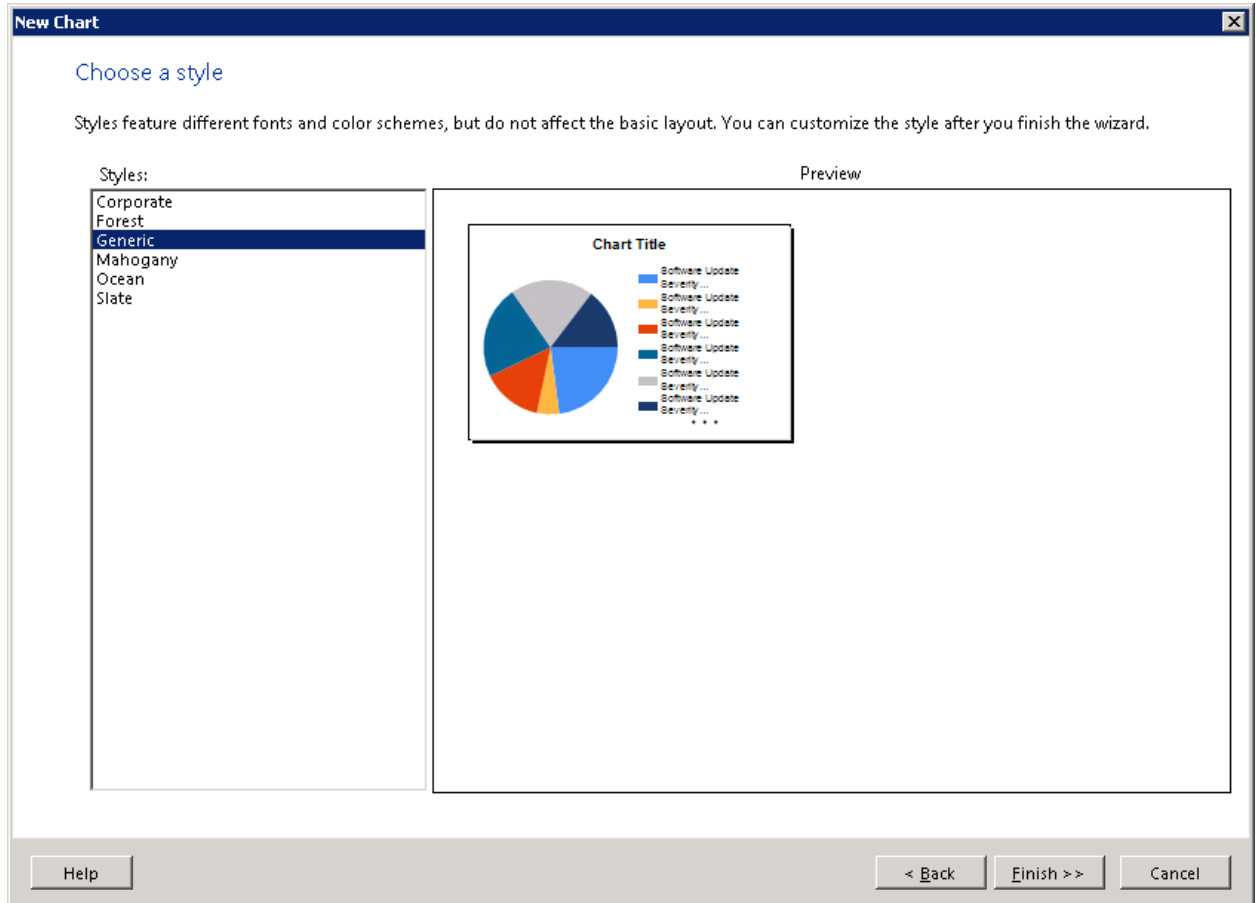21. In the New Chart window, select DataSet1 and click Next.

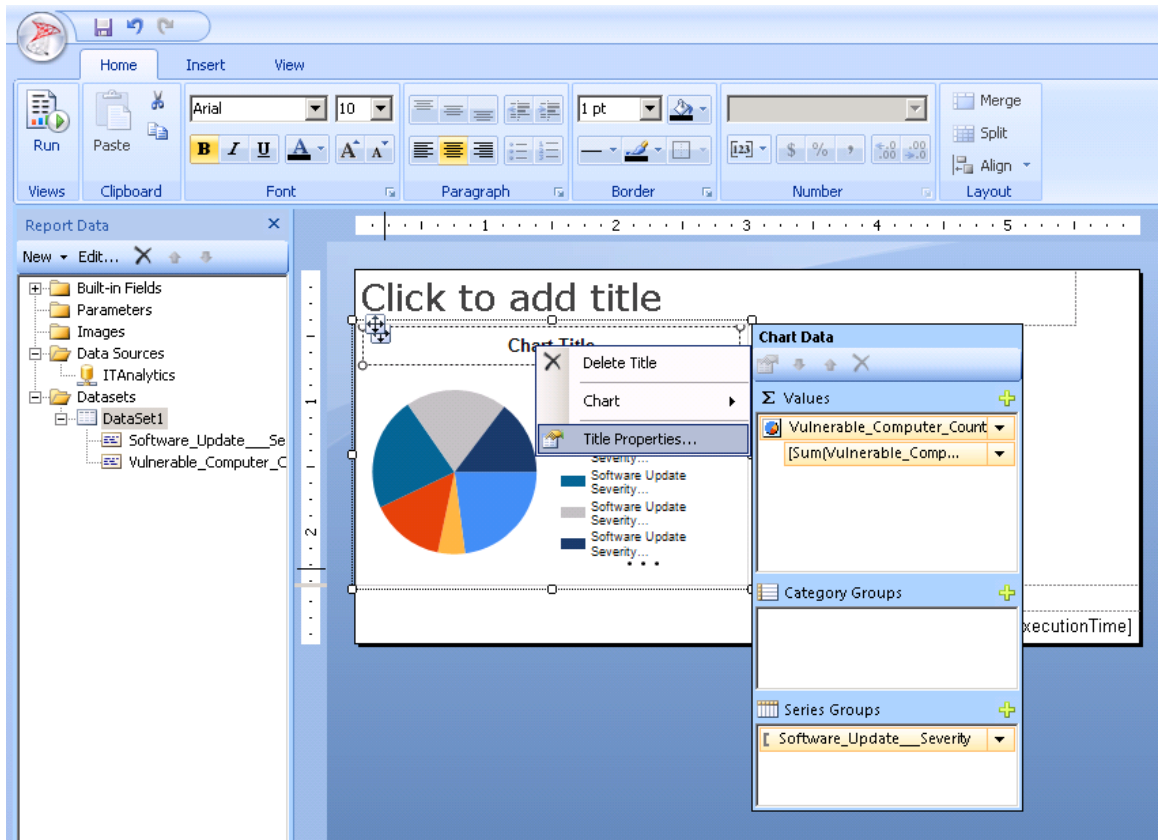22. Select Pie under Chart Type and click Next.

23. From Available fields, drag Software_Update___Severity to the Series pane and Vulnerable_Computer_Count to the Values pane and click Next.
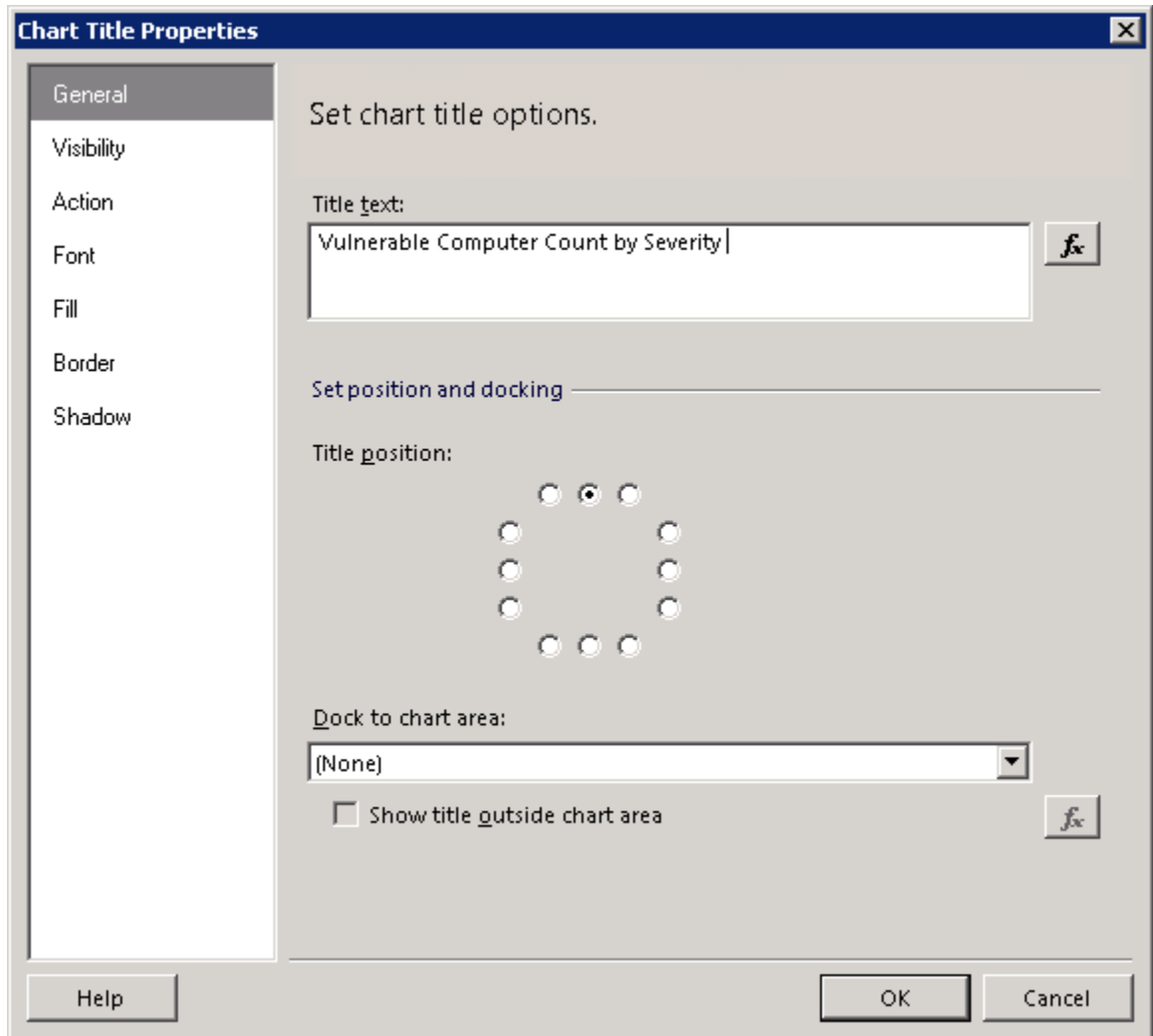
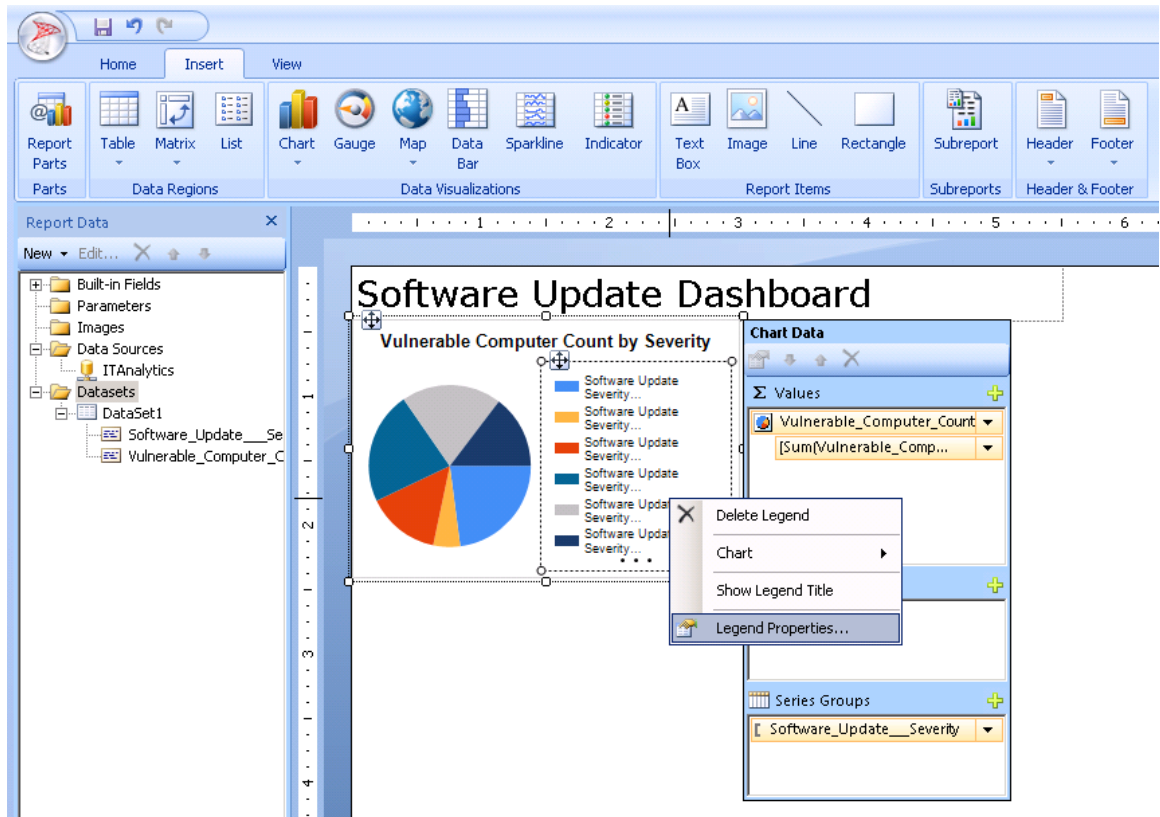24. Select Generic under the Styles pane and click Finish.

25. Right-click on Chart Title and select Title Properties.

26. Change Title text to Vulnerable Computer Count by Severity or something appropriate and click OK.

Chart Title Properties

General
Visibility
Action
Font
Fill
Border
Shadow

Set chart title options.

Title text:

Vulnerable Computer Count by Severity

fx

Set position and docking

Title position:

Dock to chart area:

(None)

☐ Show title outside chart area   *fx*

Help   OK   Cancel

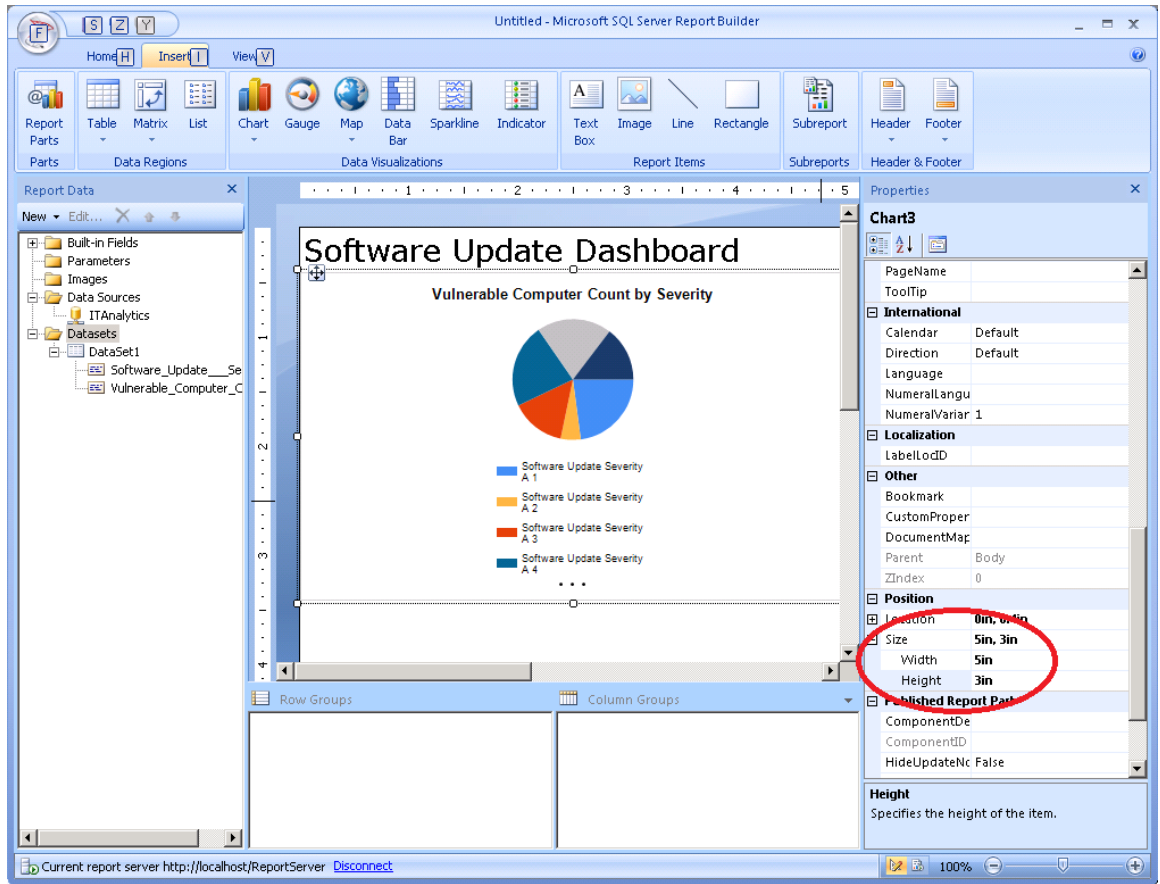27. Right-click on the legend area and select Legend Properties.

28. In the Legend Properties, set the following settings:

    a. Layout: Column
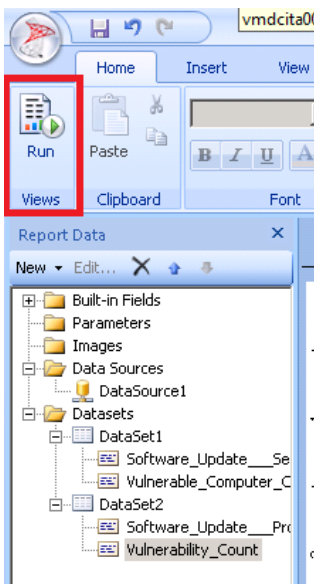
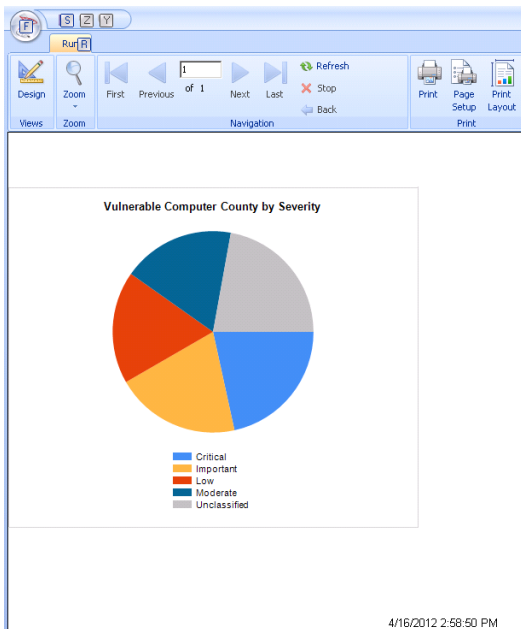   b. Legend position: Bottom, centered
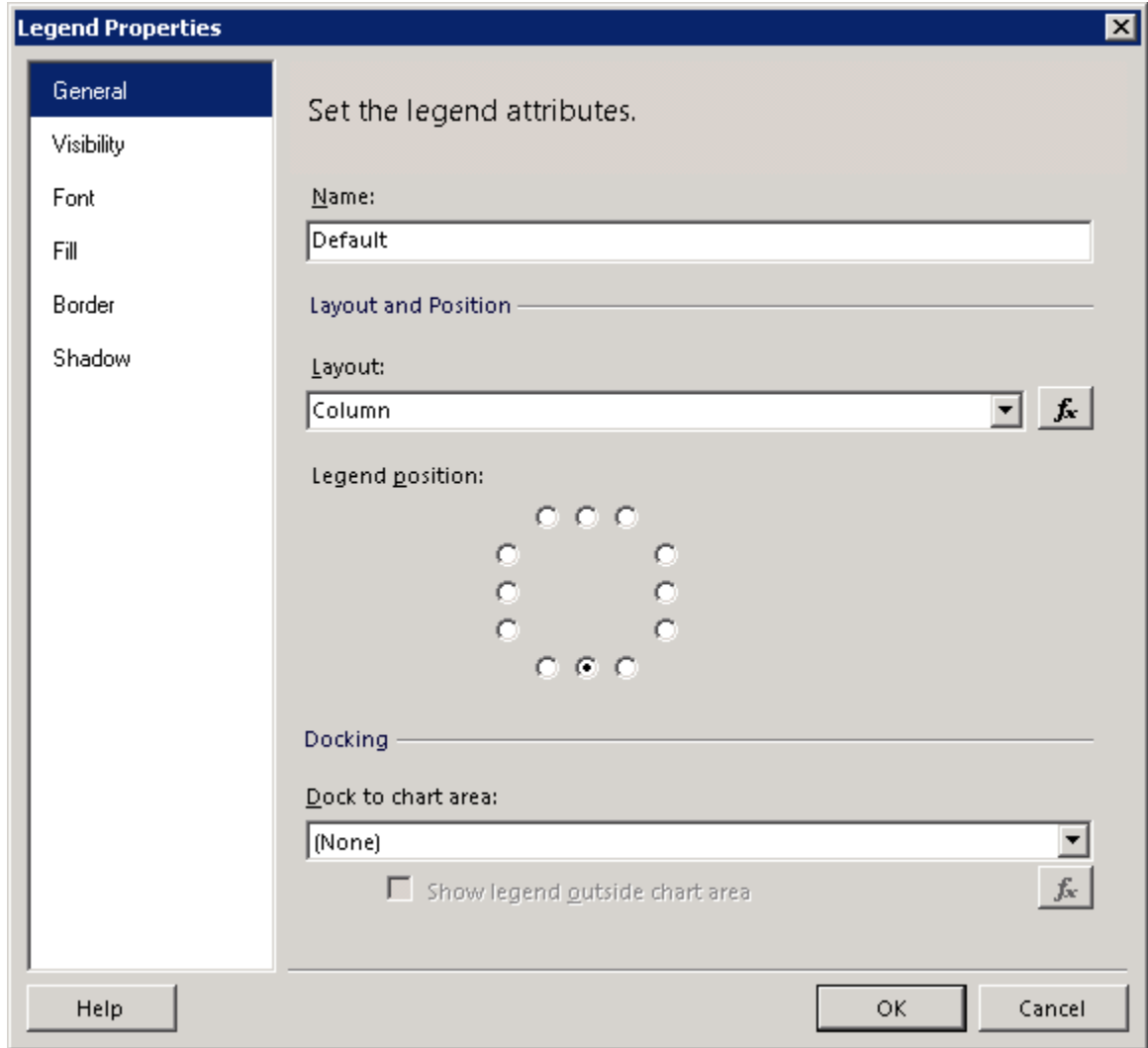
29. Click OK.

30. Select the chart and in the Properties pane, expand size and set Width to 5in and Height to 3in.
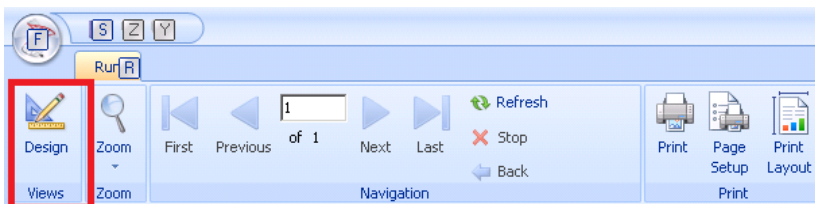

31. Preview the report by clicking the Run Report button in the toolbar and make any other adjustments.
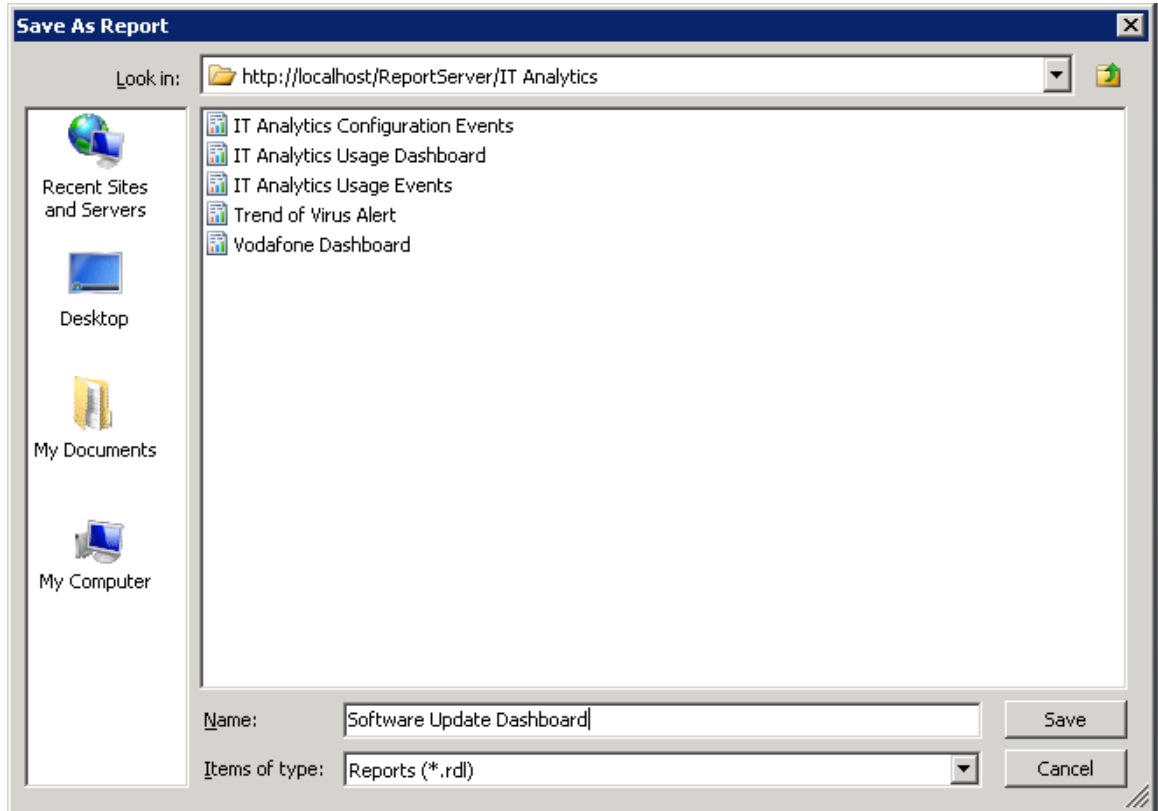
32. After selecting the Run Report button you will be presented with a preview of your report with realtime data.

33. Select the Design button on the toolbar to return to the Design view.

34. Click the 💾 icon in the Report Builder toolbar to save this report to Reporting Services IT Analytics folder and name it "Software Update Dashboard".
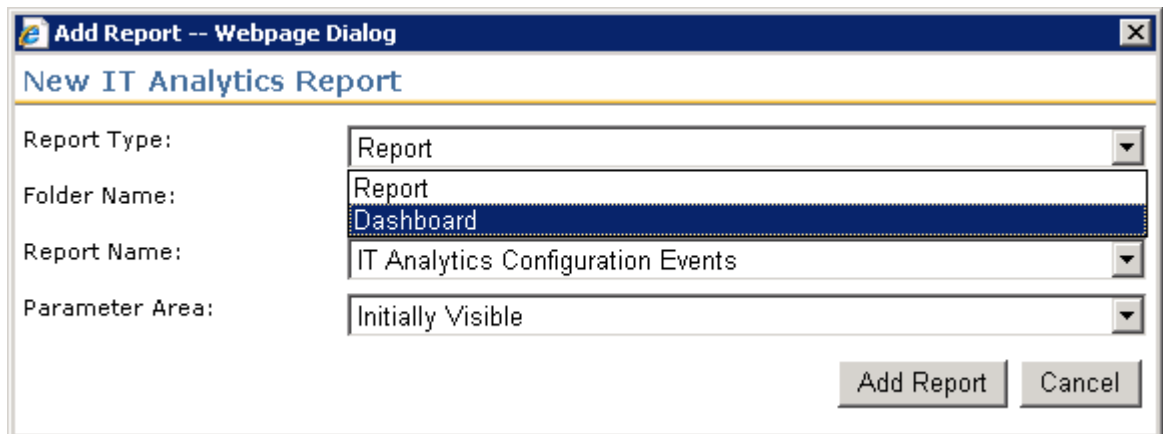

35. To link this report into the Altiris Console Open the Altiris Console from the shortcut on your desktop then navigate to the Reports > IT Analytics > Dashboards folder.
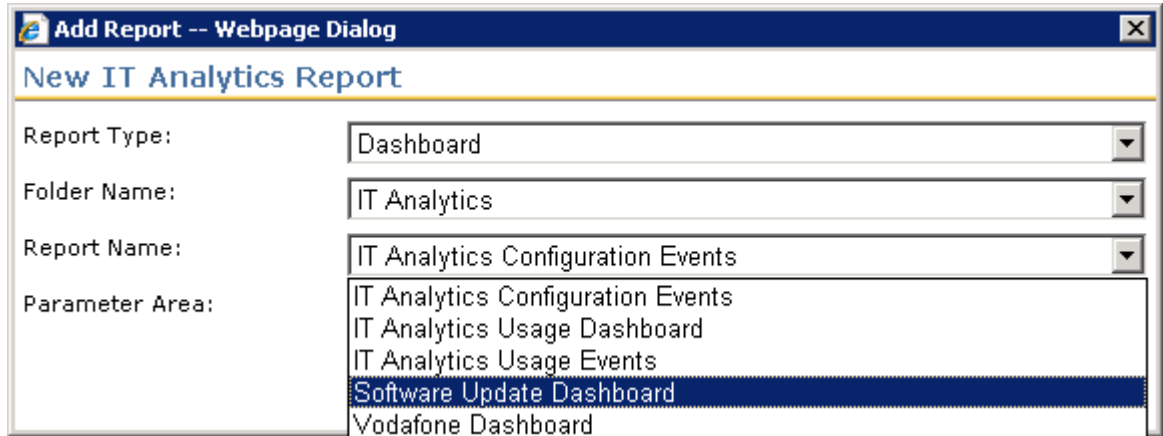
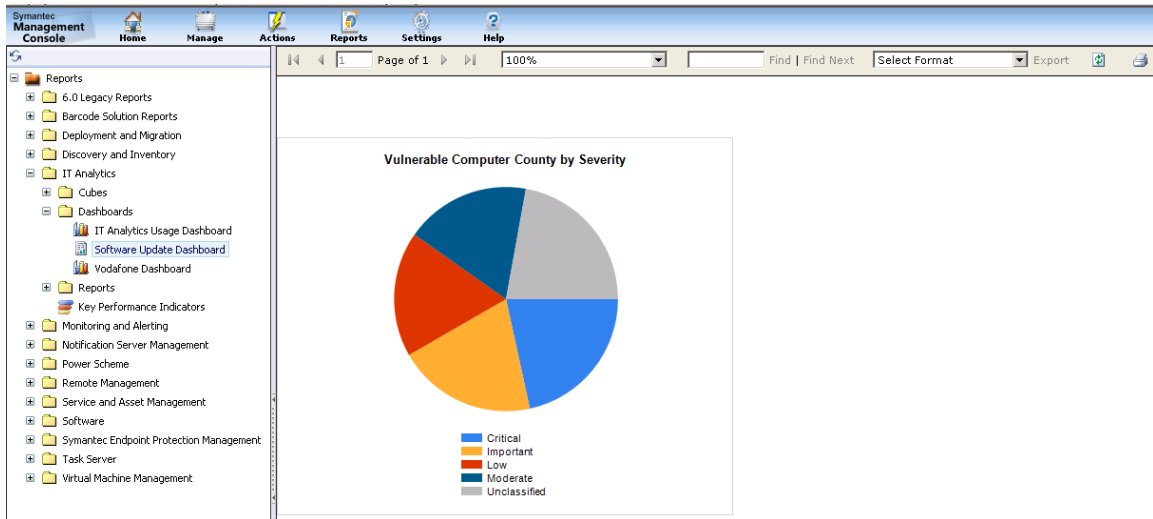36. Right-click on the Dashboards folder and select New>IT Analytics Report.
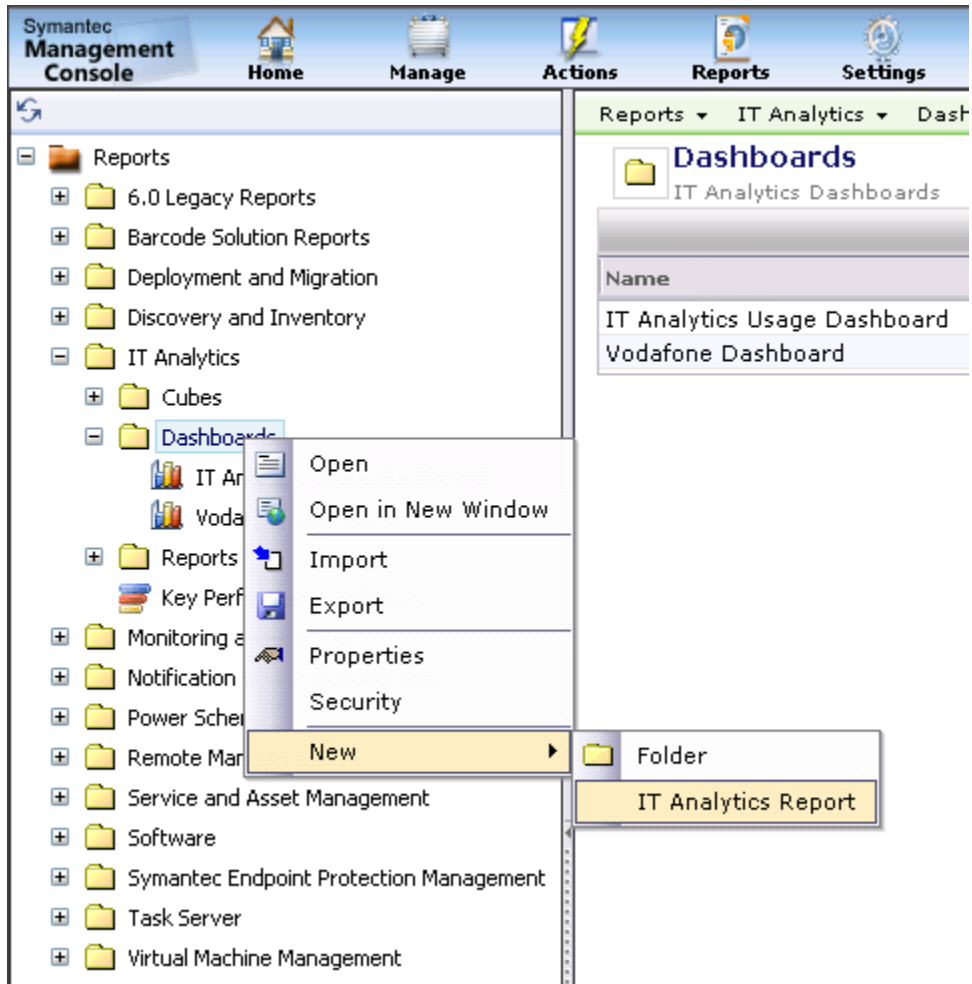
37. In the Report Type dropdown box, select Dashboard.

38. In the Report Name dropdown box locate and select the report you just saved and click the Add Report button.

39. Refresh your browser and expand the Dashboards folder.

40. Locate and select the report you just added.

Exercise 5: Optional

In this exercise we will add an additional report to the dashboard created in Exercise 5 .

1. Repeat steps 11 to 19 from exercise 4 to create another Dataset, but instead of using the measure, Vulnerable Computer Count in step 17 and the attribute Software Update – Severity in step 18, use Vulnerability Count for the measure and Software Update – Provider for the attribute.

2. Repeat steps 20 to 30 to create a second chart. Use Dataset2 for step 21 instead of Dataset1. For step 23, drag Software_Update__Provider to the Series pane and Vulnerability_Count to the Values pane. For step 26, name the chart Vulnerability Count by Provider.
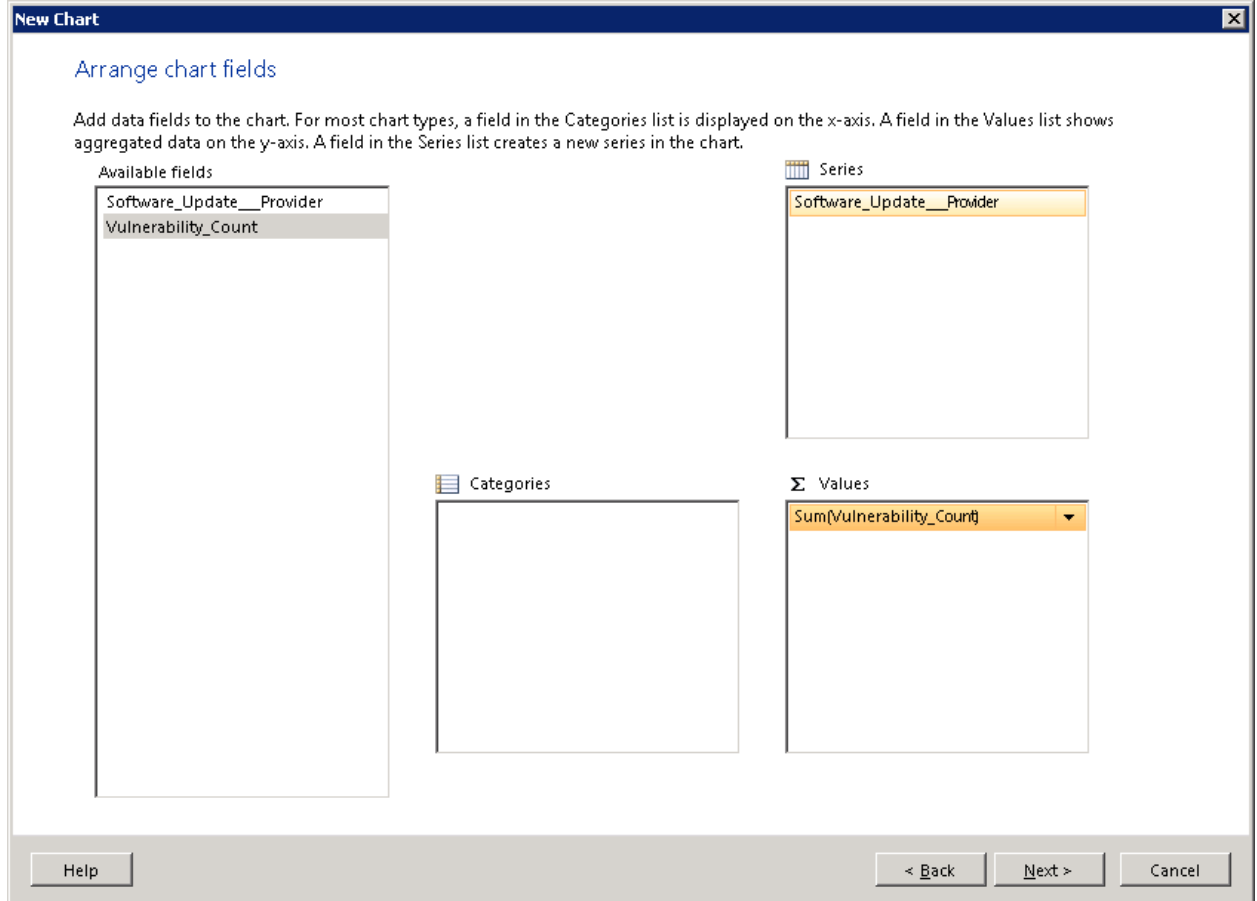
3. Move the newly inserted chart to the right of the Vulnerable Computer Count by Severity chart by dragging the chart using the ⊞ icon on the upper left corner of the chart.
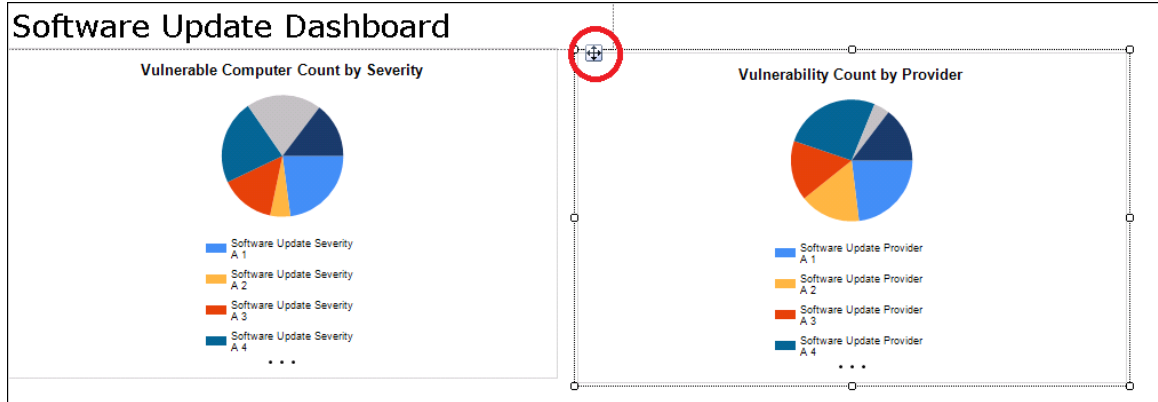
Click the 💾 icon in the Report Builder toolbar to save this report.

4. Open the Altiris Console from the shortcut on your desktop then navigate to the Reports > IT Analytics > Dashboards folder.

5. Locate and the report you just updated.