ServiceDesk Pack for Altiris™ IT Analytics 8.1 from Symantec™ User Guide

Symantec™

ServiceDesk Pack for Altiris™ IT Analytics 8.1 from Symantec™ User Guide

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

support.symantec.com

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing IT Analytics

This chapter includes the following topics:

About IT Analytics

IT Analytics complements and expands upon the reporting and analytics that is offered by Symantec ServiceDesk. The capabilities that are provided within the IT Analytics ServiceDesk Content Pack allow customers to extract maximum value from the data that is contained within their Symantec ServiceDesk database.

By implementing the IT Analytics ServiceDesk Content Pack, you attain the following benefits:

- Powerful on-the-fly forensic analysis through ad-hoc reports and charts, with pivot table.
- Out-of-the-box visually informative KPI scorecards, dashboards, and reports.
- Replace time-consuming & complex custom reporting.

See "How IT Analytics works" on page 12.

See "About IT Analytics ServiceDesk Content Pack" on page 14.

How IT Analytics works

IT Analytics is very easy to deploy and use. It is easily installed from the web as a content pack into the Symantec Management Platform (SMP), which is also downloadable from the Symantec public site on the web and is free for this purpose.

The IT Analytics platform is an ecosystem comprised of multiple architectural components that work together to provide robust reporting and analytics. These components are structured across two central foundational layers which encompass the core of the IT Analytics product:

Table 1-1 Foundational layers of IT Analytics

Layers	Description
IT Analytics Server	The IT Analytics Server is built on a portable, redistributable, extendable and commercially supported infrastructure. The server is the underlying technology that serves as a foundation for the data sources. The server also provides for installation, configuration, security, and maintenance of the content in a consistent manner across diverse customer environments.
IT Analytics content packs	IT Analytics content packs represent the enterprise-ready analytics and reporting solutions that provide product-specific content. The content packs include the actual definition of the cubes, plus the out-of-the-box KPIs, reports, and dashboards.

The architecture diagram details how the different components of IT Analytics are arranged and interact with one another. Brief descriptions of these components are also provided in Table 1-2

Table 1-2 Components of IT Analytics Pack

Component	Description
Symantec Management Platform	The primary component that interacts and accesses the functionality that IT Analytics provides.
Symantec Management Platform CMDB	The primary database that includes all IT Analytics configurations.
Microsoft SQL Server Analysis Services	Used as the primary data layer for the dashboards, pivot tables, and reports.
Microsoft SQL Server Reporting Services	Used as the presentation layer for the reports and dashboards.
Microsoft Office Web Components 11	Used as one of the presentation layers to provide raw access to browse the cubes through pivot tables.
OLAP Cubes	The primary component that contains all data attributes and measures for reporting purposes.

Table 1-2 Components of IT Analytics Pack *(continued)*

Component	Description
Symantec databases	The primary database(s) that contain all information specific to the various Symantec products.

See "About IT Analytics ServiceDesk Content Pack" on page 14.

About IT Analytics ServiceDesk Content Pack

The IT Analytics ServiceDesk Content Pack provides the underlying definitions for the cubes, reports, dashboards, and KPIs to be used within IT Analytics. This content pack integrates with the ServiceDesk database through the connections that are once established, populates the predefined IT Analytics cubes with the relevant ServiceDesk product data. The IT Analytics Server then processes these cubes on a given schedule, allowing the data to come together into the meaningful views which the end users can easily interact with, analyze, and share across the organization.

In addition to the content pack in this User Guide, Symantec also offers the IT Analytics Client and Server Management Content Pack

See "About IT Analytics" on page 12.

See "Installing and configuring IT Analytics Server" on page 16.

Chapter 2

Getting Started

This chapter includes the following topics:

Installing and configuring IT Analytics Server

You can install IT Analytics Server from the Symantec Installation Manager. From the Symantec Management Console, you can configure and set up your version of IT Analytics Server.

Table 2-1 Process for installing and configuring IT Analytics Server and content packs

Step	Action	Description
Step 1	Verify that your computer meets the hardware and the software prerequisites.	You must ensure that your computer meets the hardware prerequisites and install specific software before you install IT Analytics Server. See "Hardware prerequisites" on page 17. See "System requirements and supported platforms" on page 17.
Step 2	Install IT Analytics Server and content packs.	You can use the Symantec Installation Manager to install IT Analytics Server and content packs. See "Installing IT Analytics Server and content packs" on page 20.
Step 3	Configure the content pack connections.	You can add and configure the connections that IT Analytics content pack uses.
Step 4	Add the cubes.	You can choose the cubes that you want to include in your environment. See "Adding cubes" on page 26.
Step 5	Add the reports.	You can choose the reports that you want to include in your environment. See "Adding reports" on page 27.
Step 6	Schedule the cube processing tasks.	You can choose how often each installed cube is processed. Usually, each cube is processed daily. See "Configuring the cube processing tasks" on page 27.

Table 2-1 Process for installing and configuring IT Analytics Server and content packs *(continued)*

Step	Action	Description
Step 7	Verify your installation.	You can check to see that your installation was successful and that your version of IT Analytics Server contains all the necessary items. See "Verifying your installation" on page 28.

For an example of configuring IT Analytics, please see the following videos:

http://www.youtube.com/watch?v=AwCWJu33cs8

http://www.youtube.com/watch?v=3SOdeMUOVKU

Hardware prerequisites

The computer on which you want to install IT Analytics Server must meet the specific hardware requirements that are outlined in the *IT Management Suite Planning for Implementation Guide*.

In addition to the hardware required for the Symantec Management Platform, the following hardware is recommended:

- 2.0 GHz CPU 4 cores minimum (8 cores preferred)
- 4 GB RAM (6+ GB preferred)
- 40 GB of free disk space

See "Installing and configuring IT Analytics Server" on page 16.

System requirements and supported platforms

Before you install the content pack and IT Analytics Server, the following software must be installed and configured:

- The content pack and IT Analytic Server are installed on this computer.
- ADOMD.NET 9.0
  Install this software on the Notification Server computer.
  Install the `SQLServer2005_ADOMD_x64.msi` file with the default configuration.
  For the downloadable file, see the Microsoft MSDN Web site at the following URL:

https://www.microsoft.com/en-us/download/details.aspx?id=17943.

- Microsoft Report Viewer
  Install this software on all computers that access the Symantec Management Console.
  Supported versions: 2008 SP1, 2008 R2, 2012 and 2014.
  Report Viewer is installed with the default configuration.
  For the downloadable file, see the Microsoft MSDN Web site at the following URL:
  http://www.microsoft.com/download/en/details.aspx?id=3841.

- Open XML SDK 2.0 for Microsoft Office
  This component is required to export cube views to xlsx format. For more information about exporting the cube views, please see the following article:
  TECH232459

The operating systems that are supported by the Symantec Management Platform are also supported by the content pack and IT Analytics Server.

The following components do not need to be installed on the Symantec Management Platform, but do need to be installed and available on an appropriate system:

- Microsoft SQL Server Analysis Services
  This software is required for the cube database.
  Supported versions: 2008 SP1, 2008 R2, 2012, and 2014.
  Symantec recommends that you install SQL Server Analysis Services and SQL Server Reporting Services on the same server.

- Microsoft SQL Server Reporting Services
  This software is required for the reports.
  Supported versions: 2008 R2, 2012, and 2014.
  Symantec recommends that you disable Internet Explorer Enhanced Security on the computer that hosts Microsoft SQL Server Reporting Services.
  Symantec recommends that you install SQL Server Reporting Services and SQL Server Analysis Services on the same server.

Note: Microsoft SQL Server includes a separate utility named Report Builder, which integrates with IT Analytics ServiceDesk Content Pack and can provide additional flexibility in custom reporting. While SQL Server 2005 meets the minimum prerequisite for installation of IT Analytics ServiceDesk Content Pack, it only includes Report Builder 1.0. If possible, Symantec recommends that you use SQL Server 2008 SP1, 2008 R2 or 2012 to take advantage of the new features that are included in Report Builder 2.0/3.0 for a more robust custom report authoring experience. An example of the capabilities that Report Builder provides can be found later in this document.

The following components may need to be installed on all endpoints that access the console:

- Microsoft Office Web Components 11 (2003)
  Install this software on all computers that access the Symantec Management Console.
  The `owc11.exe` file is installed with the default configuration.
  For the downloadable file, see the Microsoft MSDN Web site at the following URL:
  http://www.microsoft.com/en-us/download/details.aspx?id=22276.
  See "Cube prerequisites (OWC behavior only)" on page 43.

See "Installing and configuring IT Analytics Server" on page 16.

Ports used by IT Analytics Server

By default, the IT Analytics Server uses specific ports.

These ports must be opened on the firewall if there is a firewall between the Symantec Management Platform and the SQL Server or between these servers and the user's workstation. Each of these ports can be remapped. Discuss this issue with your database administrator and server administrator to determine which port each service currently uses.

Table 2-2 Ports used by IT Analytics Server

Port	Access	Description
1433	SQL Server	Used when processing cubes.
2383	Analysis Server	Used when processing cubes and to access data within reports and cubes. Also used by workstations when accessing cubes.
80	Reporting Services	Used to access reports on the report server.
443	Reporting Services	Used to access reports when using SSL to access the report server.
83	Reporting Services	Used to access reports via Kerberos authentication.

See "Configuring the content pack and IT Analytics Server" on page 20.

See "Installing and configuring IT Analytics Server" on page 16.

Installing IT Analytics Server and content packs

You can install IT Analytics Server and content packs from the Symantec Installation Manager (SIM). You can download the installation files directly to your server or you can create offline installation packages.

Within SIM, available products are referred to as suites or individual solutions. For IT Analytics, the solution name for installation within SIM (Altiris IT Analytics) includes the required IT Analytics Server itself as the underlying foundation. Additionally, each IT Analytics content pack displays its own individual product for install, to be used with IT Analytics Server.

To install IT Analytics Server and content packs

1. Launch the Symantec Installation Manager.
2. On the **Installed Products** page, click **Install new products**.
3. On the **Install New Products** page, in the **Filter** drop-down list click **Solutions**.
4. In the **Available products** area, locate and check **IT Analytics 8.1** and the content packs that you want to install.

   IT Analytics supports the following packs:

   - **IT Analytics Client Server Management Pack**
   - **IT Analytics ServiceDesk Pack**
5. Click **Next**.
6. Follow the rest of the installation instructions.
7. Configure IT Analytics Server.

   After you install IT Analytics and the content packs, you must configure IT Analytics Server. See the following topic for the configuration steps:

   See "Configuring the content pack and IT Analytics Server" on page 20.

See "Installing and configuring IT Analytics Server" on page 16.

Configuring the content pack and IT Analytics Server

After you install the content pack, you must configure the IT Analytics Server to meet the needs of your environment. Before you can successfully configure it, specific software prerequisites and considerations must be met.

See "System requirements and supported platforms" on page 17.

See "Ports used by IT Analytics Server" on page 19.

To configure the content pack and IT Analytics Server

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand **IT Analytics Settings**, and then click **Configuration**.
3. In the right pane, under **Analysis Server**, in the **Analysis Server Name** box, type the host name of the Microsoft SQL Server Analysis Services.

   If you did not install SQL Server as the default instance, use the following format for the host name: `servername\instancename`.

   Symantec recommends that you type the host name of the server on which Analysis Services reside. If you use `localhost` as a host name, you restrict the access from the Symantec Management Console to the computer where Analysis Services resides.

   Note that this connection uses the Symantec Management Platform application ID credentials.
4. Click **Verify Connection**, and confirm that the Analysis Server name has been verified and saved.
5. Next to **Analysis Server Database**, create, or select an Analysis Server Database as follows:

For a new standard configuration, create a new Analysis Server database.	■ Click **Create new database**. ■ In the **Create new database** box, use the default IT Analytics name.
Select an existing Analysis Server database. **Warning:** If you select an existing database, the existing data sources are overwritten with the current Symantec Management Platform database settings.	■ Click **Use existing database**. ■ In the **Use existing database** drop-down list, click an Analysis Server database.

6. Click **Save Database Settings**.

7 Under **Reporting Server**, in the **Reporting Server Virtual Directory URL** box, type the full URL of the Reporting Services ReportServer virtual directory.

If you did not install SQL Server as the default instance, use the following format for the virtual directory:

`http://servername/ReportServer_InstanceName/` for SQL Server 2008.

Symantec recommends that you type the host name of the server on which Reporting Services reside. If you use `localhost` as a host name, you restrict the access from the Symantec Management Console to the computer where Reporting Services reside.

8 Click **Verify Connection** and confirm that the Reporting Server name has been verified and saved.

9 Next to **Report Folder Name**, create, or select a report folder as follows:

For a new standard configuration, create a new IT Analytics report folder.	■ Click **Create new report folder**. ■ In the **Create new report folder** box, use the default IT Analytics report folder name.
Select an existing folder to use for your IT Analytics report folder. **Warning:** If you select an existing folder, the existing data sources are overwritten with the current Analysis Server Database settings.	■ Click **Use existing report folder**. ■ In the **Use existing report folder** drop-down list, click a folder.

10 Click **Save Folder Settings**.

11 Next to **Authentication Type**, click the **Edit** symbol (pencil), and then select one of the following options for accessing Reporting Services:

- **Stored Credentials**
  Explicitly defines the user credentials. It also automatically manages authentication across all application tiers because access to Reporting Services is always authenticated with the same rights for all users. However, **Stored Credentials** limits the granular control that you have over the information within the reports to which users have access.
- **Windows Integrated Authentication**
  Lets the user's Windows credentials pass through to the Reporting Server. This method is recommended for restricting access to Reporting Services on a per-user basis. **Windows Integrated Authentication** allows a more granular control over the information in the reports to which you grant users

access. However, additional configuration might be necessary to ensure that authentication is appropriately managed across all application tiers.

See "About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes" on page 77.

12 (Optional) If you selected **Stored Credentials**, type the user name and password.

13 Click **Save Security Settings** and confirm that the Report Folder name is verified and saved.

14 (Optional) To adjust the **Default Open Cube Behavior**, click the **Edit** symbol, select **Open with Cube Browser** (to view the cubes in the IT Analytics browser) or **Open with OWC** (to view the cubes with Microsoft Office Web Components), and then click**Save**.

To use the **Open with OWC** you may have to install the Microsoft Office Web Components.

15 To adjust the **Number of members to display**, click the **Edit** symbol and specify a numeric value, and then click **Save**.

This setting limits the number of rows that are displayed when browsing a cube using the IT Analytics Cube Browser (the default number is 40).

16 (Optional) To adjust the **Number of rows per export to Excel**, click the **Edit** symbol and specify a numeric value, and then click **Save**.

This setting limits the number of rows that are displayed once the cube view has been exported to Excel (the default number is 1048576).

17 After you configure the content pack and IT Analytics Server, you need to install cubes and reports.

See "Adding cubes" on page 26.

See "Adding reports" on page 27.

See "About SQL Server Analysis Services" on page 66.

See "About SQL Server Reporting Services" on page 72.

See "Purging resource event data" on page 29.

See "Installing and configuring IT Analytics Server" on page 16.

Configuring the ServiceDesk connection

You need to complete these steps only if the IT Analytics ServiceDesk Content Pack is installed.

Configure a connection before you install the IT Analytics ServiceDesk cubes.

See "Installing and configuring IT Analytics Server" on page 16.

To configure the ServiceDesk connection

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folders.
3. Click **Symantec ServiceDesk**.
4. In the right pane, enter the information for each of the connection fields.

   See "ServiceDesk connection fields" on page 24.
5. Click **Save**.
6. (Optional) Edit and delete the ServiceDesk connection.

   See "Editing the ServiceDesk connection" on page 25.

   See "Deleting the ServiceDesk connection" on page 25.

ServiceDesk connection fields

You can edit and modify the ServiceDesk connection by entering information for the corresponding fields:

Table 2-3 Fields for ServiceDesk connections

Field	Description
ServiceDesk Database Server Name	The name of the server that hosts the ServiceDesk database.
ServiceDesk Database Name	The name of the ServiceDesk database.
ServiceDesk Database Username	The user name for the ServiceDesk database. **Note:** Windows credentials are not supported. You must enter SQL account credentials.
ServiceDesk Database Password	The password for the ServiceDesk database.
ServiceDesk Password Confirmation	The confirming password for the ServiceDesk database.
Process Manager Base URL	The base URL to the Process Manager that is used to open the incident from the Incident Search report.

See "Editing the ServiceDesk connection" on page 25.

See "Deleting the ServiceDesk connection" on page 25.

See "Configuring the ServiceDesk connection" on page 23.

See "Installing and configuring IT Analytics Server" on page 16.

Editing the ServiceDesk connection

IT Analytics Server lets you edit the ServiceDesk connection so that the data can be leveraged for reporting purposes.

To edit the ServiceDesk connection

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folders.
3. Click **Symantec ServiceDesk**.
4. Change the information for any of the following fields:
   - ServiceDesk Database Username
   - ServiceDesk Database Password
   - ServiceDesk Password Confirmation
     See "ServiceDesk connection fields" on page 24.
   - Report Integration URL, which lets you specify an alternate base URL to access the Process Viewer page for this ServiceDesk instance. The IT Analytics reports use this URL to launch a specific incident to display further details.
5. Click **Save**.

See "Deleting the ServiceDesk connection" on page 25.

See "Configuring the ServiceDesk connection" on page 23.

See "Installing and configuring IT Analytics Server" on page 16.

Deleting the ServiceDesk connection

IT Analytics Server lets you delete the ServiceDesk connection to remove its data from the reports.

To delete the ServiceDesk connection

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folders.
3. Click **Symantec ServiceDesk**.
4. In the right pane, select the server that you want to delete.
5. Click **Delete**.

See "Editing the ServiceDesk connection" on page 25.

See "Configuring the ServiceDesk connection" on page 23.

See "Installing and configuring IT Analytics Server" on page 16.

Adding cubes

To view IT Analytics cubes in the Symantec Management Console, you must add the cubes from the content pack.

See "About cubes" on page 32.

To add cubes

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, click **Cubes**.
3. In the right pane, on the **Cubes** page, on the **Available** tab, select the cubes that you want to install.

   To install all of the available cubes, in the header row of the table, check **Install Cube Name**.
4. Click **Save Changes**.
5. In the **Message from webpage** dialog box, click **OK** to proceed with the installation.
6. The **IT Analytics Event Viewer** displays the installation progress of each cube that you selected. Click **Close** when the process is complete.
7. To verify that the cubes were successfully installed, on the **Installed** tab, review the list of cubes.

   Next, you need to process the cubes.

   This task is essential for the content pack to function properly because the cubes do not contain any data until the cube processing is complete.

See "Configuring the cube processing tasks" on page 27.

See "Installing and configuring IT Analytics Server" on page 16.

Adding reports

You can add reports to your environment that match your needs.

To add reports

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, click **Reports**.
3. In the right pane, on the **Reports** page, on the **Available** tab, select the reports that you want to install.

   To install all of the available reports, in the header row of the table, check **Install Report Name**.
4. Click **Save Changes**.
5. In the **Message from webpage** dialog box, click **OK** to proceed with the installation.
6. The **IT Analytics Event Viewer** displays the installation progress of each report that you selected. Click **Close** when the process is complete.
7. To verify that the reports were successfully installed, on the **Installed** tab, review the list of reports.

See "Installing and configuring IT Analytics Server" on page 16.

See "Creating a new report" on page 50.

Configuring the cube processing tasks

This task is essential for the content pack to function properly because the cubes do not contain any data until the cube processing is complete.

You can create and assign processing schedules for all installed cubes. Your business needs should dictate how often the cubes are processed. For a typical configuration, all cubes should be processed daily.

Multiple processing tasks can be used for more granular control of cube processing. More than one cube can share a dimension. In this case, the last processed date of all cubes that uses that dimension updates to the last processed date of the shared dimensions. However, the actual data in the cubes is not processed until a processing task is run that is configured to process that specific cube.

To configure the cube processing tasks

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand **IT Analytics Settings**, and then click **Processing**.
3. Set up your schedule for the default processing tasks, and then check **Enabled**.

   Symantec recommends that you process cubes no more than once a day, depending on the number of cubes and amount of data in your environment.
4. Select the cubes that you want to be processed on the current schedule.

   For a typical configuration, select all cubes.
5. Click **Save Changes** and confirm that the **Default Processing Task** is saved.
6. Click **Run Now**.

   The selected processing tasks start asynchronously, which means that the task does not finish by the time that the page refreshes. This task can take several minutes to execute. The execution time depends on the number of the cubes that are selected and the size of data within the database. To monitor its progress, you can view the events in the **IT Analytics Event Viewer** while the manual processing task executes.

See "Adding cubes" on page 26.

See "Installing and configuring IT Analytics Server" on page 16.

Verifying your installation

You can verify your installation and ensure that all of your configuration steps are completed successfully.

To verify your installation

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics**. The following items should appear:
   - **Cubes**
   - **Dashboards**
   - **Reports**
   - **Key Performance Indicators**

If the pop-up dialog boxes appear while your cubes load, you need to remove the warning messages.

See "Removing warning messages" on page 57.

See "Installing and configuring IT Analytics Server" on page 16.

Purging resource event data

Certain tasks that the content pack performs are logged to event tables. Configuration tasks, processing tasks, and report access information are logged to these event tables. As a result, these tables can grow over time. By default, the data is stored for six months or a mix table row count of 1000000.

To purge resource event data

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Purging Maintenance**.
2. In the left pane, click **Purging Maintenance**.
3. In the right pane, on the **Purging Maintenance** page, on the **Resource Event Data Purging Settings** tab, verify that **Resource event data purging** is **Enabled**.
4. Under **Custom**, click **Add**.
5. In the **Select DataClasses** dialog box, under **Available items**, in the **Group** drop-down list, expand **Data Classes > Inventory**, and then click **Notification Server Events**.
6. In the **Available items** list, select **IT Analytics Configuration** and **IT Analytics Usage**, and then click **>**.

   These selections now appear in the **Selected Items** list.
7. Click **OK**.
8. On the **Resource Event Data Purge Settings** tab, click **Save Changes**.

   IT Analytics Configuration and **IT Analytics Usage** now appear in the **Event Data Class** list.

See "Configuring the content pack and IT Analytics Server" on page 20.

Uninstalling the content pack

You can uninstall the content pack with the Symantec Installation Manager.

To uninstall the content pack

1. Launch Symantec Installation Manager.
2. On the **Installed Products** page, in the **Installed products** window, scroll down and click **IT Analytics 8.1**.
3. In the **Symantec Installation Manager** dialog box, select all the content packs that you want to uninstall and click **Next**.
4. In the **Symantec Installation Manager** dialog box, click **Begin uninstall** to confirm your uninstall selection.
5. (Optional) If a second **Symantec Installation Manager** dialog box opens, click **OK** to confirm your uninstall selection.

   If you opted to install the language packs, this dialog box message lets you know that the language packs are also uninstalled.
6. On the **Uninstallation Complete** page, click **Finish**.

Chapter 3

Implementing IT Analytics ServiceDesk Content Pack

This chapter includes the following topics:

Ways to access IT Analytics reports

You can access IT Analytics reports in several ways.

Table 3-1 Ways to access IT Analytics reports

Method	Description
Symantec Management Console - Cubes	Using cubes, you can construct and save views based on predefined measures and dimensions. The cubes are configured to allow exportable, dynamic, and customized reports. You can also load previously saved views for quick access to data that you frequently need. See "Viewing a cube" on page 33.
Symantec Management Console - Dashboards/Reports	These reports were developed to give you a representative view of your IT assets. You can export the reports to many different formats including HTML, Excel, and PDF. You can also create additional reports by using the SQL Reporting Services Report Builder, and then easily import your reports in the content pack. See "Viewing a Dashboard report" on page 49. See "Viewing a detailed report" on page 50.
Microsoft SQL Server Management Studio	With the built-in cube browser, you can view cube data natively through the SQL Server Management Studio. This option allows an administrator to have raw access to cube data and to have direct access to Analysis Services.
Third-party Reporting Products	You can use third-party reporting tools, such as ProClarity or Excel 2007, to report on the data that is contained in each cube. These tools provide rich cube browsing or cube reporting capabilities.

About cubes

A cube is an interactive view of an IT Analytics cube. Cubes let you view, organize, and summarize data into on-demand, personalized reports.

You can use it to dynamically analyze data from within the Symantec Management Console. If you have specified **Open with OWC in the Default Open Cube Behavior**, it uses Microsoft Office Web Components that are embedded within Microsoft Office products or that are freely available to download.

The **Default Open Cube Behavior** is opened with Cube Browser. To switch to the OWC view, right-click a cube and select **Open with OWC**. This opens the cube in

a new tab with the traditional OWC view. If any required components for this view are missing, you are prompted to install them.

If the **Default Open Cube Behavior** is opened with OWC, you may switch to the **Cube Browser** view. To switch, right-click a cube and select **Open with Cube Browser**. The cube opens in a new tab.

See "Cube prerequisites (OWC behavior only)" on page 43.

See "Creating a table using the ServiceDesk Incidents cube example" on page 59.

About Key Performance Indicators (KPIs)

One of the advantages of using OLAP is the ability to use an intuitive reporting framework. This framework lets you quickly translate large data volumes with the goal of making informed business decisions. Analysis Services leverages this capability through Key Performance Indicators (KPIs). KPIs are defined as quantifiable measures that represent a critical success factor in an organization. The emphasis is on the action of quantifying something in the environment. For example, the KPIs must be measurable to successfully be monitored and compared against a given objective.

For an overview on KPIs, please see the following video:

http://www.youtube.com/watch?v=3SOdeMUOVKU

See "Creating Key Performance Indicators (KPIs) - ServiceDesk" on page 60.

See "Setting the status of a KPI (advanced) - ServiceDesk" on page 61.

Viewing a cube

You can access the IT Analytics reports in many ways.

See "Ways to access IT Analytics reports" on page 31.

To view a cube

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics > Cubes**.
3. Select a cube to view.

See "Adding cubes" on page 26.

Cube Browser Behavior

These instructions pertain to using the Cube Browser to consume cube data.

See “Cube Browser Behavior - Cube fields” on page 34.

See “Cube Browser Behavior - Cube view toolbar functions” on page 35.

See “Saving a cube view” on page 38.

See “Loading a cube view” on page 38.

See “Modifying a cube view” on page 39.

See “Deleting a cube view” on page 40.

See “Exporting cube results” on page 40.

See “Creating Key Performance Indicators (KPIs)” on page 41.

See “Setting the status of a KPI (advanced)” on page 42.

Cube Browser Behavior - Cube fields

The following cube fields are available.

Table 3-2 Cube fields

Field	Description
Field List	Displays the available fields within the cube to be used for creating a cube view. Note that different cubes will contain different fields. Fields can be added within a specific section to the Cube View Configuration at the bottom of the Cube Browser. Each field is defined and identified by the following: ■ Measures Measures are the aggregate count, or how you quantify results in a view. Every view you create must contain at least one measure and they can only be used within the Measures section of the Cube View Configuration. ■ Dimensions Dimensions are a grouping of specific data types you are quantifying when you create a view. Expanding each dimension will reveal the attributes to be used when creating a view. ■ Attributes Each dimension may have one or more attributes to be leveraged for view creation. These can be used within the Rows, Columns, Filters or Details sections of the Cube View Configuration.

Table 3-2 Cube fields *(continued)*

Field	Description
Cube View Configuration - Measures	The aggregate count or summary results of the attributes that are defined in the filter, row, and column sections of the Cube View Configuration.
Cube View Configuration - Rows	The rows of the cube view displayed in the interactive matrix. As attributes are added, the attribute name appears and displays (+)(-) next to the field name. These symbols let you drill down into the values of each attribute. You can place additional attributes before or after the existing attributes to modify the structure.
Cube View Configuration - Columns	The columns of the cube view displayed in the interactive matrix. As attributes are added, the attribute name appears and displays (+)(-) next to the attribute name. These symbols let you drill down into the values of each attribute. You can place additional attributes before or after the existing attribute to modify the structure.
Cube View Configuration - Filters	The value on which to filter the given results. You can place attributes within this section and then select which value to filter the report results on. Note that filters can also be set on Rows, Columns or Details attributes.
Cube View Configuration – Details	For cube views with multiple dimensions, the details view lets you see data displayed in a more tabular fashion, without having to drill into multiple attributes to see specific values.

See "About cubes" on page 32.

Cube Browser Behavior - Cube view toolbar functions

The following toolbar functions are available in the top toolbar:

Table 3-3 Toolbar functions

Function	Description
Views > Open	Opens the **Cube View Manager** window. From this window you can load the previously saved cube view or chart views. You can also delete previously saved cube views or chart views. You must select the appropriate view from the list of available views before performing an open/delete action.

Table 3-3 Toolbar functions *(continued)*

Function	Description
Views > Save	Saves the configuration of a cube view or chart view to allow for quick and easy access to the same information format in the future.
Filter > Manage Rows to Display	Gives the user the ability to specify the number of rows to be displayed in the cube view. To use this filter, click on a row then select this option from the toolbar and input a value for the number of rows to display. Alternatively, right-click a row, and then click **Display First X Rows** where X is the desired row count.
Filter > Manage Columns to Display	Gives the user the ability to specify the number of columns to be displayed in the cube view. To use this filter, click on a column then select this option from the toolbar and input a value for the number of columns to display. Alternatively, right-click a row, and then click **Display First X Columns** where X is the desired column count.
Filter > Manage Filters	Displays a **Filter Member** dialog box which allows a user to include or exclude specific values for the selected dimension. To use this option, select one dimension and then click **Manage Filters** on the toolbar, or right-click and select **Manage Filters**.
Filter > Add Filter to Include Only Selection	Includes specific data from the cube view, based on what member is selected. To filter only by a specific row or column, click the appropriate row/column header and select to include only from the **Filter** menu, or right-click and include only.
Filter > Add Filter to Exclude Selection	Excludes specific data from the cube view, based on what member is selected. To filter out a specific row or column, click the appropriate row/column header and select to exclude from the **Filter** menu, or right-click and exclude only.
Filter > Clear Filter for Selection	Clears any filters you have created that are specific to a selection.
Filter > Clear All Filters	Clears all filters from the current cube view.

Table 3-3 Toolbar functions *(continued)*

Function	Description
Sort > Sort Rows Ascending	Sorts the selected rows in ascending order. Click to clear the current sort order and to select a new sort order.
Sort > Sort Rows Descending	Sorts the selected rows in descending order. Click to clear the current sort order and to select a new sort order.
Sort > Sort Columns Ascending	Sorts the selected column in ascending order. Click to clear the current sort order and to select a new sort order.
Sort > Sort Columns Descending	Sorts the selected column in descending order. Click to clear the current sort order and to select a new sort order.
KPIs	Displays the additional options for defining a new Key Performance Indicator.
Details > View Details	Allows a user to view detail information in a tabular format (separate window) in addition to the cube view. Users can also export this information in a Microsoft Excel or CSV format. Specific dimensions to be used in the detail view must be added to the Detail section of the **Cube View Configuration** in the lower right.
Charts > Pie Chart	Creates a pie chart in a separate window for the selected data.
Charts > Bar Chart	Creates a bar chart in a separate window for the selected data.
Charts > Column Chart	Creates a column chart in a separate window for the selected data.
Charts > Area Chart	Creates an area chart in a separate window for the selected data.
Charts > Line Chart	Creates a line chart in a separate window for the selected data.

See “About cubes” on page 32.

Saving a cube view

You can save cube views, in both chart formats and table formats. To do this, you do not need to reconfigure the views that you most commonly access. These saved views can be private and available only to the user who created it. You can also choose to make a view publicly available for all users.

To save a cube view

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics > Cubes**, and then select a cube.
3. In the right pane, configure a table or chart.
4. In the toolbar at the top of the cube page, click **Views > Save**.
5. In the **Save View** dialog box, select one of the following options:

Create a new view.	Saves the current configuration as a new view with the name that you specify.
Overwrite an existing view.	Overwrites a previously saved view with the current configuration. Select a view from the drop-down list to overwrite.

6. (Optional) Check **This view is accessible by all Users (Public)** if this view should be publicly available.

   Otherwise, leave the box unchecked (default).
7. Click **OK**.

See "About cubes" on page 32.

Loading a cube view

You can load a cube view that you previously created.

To load a cube view

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics > Cubes**, and then select the cube that contains your saved view.

   For example, click the **Computers** cube.

3 In the toolbar at the top of the cube page, click **Views > Open**.

4 In the **Open Cube View** dialog box, select the saved view to load, and then click **Open**. The page refreshes and displays the view.

See "About cubes" on page 32.

Modifying a cube view

You can modify a view that you previously created.

To modify a cube view

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics > Cubes**, and then select the cube that contains your saved view.

For example, click the **Computers** cube.

3 In the toolbar at the top of the cube page, click **Views > Open**.

4 In the **Open Cube View** dialog box, select the saved view to load, and then click **Open**.

The page refreshes and displays the cube view.

5 Modify the configuration as necessary.

6 In the toolbar at the top of the page, click **Views > Save**.

7 In the **Save View** dialog box, select one of the following options:

Create new view.	Saves the current configuration as a new view with the name that you specify.
Overwrite an existing view.	Overwrites a previously saved view with the current configuration. Select a view from the drop-down list to overwrite.

8 (Optional) Check **This view is accessible by all Users (Public)** if this view should be publicly available.

Otherwise, leave the box unchecked (default).

9 Click **OK**.

See "About cubes" on page 32.

Deleting a cube view

You can delete a view that you previously created.

To delete a cube view

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics > Cubes**, and then select the cube that contains your saved view.

   For example, click the **Computers** cube.
3. In the toolbar at the top of the cube page, click **Views > Open**.
4. In the **Open Cube View** dialog box, select the saved view to delete, and then click **Delete**.

   The page refreshes and displays the view under the name of the cube.
5. In the **Confirm Delete** dialogue box, click **OK**.
6. Click **Close**.

See "About cubes" on page 32.

Exporting cube results

You can export data from cube lists to other programs, such as Microsoft Excel.

If you want to further analyze the data, you can export the list to a Microsoft Excel pivot table. You can also print a customized version of the data from a Microsoft Excel pivot table. This feature requires that you install Microsoft Excel on each computer that connects to the Symantec Management Console.

To export cube results

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics > Cubes**, and then select a cube and open an existing table view.

   If there is not an existing table view, drag and drop some measures and dimensions to create a table view. If there is no existing table view, drag and drop some measures and dimensions to create a table view.
3. In the toolbar at the top of the cube view, click **Details > View Details**.
4. Click **Export** and select the format to use for exporting.
5. Follow the on-screen instructions.

See "About cubes" on page 32.

Creating Key Performance Indicators (KPIs)

IT Analytics lets you create KPIs by manually defining them in the console navigation under the **Settings** folder. You can also directly create KPIs through the tables.

This procedure is an example of creating KPIs for computers with critical patch vulnerability defined through the cube. The example highlights how this procedure automatically populates some of the MDX code that is needed to define the KPI.

To create KPIs

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand the **IT Analytics > Cubes** folder.
3. Click **Patch Management Cube**.
4. Click and drag the **Software Update - Severity** field into the **Drop Row Fields Here** section.
5. Click and drag **Vulnerable Computer Count** into the **Drop Totals or Detail Fields Here** section.
6. Click and drag **Applicable Computer Count** into the **Drop Totals or Detail Fields Here** section.
7. Right-click the cell in the cube that represents **Vulnerable Computer Count** with **Critical Severity** and click **Create KPI from Selected Cell**.
8. In the **New KPI** dialogue box, use **Selected value** with a goal of zero then click **Next**.
9. Select **Gauge – Descending** and click **Next**.
10. Select **No Trend Indicator** and click **Next**.
11. In the **KPI Name** box, enter **Computers with Critical Vulnerability**, and then click **Next**.
12. Verify the information on the summary screen and click **Next**.
13. Click **Finish** to close the dialogue box.
14. On the **Reports > IT Analytics** menu, click **Key Performance Indicators**. The new KPI should now display in the list with the current value and goal already defined. The calculated measures that are associated with the KPI (Goal, Status, and Value) are also displayed in the pivot table field the next time you browse the cube, alongside the default measures.

See "About Key Performance Indicators (KPIs)" on page 33.

Setting the status of a KPI (advanced)

IT Analytics can leverage some of the graphical capabilities of Analysis Services and Reporting Services. It looks for visual status indicators, such as a stoplight or other images. This functionality gives a quick, high-level view of the current state of defined KPI.

The Status Expression of the KPI is defined as a number between 1 and -1. The most flexible way of defining how these values are populated is through an MDX string.

This procedure is an example of enhancing the KPI that was previously created.

To set the status of a KPI

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand the **IT Analytics** folder.
3. Click **Key Performance Indicators** to edit the KPI that was already created.
4. In the **Status Expression** box, click **MDX Expression**.
5. In the text area box that pops up, enter the following MDX code:

```
CASE
WHEN
aggregate({[Software Update].[Software Update - Severity].&[Critical]},
[Measures].[Vulnerable Computer Count])
< 0.1 * aggregate({[Software Update].[Software Update - Severity].&[Criti
[Measures].[Applicable Computer Count])
THEN   1
WHEN
aggregate({[Software Update].[Software Update - Severity].&[Critical]},
[Measures].[Vulnerable Computer Count])
> 0.25 * aggregate({[Software Update].[Software Update - Severity].&[Crit
[Measures].[Applicable Computer Count])
THEN   -1
ELSE   0
END
```

6. For **Status Graphic**, click **Traffic Light**.
7. Click **Save KPI**, and then click **Close**.
8. Refresh the list of KPIs. A stoplight should display under the **Status** column. It indicates the current status for this KPI.

See “About Key Performance Indicators (KPIs)” on page 33.

OWC Behavior

These instructions pertain to using the Cube Browser to consume cube data.

See “Cube prerequisites (OWC behavior only)” on page 43.

See “Cube Browser Behavior - Cube fields” on page 34.

See “OWC Behavior - Top cube toolbar functions” on page 44.

See “OWC Behavior - Cube toolbar functions” on page 45.

See “OWC Behavior - Charts toolbar functions” on page 46.

See “Saving a cube view” on page 46.

See “Loading a cube view” on page 47.

See “Modifying a cube view” on page 47.

See “Deleting a cube view” on page 48.

See “Exporting cube results” on page 49.

Cube prerequisites (OWC behavior only)

You must install the Microsoft Office Web Components to work with an interactive cube in your browser. If the freely available components are installed and you do not have Microsoft Office already installed, you can view the components with reduced functionality.

For instructions on how to download and install the Office Web Components, see the Microsoft Web site at the following URL:

http://www.microsoft.com/downloads/details.aspx?FamilyId=7287252C-402E-4F72-97A5-E0FD290D4B76&displaylang-en.

You must also install Microsoft SQL Server 2005 Analysis Services 9.0 OLE DB Provider for the Office Web Components. The DB Provider is a standard component that is bundled with Microsoft products such as Office 2007 and SQL Server 2005 Management Studio. It is also available from the Microsoft Web site.

For instructions on how to download and install the OLE DB Provider, see the Microsoft Web site at the following URL:

http://www.microsoft.com/downloads/details.aspx?familyid=df0ba5aa-b4bd-4705-aa0a-b477ba72a9cb&displaylang=en.

See “About cubes” on page 32.

OWC Behavior - Cube fields

The following cube fields are available.

Table 3-4 Cube fields

Field	Description
Drop Filter Fields Here	The value on which to filter the given results.
Drop Column Fields Here	The columns of the cube. As fields are added, the field name appears and displays (+)(-) next to the field name. These symbols let you drill down into the values of each field. You can place added fields before or after the existing fields to modify the structure.
Drop Row Fields Here	The rows of the cube. As fields are added, the field name appears and displays (+)(-) next to the field name. These symbols let you drill down into the values of each field. You can place added fields before or after the existing fields to modify the structure.
Drop Totals or Details Fields Here	The aggregate count or summary results of the fields that are defined in the filter, row, and column fields.

See "About cubes" on page 32.

OWC Behavior - Top cube toolbar functions

The following toolbar functions are available in the top toolbar.

Table 3-5 Top cube toolbar functions

Function	Description
Open	Loads the previously configured and saved cube views. You must select the appropriate view from the list of available views.
Save	Saves the configuration of a cube view to allow for quick and easy access to the same information format in the future.
New KPI	Displays the additional options for defining a new Key Performance Indicator.
Delete	Deletes the currently loaded cube view.

Table 3-5 Top cube toolbar functions *(continued)*

Function	Description
Display as Table	Displays the data and results as a table.
Display as Chart	Displays the data and results as a chart.

See "About cubes" on page 32.

OWC Behavior - Cube toolbar functions

The following toolbar functions are available in the cube toolbar:

Table 3-6 Cube toolbar functions

Function	Description
Copy	Copies the selected results. You must highlight the results that you want to copy.
Sort Ascending	Sorts the selected column in ascending order. Click it to clear the current sort order and to select a new sort order.
Sort Descending	Sorts the selected column in descending order. Click it to clear the current sort order and to select a new sort order.
Auto Filter	Enables or disables the auto filter function. IT Analytics retains your filter settings as you toggle on and off the Auto Filter. Fields that have an applied filter have a blue arrow at the selected field.
Show As	Changes the format with which the data results are represented. Options include the actual value or a percent of values.
Refresh	Refreshes the results of the table.
Export to Excel	Launches Microsoft Excel and exports the results into an Excel pivot table.
Commands & Options	Configures the advanced options for the table or chart, such as font type, font size, sorting, column headings, legends, and colors.

Table 3-6 Cube toolbar functions *(continued)*

Function	Description
Field List	Displays the available attributes within the cube. Each attribute can be added to the table to shape your results.

See "About cubes" on page 32.

OWC Behavior - Charts toolbar functions

The following toolbar functions are available only for charts.

Table 3-7 Charts toolbar functions

Function	Description
Chart Type	Displays the available chart types that can be displayed. For example, bar, area, line, and pie.
Show/Hide Legend	Toggles on and off the chart legend display.
By Row/Column	Switches the x axis of the chart to either row headings or column headings and allows the displayed data to be represented correctly.

See "About cubes" on page 32.

Saving a cube view

You can save views, in both chart formats and table formats. Using this functionality, you do not have to reconfigure the views that you most commonly access. In addition, these saved views can be private and available only to the user that created it. You can also choose to make a view publicly available to all console users.

To save a cube view

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics > Cubes**, and then select a cube.
3. In the right pane, configure a table or chart.
4. In the toolbar at the top of the cube page, click **Save**.
5. In the **Save Cube View** dialog box, select one of the following options:

Save the current configuration as a new view.	■ Click **Save as new view**. ■ In the **Save as new view** box, name the cube view.
Overwrite a previously saved cube view with the new configuration.	■ Click **Save as existing view**. ■ In the **Save as existing view** drop-down list, select the cube view that you want to overwrite.

6 (Optional) Check **Available to All Users** if this view should be publicly available. Otherwise, leave the box unchecked (default).

7 Click **Save**.

See "About cubes" on page 32.

Loading a cube view

You can load a cube view that you previously created.

To load a cube view

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics > Cubes**, and then select the cube that contains your saved view. For example, click the **Computers** cube.

3 In the toolbar at the top of the cube page, click **Open**.

4 In the **Open Cube View** dialog box, in the **Saved Cube Views** drop-down list, select the saved view to load, and then click **Open**. The page refreshes and displays the table view under the name of the cube.

See "About cubes" on page 32.

Modifying a cube view

You can modify a cube view that you previously created.

To modify a cube view

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics > Cubes**, and then select the cube that contains your saved view. For example, click the **Computers** cube.

3 In the toolbar at the top of the cube page, click **Open**.

4 In the **Open Cube View** dialog box, in the **Saved Cube Views** drop-down list, select the saved view to load, and then click **Open**. The page refreshes and displays the table view under the name of the cube.

5 Modify the configuration as necessary.

6 In the toolbar at the top of the page, click **Save**.

7 In the **Save Cube View** dialog box, select one of the following options:

Save the current configuration as a new view.	■ Click **Save as new view**. ■ In the **Save as new view** box, name the cube view.
Overwrite a previously saved cube view with the new configuration.	■ Click **Save as existing view**. ■ In the **Save as existing view** drop-down list, select the cube view that you want to overwrite.

8 (Optional) Check **Available to All Users** if this view should be publicly available. Otherwise, leave the box unchecked (default).

9 Click **Save**. The page refreshes and displays the table view under the name of the cube.

See "About cubes" on page 32.

Deleting a cube view

You can delete a cube view that you previously created.

To delete a view

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics > Cubes**, and then select the cube that contains your saved view. For example, click the **Computers** cube.

3 In the toolbar at the top of the cube page, click **Open**.

4 In the **Open Cube View** dialog box, in the **Saved Cube Views** drop-down list, select the saved view to load, and then click **Open**. The page refreshes and displays the table view under the name of the cube.

5 In the toolbar at the top of the cube page, click **Delete**.

6 In the **Message from webpage** dialog box, click **OK**.

7 In the **Message from webpage** dialog box, click **OK**. When you refresh the cube page, the page refreshes without the saved view under the name of the cube.

See "About cubes" on page 32.

Exporting cube results

You can export data from a cube list to other programs, such as Microsoft Excel.

If you want to further analyze the data, you can export the list to a Microsoft Excel pivot table. You can also print a customized version of the data from a Microsoft Excel pivot table. This feature requires that you install Microsoft Excel on each computer that connects to the Symantec Management Console.

To export cube results

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics > Cubes**, and then select a cube and open an existing table view. If there is not an existing table view, drag and drop some measures and dimensions to create a table view.

3 In the toolbar at the top of the table view, click the **Export to Microsoft Office Excel** symbol (green x with pencil).

4 Follow the on-screen instructions.

See "About cubes" on page 32.

Viewing a Dashboard report

Dashboards display a top-level management view of precompiled data in a graphical and color-rich format.

Dashboards also provide click-through features so that you can drill down and view the underlying reports in detail.

See "Ways to access IT Analytics reports" on page 31.

To view Dashboard reports

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics > Dashboards**.

3 Select a Dashboard to view.

See "Viewing a detailed report" on page 50.

See "Creating a new report" on page 50.

See "Adding reports" on page 27.

Viewing a detailed report

Reports provide you with access to various data views.

They also provide you with click-through capabilities to the Symantec Management Console pages.

See "Ways to access IT Analytics reports" on page 31.

To view a detailed report

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > IT Analytics > Reports**.
3. Expand a folder, and then select a report to view.

See "Viewing a Dashboard report" on page 49.

See "Creating a new report" on page 50.

See "Adding reports" on page 27.

Creating a new report

You can create new SQL Server Reporting Services reports by using the SQL Server Reporting Services Report Builder.

The Report Builder provides you with access to the cubes that let you create the customized reports that you can distribute.

Report Builder is a client-side application that you can use to create and design reports. Using Report Builder, you can design the reports that are based on your data. You can use Report Builder without having to understand the underlying schema or complex programming languages.

Depending on which version of SQL Server you are running, you may have different options available to you in Report Builder. SQL Server 2008 SP1, 2008 R2 or 2012 includes Report Builder 2.0 or 3.0.

Note: Symantec recommends using SQL Server 2008 SP1, 2008 R2 or 2012 to take advantage of the new features that are included in Report Builder 2.0/3.0. These features allow for a more robust custom report creation experience.

To create a report in Microsoft Report Builder 1.0 (SQL Server 2008 non-SP1)

To create a report in Microsoft Report Builder 2.0/3.0 (SQL Server 2008 SP1 or Higher)

To create a report in Microsoft Report Builder 1.0 (SQL Server 2008 non-SP1)

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.
3. Click **Reports**.
4. In the right pane, click the **Report Builder** tab.
5. Click **Launch Report Builder**.
6. In the right pane of the **Report Builder**, under the configuration options, select a Reporting Services Site.

   The default is http://servername/ReportServer.
7. Select a data source for your report.

   Choose from any of the installed cubes. For example, **Computer Cube**.
8. Select a report layout.

   For example, Chart.
9. Click **OK**.

   The Object Explorer appears on the left side, and a Report Model appears in the center of your screen.
10. In the top left pane, select from the available entities.

    The available fields for each entity appear in the lower left pane.
11. In the lower left pane, drag and drop fields to one of the categories in the report model.

    Keep dragging and dropping fields until the report displays what you want it to the way you want it to. For example, you can drag and drop data value fields, series fields, or category fields.
12. Name your report.

13 Click **Run Report** on the toolbar to ensure the report renders properly.

If the report does not run correctly, click **Design Report** on the toolbar and make the necessary changes.

14 Click **Save** on the toolbar to save your report.

Save your report with a name that represents how the report displays in the Symantec Management Console. The file name is used to name the report in the Symantec Management Console.

To link this report to the Symantec Management Console

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics**, and then do one of the following actions:

If you want the report to appear in the Dashboards folder:	■ Right-click **Dashboards**. ■ Click **New > IT Analytics Report**.
If you want the report to appear in one of the Report folders:	■ Expand **Reports**. ■ Right-click the folder in which you want the report to appear. ■ Click **New > IT Analytics Report**.

3 In the **Add Report** dialog box, in the **Report Type** drop-down list, select **Dashboard** or **Report**.

4 In the **Report Name** drop-down list, select the report that you saved.

5 In the **Parameter Area** drop-down list, select **Initially Visible** or **Initially Collapsed**.

6 Click **Add Report**, and then click **Close**.

7 On the **Reports** menu, click **All Reports**.

8 In the left pane, do one of the following actions:

If you added the report the **Dashboard** folder:	■ Expand **Reports > IT Analytics > Dashboards**. ■ Click the Dashboard that you added and verify that the report renders properly.

If you added the report to one of the Report folders:	■ Expand **Reports > IT Analytics > Reports**. ■ Expand the Report folder in which you added your report. ■ Click the report that you added and verify that it renders properly.

To create a report in Microsoft Report Builder 2.0/3.0 (SQL Server 2008 SP1 or Higher)

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand **IT Analytics Settings**, and then click **Reports**.
3. In the right pane, on the **Reports** page, on the **Report Builder** tab, click **Launch Report Builder**.
4. In the **Getting Started** dialog box, in the left pane click **New Report**, and then in the right pane, click **Blank Report**.
5. In the **Report Builder** workspace, click **Click to add title** and type an appropriate title for the report.
6. In the **Report Data** pane, right-click **Data Sources**, and then click **Add Data Source**.
7. In the **Data Source Properties** dialog box, in the **Name** box, type **IT Analytics** as the data source name, and then click **Use a connection embedded in my report**.
8. In the **Select connection type** drop-down list, click **Microsoft SQL Server Analysis Services**, and then click **Build**.
9. In the **Connection Properties** dialog box, do on of the following:

If SQL is local to where you are running Report Builder:	■ In the **Server name** box, type "**.**" for the name of the SQL Server. ■ In the **Select or enter a database name** drop-down list, click **IT Analytics**. ■ Click **OK**.
If SQL is not local to where you are running Report Builder:	■ In the **Server name** box, type name of the SQL Server. ■ In the **Select or enter a database name** drop-down list, click **IT Analytics**. ■ Click **OK**.

10. In the **Data Source Properties** dialog box, click **OK**.
11. In the **Report Data** pane, right-click **Datasets**, and then click **Add Dataset**.

12 In the **Dataset Properties** dialog box, in the left pane, click **Query**.

13 In the **Name** box, use the default name: **DataSet1**.

14 Click **Use a dataset embedded in my report**, then in the **Data source** drop-down list, click **IT Analytics**, and then click **Query Designer**.

15 In the **Query Designer**, click the **...** symbol.

16 In the **Cube Selection** dialog box, select a cube, and then click **OK**.

   For example, click **Computers**.

17 In the **Query Designer** in the **Metadata** pane, expand the measures and attributes within the cube and drag the desired fields into the query workspace.

   Keep dragging and dropping fields until the report displays what you want, the way you want.

18 When you are finished, click **OK**.

19 In the **Dataset Properties** dialog box, click **OK**.

20 In the **Report Builder**, in the report builder menu, on the **Insert** tab, click **Chart > Chart Wizard**.

21 In the **New Chart** wizard, on the **Choose a dataset** page, click **DataSet1** (the data set that you previously created), and then click **Next**.

22 On the **Choose a chart type** page, select a chart type, and then click **Next**.

23 On the **Arrange chart fields** page, drag relevant attributes from the **Available fields** list to the **Series** list. Drag relevant measure from the **Available fields** list to the **Values** list. Drag relevant attributes from the **Available fields** list to the **Categories** list.

24 When you are finished, click **Next**.

25 On the **Choose a style** page, select a chart style, and then click **Finish**.

26 In the **Report Builder**, modify the chart title, chart size, or legend properties as needed.

27 In the report builder menu, on the **Home** tab, click **Run** to preview the report and make additional adjustments.

   You are presented with a preview of your report with real-time data.

28 On the **Run** tab, click **Design** to return to the **Design** view.

29 In the toolbar at the top of the **Report Builder**, click the **Save** symbol (disc) and save this report to the Report Server **IT Analytics** folder.

Save your report with a name that represents how the report displays in the Symantec Management Console. The file name is used to name the report in the Symantec Management Console.

30 Close the **Report Builder**.

To link this report to the Symantec Management Console

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Reports > IT Analytics**, and then do one of the following actions:

If you want the report to appear in the Dashboards folder:	■ Right-click **Dashboards**. ■ Click **New > IT Analytics Report**.
If you want the report to appear in one of the Report folders:	■ Expand **Reports**. ■ Right-click the folder in which you want the report to appear. ■ Click **New > IT Analytics Report**.

3 In the **Add Report** dialog box, in the **Report Type** drop-down list, select **Dashboard** or **Report**.

4 In the **Report Name** drop-down list, select the report that you saved.

5 In the **Parameter Area** drop-down list, select **Initially Visible** or **Initially Collapsed**.

6 Click **Add Report**, and then click **Close**.

7 On the **Reports** menu, click **All Reports**.

8 In the left pane, do one of the following actions:

If you added the report the **Dashboard** folder:	■ Expand **Reports > IT Analytics > Dashboards**. ■ Click the Dashboard that you added and verify that the report renders properly.
If you added the report to one of the Report folders:	■ Expand **Reports > IT Analytics > Reports**. ■ Expand the Report folder in which you added your report. ■ Click the report that you added and verify that it renders properly.

See “Viewing a Dashboard report” on page 49.

See “Viewing a detailed report” on page 50.

See “Adding reports” on page 27.

Displaying cube data results in a chart or table

You can display cube data as either a chart or table. The default presentation is a pivot table.

Usually, it is easier to configure a table with the required fields and configuration. Then, you can switch to a chart, instead of building a chart from the beginning.

- Charts make it easier to compare data because you can see a summary of the information in graphical format.
- Tables make it easier to identify specific values because you can expand and collapse various rows and columns. A table is the default view for cube information.

To display results in a table

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand the **IT Analytics>Cubes** folder.
3. Click the cube that you want to create a table for.

   For example, the **Computers** cube.
4. From the toolbar at the top of the page, click **Display as Table**. Table view is the default view.
5. On the cube toolbar, click the **Field List** icon . The **Field List** box displays the fields that are available within the cube.

   You can position the available fields on the table by dragging and dropping fields from the **Field List** box.

   You can also use filters to define the data for each field that you want displayed in the chart.

   See “OWC Behavior - Cube fields” on page 44.

   See “OWC Behavior - Cube toolbar functions” on page 45.
6. Once you have configured the cube data, you can choose to save the view. By saving the view, you do not have to reconfigure the data that you most commonly access.

   See “Saving a cube view” on page 38.

To display results in a chart

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand the **Cubes** folder.
3. Click the cube that you want to configure a chart for.

   For example, the **Computers** cube.
4. From the toolbar at the top of the page, click **Display as Chart**.
5. On the cube toolbar, click the **Field List** icon. The **Field List** box displays the fields that are available within the cube.

   You can position the available fields on the table by dragging and dropping fields from the **Field List** box.

   You can also use filters to define the data for each field that you want displayed in the chart.

   See "OWC Behavior - Cube fields" on page 44.

   See "OWC Behavior - Charts toolbar functions" on page 46.
6. Once you have configured the cube data, you can choose to save the view. By saving the view, you do not have to reconfigure the data that you most commonly access.

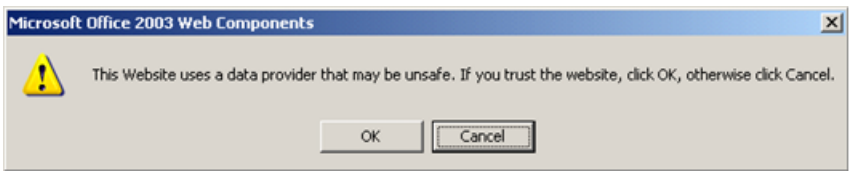
   See "Saving a cube view" on page 38.

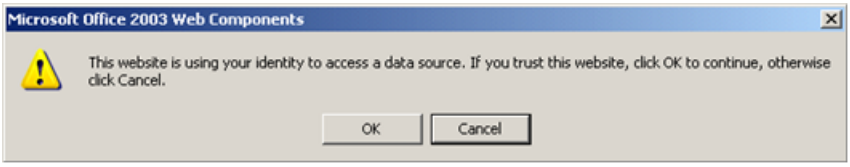
See "Creating a table using the ServiceDesk Incidents cube example" on page 59.

See "About Key Performance Indicators (KPIs)" on page 33.

Removing warning messages

While trying to access cubes, you might encounter the following warning messages:





Click **OK** in both of these instances.

These warnings can be attributes to Internet Explorer security settings and might display when the following conditions occur:

- A field list attempts to access the data that is on another domain. For example, if the hostname of the SQL Server Analysis Server is different than the hostname of Symantec Management Platform.
- The site that the control accesses is not included in the list of trusted sites.

You need to change your Internet Explorer security settings so these warning messages do not appear.

To remove warning messages

1. In Internet Explorer, on the **Tools** menu, click **Internet Options**.
2. On the **Security** tab, select the appropriate Web content zones (**Local Intranet** and **Trusted Sites**).
3. For the **Local Intranet** zone, add the URL string for the Symantec Management Console.

   For example, http://localhost/.
4. For the **Trusted Sites** zone, add the URL string for the Symantec Management Console.

   For example, http://servername/.
5. Click **Local Intranet Zone**.
6. Click **Custom Level**.
7. Under **Miscellaneous**, set **Access data sources across domains** to **Enable**.
8. Under **User Authentication**, set the **Logon** box to **Automatic logon with current user name and password**.
9. Repeat for the **Trusted Sites** zone.

   This page no longer prompts the user for credentials or trusts the Web site and data provider.

See "Verifying your installation" on page 28.

See "About cubes" on page 32.

Creating a table using the ServiceDesk Incidents cube example

You can create a ServiceDesk Incidents table that displays the count of incidents that have exceeded their SLA within the past month in this example.

To create a ServiceDesk Incidents table

1. In the **Symantec Management Console**, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand the **IT Analytics > Cubes** folder.
3. Choose the **ServiceDesk Incidents** cube.
4. Click **Field List**.

   The **Field List** displays the fields that are available within the cube. You can add each of these fields to the table to shape your results.
5. In the **ServiceDesk Incidents** cube, expand **Totals**.
6. Click **Incident Count** and then drag it to the Drop Totals or Detail Fields Here section. This selects the measure value that you want to use. Measures, or totals, are the aggregate summary counts for each cube.

   Your data is totaled in the metric.
7. Click **Exceeded SLA Count** and then drag it to the Drop Totals or Detail Fields Here section.
8. From the **Field List**, click **Date Opened - Month**, and then drag it to the **Row** area.
9. From the **Field List**, click **Incident - Status**, and then drag it to the **Row** area. This field gives you a count of the incidents in various statuses.
10. Because you already have an existing field (**Date Opened - Month**), you have the option to place the new field before or after the existing field.

    A blue bar highlights the existing field. You can place the field in different places to dynamically change how your data is presented.
11. Expand the **Date Opened - Month** row by clicking the plus sign (+) next to the current or the previous month. In the **Totals** area, you can view the number of incidents that have been opened and closed and the number of which exceeded the SLA.

See "Displaying cube data results in a chart or table" on page 56.

See "About cubes" on page 32.

Creating Key Performance Indicators (KPIs) - ServiceDesk

IT Analytics ServiceDesk Content Pack lets you create KPIs by manually defining them in the console navigation under the Settings folder. You can also directly create KPIs through the tables.

See "About Key Performance Indicators (KPIs)" on page 33.

This procedure is an example of creating KPIs for percent of the unplanned incidents that are defined through the cube. The example highlights how this procedure automatically populates some of the MDX code that is needed to define the KPI.

To create KPIs

1. In the **Symantec Management Console**, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand the **Cubes** folder.
3. Click **ServiceDesk Incidents**.
4. Click anywhere inside the cube to display the **Field List**.
5. Click and drag the **Date Opened - Month** field into the **Drop Row Fields Here** section.
6. Click and drag **Incident - Status** into the **Drop Row Fields Here** section.
7. Click and drag **Incident Count** into the **Drop Totals or Detail Fields Here** section.
8. Click and drag **Exceeded SLA Count** into the **Drop Totals or Detail Fields Here** section.
9. Click the plus sign (+) next to the current month under **Date Opened - Month**.
10. Right-click the cell in the cube that represents **Exceeded SLA Total** and click **Use as KPI Value**.
11. Right-click the cell in the cube that represents **Incident Status Total** and click **Use as KPI Value**.
12. In the **New Key Performance Indicator** section, verify that **KPI Value** and **KPI Goal** are defined.
13. Click **Create KPI**.
14. In the resulting pop-up window, in the **KPI Name** box, enter **Percent of Incidents Exceeding SLA**.
15. Verify that the following boxes are correctly filled out:

- **Database Name**. This box should be the name of the Analysis Services database that IT Analytics Server is configured to use.
- **Cube Name**. This box should already be set to the ServiceDesk Incidents cube.
- **Associated Measure Group**. This box should already be set to Client.
- **Value Expression**. This box should already be populated with the MDX code that represents the measure that was selected for the KPI Value.
- **Goal Expression**. This box should already be populated with the MDX code that represents the measure that was selected for the KPI Goal. You might want to compare the number of computers where the firewall is not installed to a percentage of all computers. By adding “0.1*” directly before the MDX string, you define your goal as 10% of all computers. With this measure in place, any KPI value that is less than your goal is acceptable. Any value that is more than your goal is an undesirable state where there are too many computers in the environment with critical patch vulnerabilities.

16 Click **Save KPI**.

17 Click **Close**.

18 Click **OK** to allow the window to refresh.

19 On the **Reports > IT Analytics** menu, click **Key Performance Indicators**.

The new KPI should now display in the list with the current value and goal already defined. The calculated measures that are associated with the KPI (Goal, Status, and Value) is displayed in the pivot table field list the next time you browse the cube, alongside the default measures.

See “Displaying cube data results in a chart or table” on page 56.

See “Setting the status of a KPI (advanced) - ServiceDesk” on page 61.

Setting the status of a KPI (advanced) - ServiceDesk

IT Analytics ServiceDesk Content Pack can leverage some of the graphical capabilities of Analysis Services and Reporting Services. It looks for visual status indicators, such as a stoplight or other images. This functionality gives a quick, high-level view of the current state of defined KPI.

The Status Expression of the KPI is defined as a number between 1 and -1. The most flexible way of defining how these values are populated is through an MDX string.

This procedure is an example of enhancing the KPI that was created in the following topic:

See "Creating Key Performance Indicators (KPIs) - ServiceDesk" on page 60.

To set the status of a KPI

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.
3. Click **Key Performance Indicators** to edit the KPI that was already created.
4. In the **Value Expression** box, change the MDX code to:

```
Round((sum({[Date Opened].[Date Opened - Month].&[8]},
[Measures].[Exceeded SLA Count]))/(sum({[Date Opened].[Date Opened - Month].&[8]},
[Measures].[Incident Count])) *100,0)
```

   This calculated the percent of incidents that exceeded the SLA is and rounds it to zero decimal points.

5. In the **Goal Expression** box, enter '5' (five). Do not enter the single quote marks. This sets the acceptable percentage of exceeded SLAs to five percent.
6. In the **Status Expression** box, click **MDX Expression**.
7. In the text area box that pops up, enter the following MDX code:

```
Case
When
  Round((sum({[Date Opened].[Date Opened - Month].&[8]}, [Measures].
  [Exceeded SLA Count]))/(sum({[Date Opened].[Date Opened - Month].&[8]},
  [Measures].[Incident Count])) *100,0) <5
  Then 1
When
  Round((sum({[Date Opened].[Date Opened - Month].&[8]},
  [Measures].[Exceeded SLA Count]))/(sum({[Date Opened].[Date Opened - Month].&[8]},
  [Measures].[Incident Count])) *100,0) >5
  Then -1
Else 0
End
```

8. For Status Graphic, click **Traffic Light**.
9. Click **Save KPI**.
10. Click **Close**.
11. Refresh the list of KPIs.

    A stoplight should display under the Status column. It indicates the current status for this KPI.

See “About Key Performance Indicators (KPIs)” on page 33.

Chapter 4

Granting access to IT Analytics Server

This chapter includes the following topics:

- Reconfiguring the Reporting Services data sources to access the Analysis Services cubes
- Configuring Kerberos on the Symantec Management Platform and SQL Server Analysis Services and Reporting Services servers
- Configuring Kerberos for the SQL Server Analysis Services server to SQL Server Reporting Services server connection

About security

In some instances, you might want to manage a standard security configuration. In this configuration, all users of IT Analytics are granted the same rights to view cubes and report information. In this instance, a recommended best practice is to create a Domain Security Group. Your group can contain all the users and groups or users that require access. For the purpose of this configuration example, this group is called IT Analytics Users.

Users typically use the Symantec Management Console to access the content pack.

Users must have access through a Symantec Management Platform security role and have at least Symantec Guests role privileges. They must also have access to the data within the Analysis Services cubes and reporting services reports to have full functionality.

For the standard security configuration, users in the IT Analytics Users group already have access to the Symantec Guests Security role in Symantec Management Platform.

See "Granting access to cubes using the Symantec Management Console" on page 68.

See "Granting access to reports using the Symantec Management Console" on page 73.

See "Granting access to the dashboards, cubes, and reports" on page 75.

See "Symantec Management Platform role-based privileges" on page 76.

About the SQL Server Database Engine

IT Analytics provides the configuration information and the user functionality that is hosted inside Symantec Management Platform. It supports all database versions that Symantec Management Platform supports.

You can access the specific configuration information and the user functionality through the Symantec Management Console. The relational data that the CMDB hosts acts as the source for the cubes that are installed in SQL Analysis Services.

During the configuration of the Analysis Server section of the **Connections** page in the **IT Analytics Settings** folder, the data source gets created. The data source is created in the specified SQL Server Analysis Services Database that inherits the configured settings for the host Symantec Management Platform database. The data source also connects from Analysis Services to the database engine at the time of cube processing.

Specific configurations within Symantec Management Platform might cause the data sources in Analysis Services to fail to connect to the relational database engine. In case this situation happens, it is important that you understand how and when the data sources in Analysis Services are created. You should also know how to reconfigure the data sources if a connection fails.

When you click **Save Database Setting** for the Analysis Server database box, the current connection settings for CMDB are used. This situation happens while you configure the Analysis Server section of the Connection Settings. The connection settings are used to either create new data sources in the Analysis Server database (if they do not already exist). They can also overwrite the existing settings. To repair the data sources that fail to connect, click the edit symbol for the Analysis Server database box. Then, click **Save Database Settings** without altering the configuration. This action sets the data sources to the current values. This step is necessary whenever the database settings for Symantec Management Platform are altered.

If you need to make advanced configuration changes to the data sources, you can directly manipulate the data sources by using SQL Server Management Studio. For example, you might want to change the host name or its credentials. The configuration changes persist as long as the Analysis Server database is not reconfigured using the instructions in this section. This action might be necessary when Notification Server is configured to connect to the CMDB using local host. It also might be necessary when the Analysis Server database is not on the same host as Notification Server and the database engine.

See “How IT Analytics works” on page 12.

See “About SQL Server Analysis Services” on page 66.

See “About SQL Server Reporting Services” on page 72.

About SQL Server Analysis Services

SQL Server Analysis Services is accessed during the configuration of the Analysis Services database and its contents. The users that access the cubes as a source

of information for tables, charts, dashboards, and reports also access Analysis Services. In addition, the currently configured application identity of Notification Server is used to access Analysis Services during the setup process.

For the application identity to configure objects in the designated Analysis Server, one of the following conditions must be true:

- The application identity is a local administrator on the Analysis Services host computer. It also has administrator rights to the local Analysis Services instance.
- The application identity is a member of the designated Analysis Services instance server role. This membership lets the users that are not local administrators have administrative privileges on the Analysis Services instance. You can add a user to the Analysis Services server role from the SQL Server Management Studio. Add a user by accessing the properties dialog box for the Analysis Services instance. Then, navigate to the **Security** page. On this page, you can add the application identity user or a group to which the user belongs.
- The target Analysis Services database for the content pack is already created on the designated Analysis Services instance before the configuration of the Server. The application identity is in a role in that database that has administrative privileges.

The most common access to Analysis Services is for users to connect to cubes to perform analysis and run reports. These connections commonly use the cubes and the data source to an SQL Server Reporting Services report that is accessed through the Symantec Management Platform. You can also use a third-party application that is designed for cube browsing including Microsoft SQL Server Management Studio, Microsoft Excel, ProClarity, and others.

You can manage the user rights in Analysis Services through the use of roles. To view a cube, a user must be in a role that has read access to a cube. Roles also let you control the details of cubes, including the dimensions of cubes and the actual dimension members and data within cubes. You can grant read access to cubes by using the **Security** tab on the **Cube Setup** page in the Symantec Management Console.

See “How IT Analytics works” on page 12.

See “About the SQL Server Database Engine” on page 65.

See “About SQL Server Reporting Services” on page 72.

See “About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes” on page 77.

See “Configuring the content pack and IT Analytics Server” on page 20.

Granting access to cubes using the Symantec Management Console

You can grant cube access to users that do not already have administrative privileges on the Analysis Server instance that hosts the IT Analytics cubes.

To grant access to cubes

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.
3. Click **Cubes**.
4. In the right pane, click the **Security** tab.
5. (Optional) Add members to the default IT Analytics Users role or create and manage new roles.

See "Adding a user to a default role" on page 68.

See "Modifying role privileges" on page 69.

See "Creating a role" on page 70.

See "Deleting a role" on page 70.

See "Granting access to cubes using SQL Server Management Studio" on page 71.

Adding a user to a default role

You can add members to the default IT Analytics Users role.

To add a user to the default role

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.
3. Click **Cubes**.
4. In the right pane, click the **Security** tab.
5. In the **Role Members** section, click **Add**.
6. Select users or groups of users from the local computer or domain.
7. Click **OK**.

   After the screen refreshes, the selected users or groups display in the **Role Members** section.

See "Granting access to cubes using the Symantec Management Console" on page 68.

See "Modifying role privileges" on page 69.

See "Creating a role" on page 70.

See "Deleting a role" on page 70.

Modifying role privileges

You can modify the privileges for each defined role.

To modify privileges for a role

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.
3. Click **Cubes**.
4. In the right pane, click the **Security** tab.
5. Under **Automatically Scoped Roles**, check the **Enable Schedule** box to synchronize the content pack-founded security with the Symantec Management Platform's role and scoped security.

   Once the schedule box is enabled, any resource scoping that is defined in the organizational groups or views are automatically applied to the cubes. Only items in that cube which are within the same organizational group or view they have been granted access to see. The schedule indicates when the synchronization should occur.
6. Under **Security Roles**, is the list of roles within the Symantec Management Platform. Click the **Manage Cube Permissions** link next to the desired role to manage cube access for that specific role.

   An empty box indicates that members of this role do not have access to that cube. An empty box also indicates that any cubes, dashboard, or the reports that include this cube have reduced data sets or return no results. The **Synchronize** check box indicates if the role should be included in the **Automatic Scoped Roles** synchronization process.
7. In the **Manually Managed Security Roles** section, in the drop-down box, select the appropriate role to modify.

   Use the + or X options to add or remove members of the role.

   Check or uncheck the cubes to which the role should or should not have access.
8. Click **Apply**.

See "Granting access to cubes using the Symantec Management Console" on page 68.

See "Adding a user to a default role" on page 68.

See "Creating a role" on page 70.

See "Deleting a role" on page 70.

Creating a role

You can create a new role that is separate from the default IT Analytics Users role.

To create a role

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.
3. Click **Cubes**.
4. In the right pane, click the **Security** tab.
5. Under **Manually Managed Security Roles**, click **New**.
6. Enter a name for the role.
7. Add members to the role.
8. Grant read access to the required cubes.
9. Click **Save Changes**.

See "Granting access to cubes using the Symantec Management Console" on page 68.

See "Adding a user to a default role" on page 68.

See "Modifying role privileges" on page 69.

See "Deleting a role" on page 70.

Deleting a role

You can delete any roles that you created.

To delete a role

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.

3 Click **Cubes**.

4 In the right pane, click the **Security** tab.

5 Under **Roles**, select the role that you want to delete from the drop-down list.

6 Wait for the screen to refresh, and then click **Delete**.

The screen refreshes again, and a message displays at the top of the page, which states that the role was successfully deleted.

7 Click **Apply**.

See "Granting access to cubes using the Symantec Management Console" on page 68.

See "Adding a user to a default role" on page 68.

See "Modifying role privileges" on page 69.

See "Creating a role" on page 70.

Granting access to cubes using SQL Server Management Studio

As an alternative to granting access to cubes using the Symantec Management Console, you can also use SQL Server Management Studio.

See "Granting access to cubes using the Symantec Management Console" on page 68.

To grant access to a cube using SQL Server Management Studio

1 Open SQL Management Studio.

2 Connect to Analysis Services using an account that has administrative rights.

3 Within the content pack database, right-click the **Roles** folder.

4 Click **New Role**.

5 On the **Create Role** dialog box, enter IT Analytics Users as the role name.

6 Select the Read Definition database permission for the role.

7 On the **Cubes** page, set the **Access** drop-down list to Read for each cube that you want this role to have access to.

If you install additional cubes in the future, you need to explicitly grant the read privilege for each cube after you install it.

8 On the **Membership** page, click **Add** to specify users and groups for this role.

9 Click **Object Types**, and then select **Groups** to allow the security group to be added to the role.

10 Click **OK**.

11 Click **Location** and change the location to the domain for which you created the IT Analytics Users security group.

12 Click **OK**.

13 In the box for objects to select, add the IT Analytics Users group.

14 Click **OK**.

Members of this role now have the appropriate rights to view the cubes that this role permits. You might need to configure Notification Server security to see the **IT Analytics** tab and installed cubes or reports.

About SQL Server Reporting Services

SQL Server Reporting Services is accessed during the configuration of the reporting services folder and its content. The contents include the data source reports that are used to access cubes as well as the installation of dashboards and reports.

Reporting Services is also accessed each time that a user runs a report in the Symantec Management Platform. They can also access reports directly through the Reporting Services Report Manager Web site.

During configuration of the reporting services folder, the currently configured application identity of Notification Server is used to access Reporting Services.

The content pack configuration pages help with this configuration. The application identity must be granted the content manager privilege to a Reporting Server. The application identity needs this privilege to configure objects in the designated Reporting Server.

By default, the local administrators group on the Reporting Server has content manager privileges. However, if the application identity is not part of this group, it can be granted the system administrator privilege. You can start this process by navigating to the permissions page of the properties dialog box within SQL Server Management Studio for that Reporting Server.

By default, only the users in the local administrators group have access to the reports on the SQL Reporting Service. The browser role must be granted in SQL Server Reporting Server.

This role is used to access the reports through either the Symantec Management Platform or the SQL Reporting Server Web console.

The browser role can be applied at the top-level folder, where all child reports inherit the role. Alternatively, security can be applied to individual reports if you want more granular control. You can apply security within the Security tab of the Report Setup page. This functionality is similar to how Read access is administered for individual cubes. Alternatively, the Report Manager Web site within SQL Reporting Services can be used to manage user Read access to specific reports. For reports to return data, the account that you use must have at least Read access to the Analysis Server cubes that the report accesses.

See "How IT Analytics works" on page 12.

See "About the SQL Server Database Engine" on page 65.

See "About SQL Server Analysis Services" on page 66.

See "About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes" on page 77.

Granting access to reports using the Symantec Management Console

You can grant access to reports to the users that do not already have browser privileges. You can grant access by using the Symantec Management Console.

To grant access to a report using the Symantec Management Console

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Settings** folder.
3. Click **Reports**.
4. In the right pane, click the **Security** tab.
5. On the **Report configuration** page on the **Security** tab, take one of the following actions:

If you see the error "Unable to locate Browser role. Please specify the name of the Browser Role as it appears in SQL Reporting Services"	The error indicates that the content pack was unable to determine the correct name for the Browser role in Report Services. Go to step 6.
If you do not see the error "Unable to locate Browser role. Please specify the name of the Browser Role as it appears in SQL Reporting Services"	Go to step 11.

6 On the Internet, go to the **SQL Server Reporting Services Report Manager** page at the following URL:

http://*servername*/Reports

7 In SQL Reporting Services 2005, on the **Properties** tab, click **Folder Settings > New Role Assignment**.

8 Identify the correct role.

The role is in the native language for the server; therefore, it may be in a different language than is currently set in Internet Explorer. The English translation for the role is *Browser* or *Explorer*.

9 On the **Report configuration** page, in the text box, enter the role in the native language.

10 Click **Save Changes**.

11 In the **Role Members** dialog box, add members to the role.

See "About security" on page 65.

See "Granting access to reports using the Report Manager Web site" on page 74.

Granting access to reports using the Report Manager Web site

You can grant reports access to users that do not already have browser privileges on the report server instance that hosts the content pack.

See "About security" on page 65.

See "Granting access to reports using the Symantec Management Console" on page 73.

To grant access to a report using the Report Manager Web site

1 As a user with system administrator privileges for the reporting services instance, access the Report Manager Web site.

The URL for the report manager is similar to http://servername/Reports/. If you did not install SQL Server Reporting Services as the default instance, the URL might be http://servername/Reports$InstanceName/.

2 Navigate to the folder that is configured to host the IT Analytics reports.

By default, it is the **IT Analytics** folder.

3 Navigate to the **Properties** tab for the current folder.

4 In the left pane, navigate to the **Security** page.

5 Click **New Role Assignment**.

6 In the **Group or user name** box, enter IT Analytics Users.

7 Select the browser role.

8 Click **OK**.

Members of this role now have the appropriate rights to view the reports that this role permits. You might need to configure Notification Server security to see the **IT Analytics** tab and any installed cubes or reports.

9 (Optional) If the IT Analytics User or any individual users need access to create reports using Report Builder, you must grant the System User privilege.

To grant System User privilege, complete the following steps:

- Click **Site Settings** in the top right-hand corner.
- Under the **Security** header, click **Configure site-wide security**.
- Click **New Role Assignment**.
- In the **Group or user name** box, enter IT Analytics Users.
- Select the **System User** role.
- Click **OK**.

Members of this role now have the appropriate rights to create reports through Report Builder.

Granting access to the dashboards, cubes, and reports

You can grant access through a Notification Server security role to the dashboards, the cubes, and the reports that are available on the **IT Analytics Privileges** section.

To grant access to the dashboards, cubes and reports

1 In the Symantec Management Console, on the **Settings** menu, click **Security** > **Account Management**.

2 In the left pane, click **Roles**.

3 From the list of roles, select **IT Analytics Users**.

4 On the **Members** tab, click **Add Member**.

5 Select **Add Account** or **Add Role**.

6 Select the accounts and roles, and then click **OK**.

7 Click **Save changes**.

All users assigned to the IT Analytics Users role now have access to the content pack features in the Symantec Management Console. They also have full access to the installed cubes and reports.

Other Notification Server role-based privileges are provided to help you secure the data that is available within the content pack. These added privileges let administrators specify which Notification Server roles can save (author) and read (load) cube views.

See "About security" on page 65.

See "Granting access to cubes using the Symantec Management Console" on page 68.

See "Granting access to cubes using SQL Server Management Studio" on page 71.

See "Granting access to reports using the Symantec Management Console" on page 73.

See "Granting access to reports using the Report Manager Web site" on page 74.

See "Granting access to save and load views and create new reports" on page 77.

Symantec Management Platform role-based privileges

The following Symantec Management Platform role-based privileges exist.

Table 4-1 Symantec Management Platform role-based privileges

Privilege	Description
Author Private Cube Views	Lets the users save the configured table or the chart views as private views.
Author Public Cube Views	Lets the users save the configured table or the chart views as public views.
Read Private Saved Cube Views	Lets the users open or load the previously saved table or the chart views that are marked as private.
Read Public Saved Cube Views	Lets the users open or load the previously saved table or the chart views that are marked as public.
Author Key Performance Indicators	Lets the user create or edit a Key Performance Indicator from a configured table view.

See "About security" on page 65.

See "Modifying role privileges" on page 69.

Granting access to save and load views and create new reports

You can grant the privileges that allow other users to author and save table or chart views. You can let others load and read those same views and create new reports.

To grant access to save and load views and create new reports

1. In the Symantec Management Console, on the **Settings** menu, click **Security > Roles**.
2. In the left pane, select the role that you want to grant access to.
3. In the right pane, click the **Privileges** tab.
4. Scroll down to the IT Analytics privileges section, and expand it if necessary.
5. Select the privileges that you want to grant the role.
6. Click **Apply**.

   You can configure additional, scope-based security for each individual dashboard, report, or cube.

See "About security" on page 65.

See "Granting access to the dashboards, cubes, and reports" on page 75.

About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes

Before granting users access to reports, you must determine the level of control that you need over the reports and the information within the reports. How Reporting Services data sources is configured to access the Analysis Service cubes determines your level of control over reports and information within the reports.

See "Configuring the content pack and IT Analytics Server" on page 20.

The **Authentication Type** lets you choose how to configure the Reporting Services. You can use **Stored Credentials** or **Windows Integrated Authentication** as the **Authentication Type**. In the Symantec Management Console, navigate to the **IT Analytics > Settings**.

Under **Reporting Server** on the **SQL Server Settings** tab, you can view the **Authentication Type** that you selected when you initially configured the content pack.

Stored Credentials explicitly defines the user credentials. It automatically manages authentication across all application tiers because access to Reporting Services is always authenticated with the same rights for all users.

After a user logs on to IT Analytics, all user inquiries to the reports impersonate the user privileges that are specified in **Stored Credentials**. You can grant individual access to the reports, but you cannot control individual access to the information within the reports.

For example, you can allow the Asset managers to view the Asset Management reports. You can allow the Patch Management administrators to view the Patch Management reports. If you want more granular control over the information in the reports, you need to use **Windows Integrated Authentication**.

Windows Integrated Authentication lets a user's Windows credentials pass through to the Reporting Server. This method is recommended for restricting access to the Reporting Services on a per-user basis. If you use **Windows Integrated Authentication**, additional configuration might be necessary to ensure that authentication is appropriately managed across all application tiers.

Windows Integrated Authentication lets you grant individual access to the reports. It also provides a more granular control over the information that you allow users to see in the reports. **Windows Integrated Authentication** lets you filter the available cube data.

For example, you can allow Patch Management managers in different districts to view the same Patch Management reports. Because **Windows Integrated Authentication** lets you filter the available cube data, you can limit each Patch Management manager's view of the information within the reports. Now, the Patch Management managers can only view the information in the reports that is relevant to their district.

If you use **Windows Integrated Authentication** in the following environments, you need to configure Kerberos to allow a user's Windows credentials to be used for authentication purposes:

- Symantec Management Platform is installed on a different server than SQL Server Analysis Services and Reporting Services, and the Report Server **Authentication Type** is set to **Windows Integrated Authentication**

  See "Configuring Kerberos on the Symantec Management Platform and SQL Server Analysis Services and Reporting Services servers" on page 80.

- SQL Server Analysis Services and SQL Reporting Services are all installed on different servers, and the Report Server **Authentication Type** is to **Windows Integrated Authentication**

  See "Configuring Kerberos for the SQL Server Analysis Services server to SQL Server Reporting Services server connection" on page 82.

The delegation features and impersonation features that are available with **Windows Integrated Authentication** can exist across multiple servers. In order for this feature to work, the network environment in which the content pack is installed must be configured to use the Kerberos protocol.

Without the Kerberos protocol, Windows credentials are passed across only one server connection before they expire. The Kerberos protocol allows credential delegation over multiple connections.

If **Stored Credentials** provides enough control over the reports, you can reconfigure the Reporting Services data sources to use **Stored Credentials** to access the Analysis Services cubes. If you need control over the information in the reports, you can reconfigure the Reporting Services data sources to use **Windows Integrated Authentication** to access the Analysis Services cubes.

See "Reconfiguring the Reporting Services data sources to access the Analysis Services cubes" on page 79.

Reconfiguring the Reporting Services data sources to access the Analysis Services cubes

When you initially configure the content pack and IT Analytics Server, you select either **Stored Credentials** or **Windows Integrated Authentication** to access Reporting Services.

See "Configuring the content pack and IT Analytics Server" on page 20.

If you want to change your selection, you can reconfigure the Reporting Services data sources to access the Analysis Services cubes.

See "About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes" on page 77.

To reconfigure the Reporting Services data sources to access the Analysis Services cubes

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, click **Configuration**.

3 In the right pane, click the edit symbol (the yellow pencil) next to **Authentication Type**.

4 Under **Authentication Type**, select one of the following options:

- **Stored Credentials**
  Explicitly defines the user credentials. Access to Reporting Services is always authenticated with the same rights for all users.
- **Windows Integrated Authentication**
  Depending on the set-up of your environment, you may need to configure Kerberos so users can access the reports to which you grant them access.

5 Enter your user name and password.

6 Click **Save Security Settings**.

Configuring Kerberos on the Symantec Management Platform and SQL Server Analysis Services and Reporting Services servers

If you install Symantec Management Platform on a different server than the SQL Server Analysis and Reporting Services and the **Authentication Type** is set to **Windows Integrated Authentication**, users cannot access the reports to which you grant them access unless you configure Kerberos.

See "About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes" on page 77.

If **Stored Credentials** provides enough control over the reports, you can reconfigure the Reporting Services data sources to use **Stored Credentials** to access the Analysis Services cubes. Then, you do not need to configure Kerberos.

See "Reconfiguring the Reporting Services data sources to access the Analysis Services cubes" on page 79.

If you need the control that **Windows Integrated Authentication** provides over the information in the reports, you must configure Kerberos. Kerberos allows the user's credentials to pass from the Symantec Management Platform server to the SQL Server Analysis and Reporting Services server. Kerberos must be correctly configured on the following servers: Symantec Management Platform and the SQL Server Analysis and Reporting Services servers.

Kerberos Authentication and configuration is a function of Microsoft Active Domain. Although configuration and support of Kerberos authentication is beyond the support

policies of Symantec, we provide the following as guidance to help in configuring Kerberos in your environment.

To configure Kerberos on the Symantec Management Platform and SQL Server Analysis Services and Reporting Services servers

1. From Active Directory, set the computer on which the Symantec Management Platform is hosted to **Trust this computer for delegation to any server (Kerberos only)**.

   If the Application Pool that Symantec Management Platform uses in IIS uses a domain account, you also need to set that account to be trusted for delegation. If the Application Pool is using the default value "ApplicationPoolIdentity", you may skip this step.

2. Add the following Service Principal Names to the Symantec Management Platform:

   - **Setspn** - S http/*netbiosName netbiosName*
     For example, **Setspn** - S http/computer1 computer1
   - **Setspn** - S http/*Fully Qualified Domain Name netbiosName*
     For example, **Setspn** - S http/computer1.domain.com computer1

   If the Application Pool that Symantec Management Platform uses in IIS uses a domain account, you may need to set the Service Principal Names for that account instead of computer1.

   For example:

   Setspn - S http/computer1 *domain\username*

   Setspn - S http/computer1.domain.com *domain\username*

   For additional information on **Setspn**, see the Microsoft Technet Web site at the following URL:

   http://technet.microsoft.com/en-us/library/cc773257(WS.10).aspx

3. If you use SQL 2008, on the Reporting Services server edit the ReportServer.config file. Edit the config file so that *RSWindowsNegotiate/* is listed at the top of the *Authentication* node.

   You can locate this file at *SQL Server Install Directory*\MSRS10.MSSQLSERVER\ReportingServer

   The ReportServer.config file is installed on the box that hosts the Reporting Services. The config file is an XML file; use a program such as Notepad to edit the file.

   If you do not use SQL 2008, you do not need to edit the config file on the Reporting Services server.

4 If SQL Reporting Services is running as a domain account, add the following Service Principal Names for the account that the SQL Reporting Services service is running as.

- **Setspn** - S http/*netbiosName domain\username*
- **Setspn** - S http/*fqdn domain\username*

For additional information on **Setspn**, see the Microsoft | Technet Web site at the following URL:

http://technet.microsoft.com/en-us/library/cc773257(WS.10).aspx

If SQL Reporting Services is not running as a domain account, you do not need to add the Service Principal Names.

5 To make the changes take effect, restart all affected systems.

See "About security" on page 65.

See "About SQL Server Analysis Services" on page 66.

See "About SQL Server Reporting Services" on page 72.

Configuring Kerberos for the SQL Server Analysis Services server to SQL Server Reporting Services server connection

Symantec recommends that the SQL Server Analysis Services and SQL Server Reporting Services instances that IT Analytics uses reside on the same host server.

You can host these services on different servers in a highly distributed environment. However, when you host these services on different servers, additional configuration might be necessary to ensure that authentication is managed appropriately across all application tiers.

When SQL Server Analysis Services and SQL Server Reporting Services are hosted on different servers and the **Authentication Type** is set to **Windows Integrated Authentication**, an additional connection is required to pass the credentials of the user from the Reporting Server to the Analysis Server. To ensure that the user's credentials are passed successfully, you must configure Kerberos. Without configuring Kerberos, the connection is attempted as an anonymous user, which fails authentication in a typical configuration. When authentication fails, users cannot access the reports to which you grant them access. Therefore, if you need the control that **Windows Integrated Authentication** provides over the information in the reports, you must configure Kerberos.

See "About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes" on page 77.

If **Stored Credentials** provides enough control over the reports, you can reconfigure the Reporting Services data sources to use **Stored Credentials** to access the Analysis Services cubes. Then you do not need to configure Kerberos.

See "Reconfiguring the Reporting Services data sources to access the Analysis Services cubes" on page 79.

Kerberos Authentication and configuration is a function of Microsoft Active Domain. Although configuration and support of Kerberos authentication is beyond the support policies of Symantec, we provide the following as guidance to help in configuring Kerberos in your environment.

To configure Kerberos for the SQL Server Analysis Services server to SQL Server Reporting Services server connection

1. Configure the Kerberos protocol for the SQL Server Reporting Services server to SQL Server Analysis Services server connection to allow credential delegation over multiple connections.

   If Symantec Management Platform is installed on the same server as SQL Server Reporting Services, no additional configuration is required.

   If Symantec Management Platform is installed on a different server than SQL Server Reporting Services, go to step 2.

2. Configure Kerberos so that the user's credentials can pass from the Symantec Management Platform server to the SQL Server Reporting Services server.

3. From Active Directory, set the computer on which the Symantec Management Platform is hosted to **Trust this computer for delegation to any server (Kerberos only)**.

   If the Application Pool which Symantec Management Platform uses in IIS uses a domain account, you also need to set that account to be trusted for delegation.

4. Add the following Service Principal Names to the Symantec Management Platform:

   - **Setspn** - S http/*netbiosName netbiosName*
     For example, **Setspn** - S http/computer1 computer1
   - **Setspn** - S http/*Fully Qualified Domain Name netbiosName*
     For example, **Setspn** - S http/computer1.domain.com computer1

   If the Application Pool which Symantec Management Platform uses in IIS uses a domain account, you may need to set the Service Principal Names for that account instead of computer 1.

For example,

Setspn - S http/computer1 *domain\username*

Setspn - S http/computer1.domain.com *domain\username*

For additional information on **Setspn** see the Microsoft Technet Web site at the following URL:

http://technet.microsoft.com/en-us/library/cc773257(WS.10).aspx

5 If you use SQL 2008, on the Reporting Services server edit the ReportServer.config file. Edit the config file so that *RSWindowsNegotiate/* is listed at the top of the *Authentication* node.

You can locate this file at *SQL Server Install Directory*\MSRS10.MSSQLSERVER\ReportingServer

The ReportServer.config file is installed on the server that hosts the Reporting Services. The config file is an XML file; use a program such as Notepad to edit the file.

If you do not use SQL 2008, you do not need to edit the ReportServer.config file on the Reporting Services server.

6 If SQL Reporting Services is running as a domain account, add the following Service Principal Names for the account that the SQL Reporting Services service is running as.

- **Setspn** - S http/*netbiosName domain\username*
- **Setspn** - S http/*fqdn domain\username*

For additional information on **Setspn**, see the Microsoft | Technet Web site at the following URL:

http://technet.microsoft.com/en-us/library/cc773257(WS.10).aspx

If the SQL Reporting Services is not running as a domain account, you do not need to add the Service Principal Names.

7 To make the changes take effect, restart all affected systems.

See "About security" on page 65.

See "About SQL Server Analysis Services" on page 66.

See "About SQL Server Reporting Services" on page 72.

Appendix A

Cube reference

This appendix includes the following topics:

ServiceDesk Changes Cube

`ServiceDesk Changes Cube` – Contains data that is associated with ServiceDesk Change Management and represents a current status. It also represents a historical view of Change Requests in ServiceDesk.

Dimensions

- **Backout Task**
- **Change**
- **Contact Type**
- **Current Task**
- **Date Closed**
- **Date Ended**
- **Date Needed**
- **Date Opened**
- **Date Planned Start**
- **Date Scheduled**
- **Date Started**
- **Impact**
- **Location**
- **Planning Task**
- **Primary Contact**
- **Priority**
- **Reference**
- **Source**
- **Status**
- **Test Task**
- **Time Closed**
- **Time Ended**
- **Time Needed**
- **Time Opened**

- **Time Planned Start**
- **Time Scheduled**
- **Time Started**
- **Type**
- **Urgency**
- **User**
- **Voting Task**
- **Waiting Task**

Measures

`Change Count`
: The number of changes.

`Failed Change Counts`
: The number of changes that failed.

`Rejected Change Counts`
: The number of changes that were rejected.

`Closed Change Count`
: The number of closed changes.

`Completed On Time`
: The number of changes that were completed within the allotted time period.

`Contact Count`
: The number of users that are associated with the change.

`Open Change Count`
: The number of changes where the status is not a closed state.

`Reference Count`
: The number of references. References are items in your environment, such as locations, departments, and assets.

`Avg Age (Days)`
: The number of days that the change has been opened. This number is useful for understanding the age of the change. The measure is valid for all changes that do not have a Resolved or Closed state.

`Avg Age (Hours)`

The number of hours that the change has been opened. This number is useful for understanding the age of the change. This measure is valid for all changes that do not have a Resolved or Closed state.

`Avg Age (Minutes)`

The number of minutes that the change has been opened. This number is useful for understanding the age of the change. This measure is valid for all changes that do not have a Resolved or Closed state.

`Avg Cost To Implement`

The cost to implement the change. This number is averaged across all of the changes using the selected criteria.

`Avg Cost To Not Implement`

The cost to not implement the change. This number is averaged across all of the changes using the selected criteria.

`Avg Days to Close`

The number of days it takes to resolve the change.

`Avg Hours to Close`

The number of hours it takes to resolve the change.

`Avg Minutes to Close`

The number of minutes it takes to resolve the change.

`Avg Percent Complete`

The average percent complete for the changes using the selected criteria.

ServiceDesk Incidents Cube

`ServiceDesk Incidents Cube` – Contains data that is associated with ServiceDesk Incident Management and represents a current and a historical view of Incidents in ServiceDesk.

Dimensions

- **Affected User**
- **Assigned to Group**
- **Assigned to User**
- **Classification**
- **Close Code**
- **Contact Type**
- **Created by User**
- **Date Closed**
- **Date Modified**
- **Date Needed**
- **Date Opened**
- **Date Resolved**
- **Impact**
- **Incident**
- **Last Modified by User**
- **Location**
- **Owned By User**
- **Priority**
- **Queue**
- **Reference**
- **Request Channel**
- **Resolved by User**
- **SLA Escalation**
- **SLA Milestone**

- **SLA Status**
- **Status**
- **Time Closed**
- **Time Modified**
- **Time Needed**
- **Time Opened**
- **Time Resolved**
- **Type**
- **Urgency**
- **User**
- **Waiting Task**

Measures

`Avg Age (Days)`

The average number of days since the incident was created. The number is useful for understanding the age of the incident. This measure is valid for all incidents that do not have a status of Resolved or Closed.

`Avg Age (Hours)`

The average number of hours since the incident was created. The number is useful for understanding the age of the incident. This measure is valid for all incidents that do not have a status of Resolved or Closed.

`Avg Age (Minutes)`

The average number of minutes since the incident was created. This number is useful for understanding the age of the incident. This measure is valid for all incidents that do not have a status of Resolved or Closed.

`Avg Days Since Modified`

The average number of days since the incident was last modified. This measure is valid for all incidents that do not have a status of Resolved or Closed.

`Avg Days Spent`

The average days spent.

`Avg Days To Close`

The average time to close (in days). This measure is valid for all incidents that have a status of Closed.

`Avg Days To Resolve`

The average time to resolve (in days). This measure is valid for all incidents that have a status of Resolved or Closed.

`Avg Hours Since Modified`

The average number of hours since the incident was last modified. This measure is valid for all incidents that do not have a status of Resolved or Closed.

`Avg Hours Spent`

The average time spent (in hours).

`Avg Hours To Close`

The average time to close (in hours). This measure is valid for all incidents that have a status of Closed.

`Avg Hours To Resolve`

The average time to resolve (in hours). This measure is valid for all incidents that have a status of Resolved or Closed.

`Avg Minutes Since Modified`

The average number of minutes since the incident was last modified. This measure is valid for all incidents that do not have a status of Resolved or Closed.

`Avg Minutes Spent`

The average time spent (in minutes).

`Avg Minutes To Close`

The average time to close in minutes. This measure is valid for all incidents that have a status of Closed.

`Avg Minutes To Resolve`

The average time to resolve in minutes. This measure is valid for all incidents that have a status of Resolved or Closed.

`Avg Percent Complete`

The average percentage that is complete.

`Entered Thru Self Service`

The number of incidents that were entered through self service.

`Exceeded SLA Count`

The number of incidents that exceeded the defined SLA.

`SLA Count`

The number of SLAs associated.

`Incident Count`

The total number of incidents.

`Closed Incident Count`

The total number of closed incidents. This measure is valid for all incidents that have a status of Closed.

`Resolved Incident Count`

The total number of resolved incidents. This measure is valid for all incidents that have a status of Resolved or Closed.

`Resolved on First Attempt Count`

The number of incidents that were resolved on first attempt. This measure is valid for all incidents that have a status of Resolved or Closed.

`Contact Count`

The number of users that attached to the incident. The user types for a given incident include Affected User, Submitter, Resolution Provider, etc.

`Open Incident Count`

The total number of open incidents. This measure is valid for all incidents that do not have a status of Resolved or Closed.

`Reference Count`

The number of references. A reference can be a number of different associations. For example, Location, Computer, and Business Services.

`Reopened Incident Count`

The number of incidents that have been reopened.

Key Performance Indicators

`Incidents Opened in Last 30 Days`

The number of new incidents in the last 30 days.

`Percent of Incidents Escalated in Last 30 Days`

The percentage of the incidents that have been escalated in the last 30 days.

ServiceDesk Problems Cube

`ServiceDesk Problems Cube` – Contains data that is associated with the ServiceDesk Problem Management software and represents a historical view of Problems that were created in ServiceDesk.

Dimensions

- **Assigned to User**
- **Category**
- **Classification**
- **Contact Type**
- **Date Closed**
- **Date Due**
- **Date Implemented**
- **Date Opened**
- **Document Category**
- **Forum**
- **Impact**
- **Location**
- **Priority**
- **Problem**
- **Reference**
- **Source**
- **Status**
- **Time Closed**
- **Time Due**
- **Time Implemented**
- **Time Opened**
- **Urgency**
- **User**

Measures

`Avg Age (Days)`

The average number of days since the problem was created. The number is useful for understanding the age of the problem. This measure is valid for all problems that do not have a Resolved or Closed state.

`Avg Age (Hours)`

The average number of hours since the problem was created. The number is useful for understanding the age of the problem. This measure is valid for all problems that do not have a Resolved or Closed state.

`Avg Age (Minutes)`

The average number of minutes since the problem was created. The number is useful for understanding the age of the problem. This measure is valid for all problems that do not have a Resolved or Closed state.

`Avg Days Spent`

The average number of days spent.

`Avg Days To Close`

The number of days to close. This measure is valid for all problems that have a Closed state.

`Avg Hours Spent`

The average number of hours spent.

`Avg Hours To Close`

The average number of hours to close. This measure is valid for all problems that have a Closed status.

`Avg Minutes Spent`

The average number of minutes spent.

`Avg Minutes To Close`

The average number of minutes to close. This measure is valid for all problems that have a Closed status.

`Avg Percent Complete`

The average percentage that is complete.

`Problem Count`

The total number of problems.

`RFC Count`

The total number of Requests For Change.

`Closed Problem Count`

The total number of closed problems. This measure is valid for all problems that have a Resolved or Closed status.

`Contact Count`

The number of users that are attached to this problem. User types can be different values, such as Affected User, Submitter, and Resolution Provider.

`Open Problem Count`

The total number of open problems. This measure is valid for all problems that do not have a Resolved or Closed status.

`Problem Assignment Count`

The number of users and groups that are assigned to a problem. A problem can have more than one person assigned to it.

`Reference Count`

The number of references. A reference can be different associations. For example, Location, Computer, and Business Services.

Key Performance Indicators

`Problems Created in Last 30 Days`

The number of problems that have been created in the last 30 days.

Appendix B

Dashboard reference

This appendix includes the following topics:

ServiceDesk Change Trend Dashboard

Provides a high-level overview of the trends in change management. This dashboard contains the measures that include the average age, average cost to implement, average hours to close, and average percent complete.

This report also includes the graphs that show the trends for the following measures:

- Change volume over time
- Average hours to close
- Changes by day of week created
- Changes by hour of day created

ServiceDesk Incident Trend Dashboard

Provides a high-level overview of the trends in incident activity. This dashboard contains the measures that include the average age, average percent completed, average hours to resolve, and average hours to close.

The report also includes the graphs that show the trends for the following measures:

- Incident volume over time
- Average hours to resolve

- Incidents by day of week created
- Incidents by hour of day created

This report lets users filter the results by a **date range**, **type**, **classification**, **impact**, **priority**, **urgency**, **status, assigned to** and **creator**.

ServiceDesk Problem Trend Dashboard

Provides a high-level overview of the trends in problem management. This dashboard contains the measures that include the average age, average hours spent, average hours to close and average percent complete.

The report also includes the graphs that show the trends for the following measures:

- Problem volume over time
- Average hours to close
- Problems by day of week created
- Problems by hour of day created

This report lets users filter the results by a **date range**, **status**, **category**, **impact**, **priority**, **urgency**, and **assigned to**.

Appendix C

Report reference

This appendix includes the following topics:

- ServiceDesk Problems by Impact report
- ServiceDesk Problems by Priority report
- ServiceDesk Problems by Status report
- ServiceDesk Problems by Urgency report

ServiceDesk Change Search report

Displays a summary of change information.

The report lets users filter the results by a date range, type, impact, priority, urgency, and primary contact.

ServiceDesk Changes by Impact report

Displays a count of changes by impact with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, type, impact, priority, urgency, and assignee.

ServiceDesk Changes by Primary Contact report

Displays a count of changes by primary contact with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, type, impact, priority, urgency, and assignee.

ServiceDesk Changes by Priority report

Displays a count of changes by priority with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, type, impact, priority, urgency, and primary contact.

ServiceDesk Changes by Status report

Displays a count of changes by status with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, type, impact, priority, urgency, and primary contact.

ServiceDesk Changes by Type report

Displays a count of changes by type with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, type, impact, priority, urgency, and primary contact.

ServiceDesk Changes by Urgency report

Displays a count of changes by urgency with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, type, impact, priority, urgency, and primary contact.

ServiceDesk Incident Search report

Displays a summary of incident information.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Incidents by Assigned to User report

Displays a count of incidents by worker with a breakdown by year, quarter, and month.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Incidents by Classification report

Displays a count of incidents by category with a breakdown by year, quarter, and month.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Incidents by Impact report

Displays a count of incidents by impact with a breakdown by year, quarter, and month.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Incidents by Priority report

Displays a count of incidents by priority with a breakdown by year, quarter, and month.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Incidents by Status report

Displays a count of incidents by status with a breakdown by year, quarter, and month.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Incidents by Type report

Displays a count of incidents by type with a breakdown by year, quarter, and month.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Incidents by Urgency report

Displays a count of incidents by urgency with a breakdown by year, quarter, and month.

The report lets users filter the results by a month and a year date range, type, classification, impact, priority, urgency, creator, status, and assignee.

ServiceDesk Problem Search report

Displays a summary of problem information.

The report lets users filter the results by a date range, category, impact, priority, urgency, status, and assignee.

ServiceDesk Problems by Assigned to User report

Displays a count of problems by worker with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, category, impact, priority, urgency, status, and assignee.

ServiceDesk Problems by Category report

Displays a count of problems by category with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, category, impact, priority, urgency, status, and assignee.

ServiceDesk Problems by Impact report

Displays a count of problems by impact with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, category, impact, priority, urgency, status, and assignee.

ServiceDesk Problems by Priority report

Displays a count of problems by priority with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, category, impact, priority, urgency, status, and assignee.

ServiceDesk Problems by Status report

Displays a count of problems by status with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, category, impact, priority, urgency, status, and assignee.

ServiceDesk Problems by Urgency report

Displays a count of problems by urgency with a breakdown by year, quarter, and month.

The report lets users filter the results by a date range, category, impact, priority, urgency, status, and assignee.

Appendix D

Dimension attribute reference

This appendix includes the following topics:

- ServiceDesk Date Closed
- ServiceDesk Date Due
- ServiceDesk Date Ended
- ServiceDesk Date Implemented
- ServiceDesk Date Modified
- ServiceDesk Date Needed
- ServiceDesk Date Opened
- ServiceDesk Date Planned Start
- ServiceDesk Date Resolved
- ServiceDesk Date Reviewed
- ServiceDesk Date Scheduled
- ServiceDesk Date Started
- ServiceDesk Document Category
- ServiceDesk Forum
- ServiceDesk Incident
- ServiceDesk Incident Classification
- ServiceDesk Incident Close Code
- ServiceDesk Incident Impact
- ServiceDesk Incident Location
- ServiceDesk Incident Priority
- ServiceDesk Incident Request Channel
- ServiceDesk Incident Status
- ServiceDesk Incident Type
- ServiceDesk Incident Urgency
- ServiceDesk Last Modified by User
- ServiceDesk Owned by User
- ServiceDesk Planning Task

- ServiceDesk Primary Contact
- ServiceDesk Problem
- ServiceDesk Problem Category
- ServiceDesk Problem Impact
- ServiceDesk Problem Location
- ServiceDesk Problem Priority
- ServiceDesk Problem Source
- ServiceDesk Problem Status
- ServiceDesk Problem Urgency
- ServiceDesk Queue
- ServiceDesk Reference
- ServiceDesk Resolved by User
- ServiceDesk SLA Escalation
- ServiceDesk SLA Milestone
- ServiceDesk SLA Status
- ServiceDesk Test Task
- ServiceDesk Time Closed
- ServiceDesk Time Due
- ServiceDesk Time Ended
- ServiceDesk Time Implemented
- ServiceDesk Time Modified
- ServiceDesk Time Needed
- ServiceDesk Time Opened
- ServiceDesk Time Planned Start
- ServiceDesk Time Resolved
- ServiceDesk Time Reviewed
- ServiceDesk Time Scheduled

- ServiceDesk Time Started
- ServiceDesk User
- ServiceDesk Voting Task
- ServiceDesk Waiting Task

ServiceDesk Affected User

ServiceDesk Affected User contains the following dimension attributes:

- **Affected User - Address1**
- **Affected User - Address2**
- **Affected User - City**
- **Affected User - Department**
- **Affected User - Display Name**
- **Affected User - First Name**
- **Affected User - Last Name**
- **Affected User - Organizational Title**
- **Affected User - Primary Email**
- **Affected User - State**
- **Affected User - VIP**
- **Affected User - Zip**

ServiceDesk Assigned to Group Backout Task

ServiceDesk Assigned to Group contains the following dimension attributes:

- **Assigned to Group - Name**

ServiceDesk Assigned to User

ServiceDesk Assigned to User contains the following dimension attributes:

- **Assigned to User - Address1**
- **Assigned to User - Address2**
- **Assigned to User - City**

- **Assigned to User - Department**
- **Assigned to User - Display Name**
- **Assigned to User - First Name**
- **Assigned to User - Last Name**
- **Assigned to User - Organizational Title**
- **Assigned to User - Primary Email**
- **Assigned to User - State**
- **Assigned to User - VIP**
- **Assigned to User - Zip**

ServiceDesk Backout Task

ServiceDesk Backout Task contains the following dimension attributes:

- **Backout Task - Can Be Completed**
- **Backout Task - Completed By**
- **Backout Task - Created By**
- **Backout Task - Description**
- **Backout Task - Do Not Show In Task**
- **Backout Task - Is Completed**
- **Backout Task - Name**
- **Backout Task - Task Number**
- **Backout Task - Task Type Name**

ServiceDesk Change

ServiceDesk Change contains the following dimension attributes:

- **Change - Assigned CAB Name**
- **Change - Backout Plan Status**
- **Change - CAB Approval Status**
- **Change - Close Code**
- **Change - Completed**

- **Change - Implementation Plan Status**
- **Change - Open For Voting**
- **Change - Request Title**
- **Change - Risk Score**
- **Change - Test Plan Status**
- **Change - Ticket Number**
- **Change - URL**

ServiceDesk Change Impact

ServiceDesk Change Impact contains the following dimension attributes:

- **Change - Impact**

ServiceDesk Change Location

ServiceDesk Change Location contains the following dimension attributes:

- **Change - Location**

ServiceDesk Change Priority

ServiceDesk Change Priority contains the following dimension attributes:

- **Change - Priority**

ServiceDesk Change Source

ServiceDesk Change Source contains the following dimension attributes:

- **Change - Request Channel**

ServiceDesk Change Status

ServiceDesk Change Status contains the following dimension attributes:

- **Change - Status**

ServiceDesk Change Type

ServiceDesk Change Type contains the following dimension attributes:

- **Change - Type**

ServiceDesk Change Urgency

ServiceDesk Change Urgency contains the following dimension attributes:

- **Change - Urgency**

ServiceDesk Classification

ServiceDesk Classification contains the following dimension attributes:

- **Problem - Classification**

ServiceDesk Contact Type

ServiceDesk Contact Type contains the following dimension attributes:

- **Contact - Type**

ServiceDesk Created by User

ServiceDesk Created by User contains the following dimension attributes:

- **Created by User - Address1**
- **Created by User - Address2**
- **Created by User - City**
- **Created by User - Department**
- **Created by User - Display Name**
- **Created by User - First Name**
- **Created by User - Last Name**
- **Created by User - Organizational Title**
- **Created by User - Primary Email**
- **Created by User - State**
- **Created by User - VIP**

- **Created by User - Zip**

ServiceDesk Current Task

ServiceDesk Current Task contains the following dimension attributes:

- **Current Task - Can Be Completed**
- **Current Task - Completed By**
- **Current Task - Created By**
- **Current Task - Description**
- **Current Task - Do Not Show In Task**
- **Current Task - Is Completed**
- **Current Task - Name**
- **Current Task - Task Number**
- **Current Task - Task Type Name**

ServiceDesk Date Closed

ServiceDesk Date Closed contains the following dimension attributes:

- **Date Closed - Date**
- **Date Closed - Day of Week**
- **Date Closed - Month**
- **Date Closed - Quarter**
- **Date Closed - Year**

ServiceDesk Date Due

ServiceDesk Date Due contains the following dimension attributes:

- **Date Due - Date**
- **Date Due - Day of Week**
- **Date Due - Month**
- **Date Due - Quarter**
- **Date Due - Year**

ServiceDesk Date Ended

ServiceDesk Date Ended contains the following dimension attributes:

- **Date Ended - Date**
- **Date Ended - Day of Week**
- **Date Ended - Month**
- **Date Ended - Quarter**
- **Date Ended - Year**

ServiceDesk Date Implemented

ServiceDesk Date Implemented contains the following dimension attributes:

- **Date Implemented - Date**
- **Date Implemented - Day of Week**
- **Date Implemented - Month**
- **Date Implemented - Quarter**
- **Date Implemented - Year**

ServiceDesk Date Modified

ServiceDesk Date Modified contains the following dimension attributes:

- **Date Modified - Date**
- **Date Modified - Day of Week**
- **Date Modified - Month**
- **Date Modified - Quarter**
- **Date Modified - Year**

ServiceDesk Date Needed

ServiceDesk Date Needed contains the following dimension attributes:

- **Date Needed - Date**
- **Date Needed - Day of Week**
- **Date Needed - Month**

- **Date Needed - Quarter**
- **Date Needed - Year**

ServiceDesk Date Opened

ServiceDesk Date Opened contains the following dimension attributes:

- **Date Opened - Date**
- **Date Opened - Day of Week**
- **Date Opened - Month**
- **Date Opened - Quarter**
- **Date Opened - Year**

ServiceDesk Date Planned Start

ServiceDesk Date Planned Start contains the following dimension attributes:

- **Date Opened - Date**
- **Date Opened - Day of Week**
- **Date Opened - Month**
- **Date Opened - Quarter**
- **Date Opened - Year**

ServiceDesk Date Resolved

ServiceDesk Date Resolved contains the following dimension attributes:

- **Date Resolved - Date**
- **Date Resolved - Day of Week**
- **Date Resolved - Month**
- **Date Resolved - Quarter**
- **Date Resolved - Year**

ServiceDesk Date Reviewed

ServiceDesk Date Reviewed contains the following dimension attributes:

- **Date Reviewed - Date**
- **Date Reviewed - Day of Week**
- **Date Reviewed - Month**
- **Date Reviewed - Quarter**
- **Date Reviewed - Year**

ServiceDesk Date Scheduled

ServiceDesk Date Scheduled contains the following dimension attributes:

- **Date Scheduled - Date**
- **Date Scheduled - Day of Week**
- **Date Scheduled - Month**
- **Date Scheduled - Quarter**
- **Date Scheduled - Year**

ServiceDesk Date Started

ServiceDesk Date Started contains the following dimension attributes:

- **Date Started - Date**
- **Date Started - Day of Week**
- **Date Started - Month**
- **Date Started - Quarter**
- **Date Started - Year**

ServiceDesk Document Category

ServiceDesk Document Category contains the following dimension attributes:

- **Document Category - Name**
- **Document Category - Process Events**

ServiceDesk Forum

ServiceDesk Forum contains the following dimension attributes:

- **Forum - Name**

ServiceDesk Incident

ServiceDesk Incident contains the following dimension attributes:

- **Incident - Entered Thru Self Service**
- **Incident - Request Title**
- **Incident - Resolved Immediately**
- **Incident - Ticket Number**
- **Incident - URL**

ServiceDesk Incident Classification

ServiceDesk Incident Classification contains the following dimension attributes:

- **Incident - Classification**

ServiceDesk Incident Close Code

ServiceDesk Incident Close Code contains the following dimension attributes:

- **Incident - Close Code**

ServiceDesk Incident Impact

ServiceDesk Incident Impact contains the following dimension attributes:

- **Incident - Impact**

ServiceDesk Incident Location

ServiceDesk Incident Location contains the following dimension attributes:

- **Incident - Location**

ServiceDesk Incident Priority

ServiceDesk Incident Priority contains the following dimension attributes:

- **Incident - Priority**

ServiceDesk Incident Request Channel

ServiceDesk Incident Request Channel contains the following dimension attributes:

- **Incident - Request Channel**

ServiceDesk Incident Status

ServiceDesk Incident Status contains the following dimension attributes:

- **Incident - Status**

ServiceDesk Incident Type

ServiceDesk Incident Type contains the following dimension attributes:

- **Incident - Type**

ServiceDesk Incident Urgency

ServiceDesk Incident Urgency contains the following dimension attributes:

- **Incident - Urgency**

ServiceDesk Last Modified by User

ServiceDesk Last Modified by User contains the following dimension attributes:

- **Last Modified by User - Address1**
- **Last Modified by User - Address2**
- **Last Modified by User - City**
- **Last Modified by User - Department**
- **Last Modified by User - Display Name**
- **Last Modified by User - First Name**
- **Last Modified by User - Last Name**
- **Last Modified by User - Organizational Title**
- **Last Modified by User - Primary Email**
- **Last Modified by User - State**

- **Last Modified by User - VIP**
- **Last Modified by User - Zip**

ServiceDesk Owned by User

ServiceDesk Owned by User contains the following dimension attributes:

- **Last Modified by User - Address1**
- **Last Modified by User - Address2**
- **Last Modified by User - City**
- **Last Modified by User - Department**
- **Last Modified by User - Display Name**
- **Last Modified by User - First Name**
- **Last Modified by User - Last Name**
- **Last Modified by User - Organizational Title**
- **Last Modified by User - Primary Email**
- **Last Modified by User - State**
- **Last Modified by User - VIP**
- **Last Modified by User - Zip**

ServiceDesk Planning Task

ServiceDesk Planning Task contains the following dimension attributes:

- **Planning Task - Can Be Completed**
- **Planning Task - Completed By**
- **Planning Task - Created By**
- **Planning Task - Description**
- **Planning Task - Do Not Show In Task**
- **Planning Task - Is Completed**
- **Planning Task - Name**
- **Planning Task - Task Number**
- **Planning Task - Task Type Name**

ServiceDesk Primary Contact

ServiceDesk Primary Contact contains the following dimension attributes:

- **Last Modified by User - Address1**
- **Last Modified by User - Address2**
- **Last Modified by User - City**
- **Last Modified by User - Department**
- **Last Modified by User - Display Name**
- **Last Modified by User - First Name**
- **Last Modified by User - Last Name**
- **Last Modified by User - Organizational Title**
- **Last Modified by User - Primary Email**
- **Last Modified by User - State**
- **Last Modified by User - VIP**
- **Last Modified by User - Zip**

ServiceDesk Problem

ServiceDesk Problem contains the following dimension attributes:

- **Problem - Action To Date**
- **Problem - ID**
- **Problem - Next Step**
- **Problem - Resolution**
- **Problem - Resolved**
- **Problem - RFC**
- **Problem - Title**
- **Problem - URL**

ServiceDesk Problem Category

ServiceDesk Problem Category contains the following dimension attributes:

- **Problem - Category**

ServiceDesk Problem Impact

ServiceDesk Problem Impact contains the following dimension attributes:

- **Problem - Impact**

ServiceDesk Problem Location

ServiceDesk Problem Location contains the following dimension attributes:

- **Problem - Location**

ServiceDesk Problem Priority

ServiceDesk Problem Priority contains the following dimension attributes:

- **Problem - Priority**

ServiceDesk Problem Source

ServiceDesk Problem Source contains the following dimension attributes:

- **Problem - Source**

ServiceDesk Problem Status

ServiceDesk Problem Status contains the following dimension attributes:

- **Problem - Status**

ServiceDesk Problem Urgency

ServiceDesk Problem Urgency contains the following dimension attributes:

- **Problem - Urgency**

ServiceDesk Queue

ServiceDesk Queue contains the following dimension attributes:

- **ServiceDesk - Location Name**
- **ServiceDesk - Queue**

- **ServiceDesk - Queue Description**
- **ServiceDesk - Queue Id**

ServiceDesk Reference

ServiceDesk Reference contains the following dimension attributes:

- **Reference - Name**
- **Reference - System Name**
- **Reference - Type**
- **Reference - URL**

ServiceDesk Resolved by User

ServiceDesk Resolved by User contains the following dimension attributes:

- **Resolved by User - Address1**
- **Resolved by User - Address2**
- **Resolved by User - City**
- **Resolved by User - Department**
- **Resolved by User - Display Name**
- **Resolved by User - First Name**
- **Resolved by User - Last Name**
- **Resolved by User - Organizational Title**
- **Resolved by User - Primary Email**
- **Resolved by User - State**
- **Resolved by User - VIP**
- **Resolved by User - Zip**

ServiceDesk SLA Escalation

ServiceDesk SLA Escalation contains the following dimension attributes:

- **Incident - SLA Escalation Name**
- **Incident - SLA Escalation Service ID**

ServiceDesk SLA Milestone

ServiceDesk SLA Milestone contains the following dimension attributes:

- **Incident - SLA Milestone Service ID**
- **Incident - SLA Milestone Status**

ServiceDesk SLA Status

ServiceDesk SLA Status contains the following dimension attributes:

- **Incident - SLA Status**

ServiceDesk Test Task

ServiceDesk Test Task contains the following dimension attributes:

- **Test Task - Can Be Completed**
- **Test Task - Completed By**
- **Test Task - Created By**
- **Test Task - Description**
- **Test Task - Do Not Show In Task**
- **Test Task - Is Completed**
- **Test Task - Name**
- **Test Task - Task Number**
- **Test Task - Task Type Name**

ServiceDesk Time Closed

ServiceDesk Time Closed contains the following dimension attributes:

- **Time Closed - Hour**
- **Time Closed - Minute**
- **Time Closed - Second**
- **Time Closed - Time**

ServiceDesk Time Due

ServiceDesk Time Due contains the following dimension attributes:

- **Time Due - Hour**
- **Time Due - Minute**
- **Time Due - Second**
- **Time Due - Time**

ServiceDesk Time Ended

ServiceDesk Time Ended contains the following dimension attributes:

- **Time Ended - Hour**
- **Time Ended - Minute**
- **Time Ended - Second**
- **Time Ended - Time**

ServiceDesk Time Implemented

ServiceDesk Time Implemented contains the following dimension attributes:

- **Time Implemented - Hour**
- **Time Implemented - Minute**
- **Time Implemented - Second**
- **Time Implemented - Time**

ServiceDesk Time Modified

ServiceDesk Time Modified contains the following dimension attributes:

- **Time Modified - Hour**
- **Time Modified - Minute**
- **Time Modified - Second**
- **Time Modified - Time**

ServiceDesk Time Needed

ServiceDesk Time Needed contains the following dimension attributes:

- **Time Needed - Hour**
- **Time Needed - Minute**
- **Time Needed - Second**
- **Time Needed - Time**

ServiceDesk Time Opened

ServiceDesk Time Opened contains the following dimension attributes:

- **Time Opened - Hour**
- **Time Opened - Minute**
- **Time Opened - Second**
- **Time Opened - Time**

ServiceDesk Time Planned Start

ServiceDesk Time Planned Start contains the following dimension attributes:

- **Time Opened - Hour**
- **Time Opened - Minute**
- **Time Opened - Second**
- **Time Opened - Time**

ServiceDesk Time Resolved

ServiceDesk Time Resolved contains the following dimension attributes:

- **Time Resolved - Hour**
- **Time Resolved - Minute**
- **Time Resolved - Second**
- **Time Resolved - Time**

ServiceDesk Time Reviewed

ServiceDesk Time Reviewed contains the following dimension attributes:

- **Time Reviewed - Hour**
- **Time Reviewed - Minute**
- **Time Reviewed - Second**
- **Time Reviewed - Time**

ServiceDesk Time Scheduled

ServiceDesk Time Scheduled contains the following dimension attributes:

- **Time Scheduled - Hour**
- **Time Scheduled - Minute**
- **Time Scheduled - Second**
- **Time Scheduled - Time**

ServiceDesk Time Started

ServiceDesk Time Started contains the following dimension attributes:

- **Time Started - Hour**
- **Time Started - Minute**
- **Time Started - Second**
- **Time Started - Time**

ServiceDesk User

ServiceDesk User contains the following dimension attributes:

- **User - Address1**
- **User - Address2**
- **User - City**
- **User - Department**
- **User - Display Name**
- **User - First Name**

- **User - Last Name**
- **User - Organizational Title**
- **User - Primary Email**
- **User - State**
- **User - VIP**
- **User - Zip**

ServiceDesk Voting Task

ServiceDesk Voting Task contains the following dimension attributes:

- **Voting Task - Can Be Completed**
- **Voting Task - Completed By**
- **Voting Task - Created By**
- **Voting Task - Description**
- **Voting Task - Do Not Show In Task**
- **Voting Task - Is Completed**
- **Voting Task - Name**
- **Voting Task - Task Number**
- **Voting Task - Task Type Name**

ServiceDesk Waiting Task

ServiceDesk Waiting Task contains the following dimension attributes:

- **Waiting Task - Can Be Completed**
- **Waiting Task - Completed By**
- **Waiting Task - Created By**
- **Waiting Task - Description**
- **Waiting Task - Do Not Show In Task**
- **Waiting Task - Is Completed**
- **Waiting Task - Name**
- **Waiting Task - Task Type Name**

Index

S

T

U

V

W