Altiris™ IT Analytics Solution 7.1 SP2 from Symantec™ User Guide

Altiris™ IT Analytics Solution 7.1 from Symantec™ User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 Web site at the following URL:

www.symantec.com/business/support/

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

Introducing IT Analytics Solution

This chapter includes the following topics:

About IT Analytics Solution

IT Analytics Solution software complements and expands upon the reporting that is offered in many Symantec solutions. It brings multi-dimensional analysis and robust graphical reporting features to Symantec Management Platform. This functionality lets you explore data on your own, without advanced knowledge of databases or third-party reporting tools. It also lets you ask and answer you own questions quickly and easily.

See "How IT Analytics works" on page 19.

See "What's new in IT Analytics 7.1 SP2" on page 20.

See "Where to get more information" on page 22.

How IT Analytics works

IT Analytics extracts data from the CMDB as well as from external databases. Extracted data is stored in cubes within the Microsoft Analysis Services database. These cubes act as the data source for the information that is presented to you.

See “About IT Analytics Solution” on page 19.

IT Analytics Solution uses the following software components:

- Symantec Management Platform 7.1
  The primary component that interacts and accesses the functionality that IT Analytics Solution provides.
- Microsoft SQL Server Analysis Services
  Used as the primary data layer for the dashboards, cubes, and reports.
- Microsoft SQL Server Reporting Services
  Used as the presentation layer for the reports and dashboards.
- Microsoft Office Web Components 11 (2003)
  Used as one of the presentation layers to provide raw access to browse the cubes through pivot tables.

IT Analytics Solution is the foundation solution that provides all of the functional components. The solution is a prerequisite solution for IT Analytics Packs (similar to Symantec Management Platform). However, on its own, IT Analytics Solution does not contain any cubes or reports.

The actual definitions for the cubes, reports, and dashboards are contained within the IT Analytics Packs that align with the existing Symantec suites. These definitions provide the business value for IT Analytics Solution.

The following IT Analytics Packs are available for IT Analytics Solution 7.1:

- IT Analytics Client and Server Management Pack
- IT Analytics Symantec Endpoint Protection Pack
- IT Analytics ServiceDesk Pack

What's new in IT Analytics 7.1 SP2

In the 7.1 SP2 release of IT Analytics, the following new features are introduced.

Table 1-1 New features

Feature	Description
Display resource list	This feature lets users right-click a cell that contains a valid measure cell and open the **Resource List** window. This window displays all of the resources that can be derived from this cell. In this window, users can select one or more resources and launch any Item Action that is valid to those resources. See "Managing resources from the built-in cube browser" on page 69.
Cube exclusion	This feature lets users select cubes to exclude from external CMDBs cube processing to avoid duplication of data or for other purposes. For example, the user may have multiple client-facing Symantec Management Platform servers. In addition, the user may have a top tier Symantec Management Platform that serves as an Asset Management Server. The user can prevent data duplication by excluding the Asset Management Server from processing the Inventory cube, Patch Management cube, etc. See "Excluding cubes from external CMDBs cube processing" on page 36.
Localization support	IT Analytics supports the following languages, which Symantec Management Platform console also supports: ■ English ■ French ■ German ■ Italian ■ Japanese ■ Korean ■ Portuguese (Brazil) ■ Russian ■ Simplified Chinese ■ Spanish ■ Traditional Chinese
Improved prerequisite checking	This enhancement adds Installation Readiness checks to the installation process. The checks ensure that all of the components that are necessary to properly configure IT Analytics are installed on the Symantec Management Platform server.

Table 1-1 New features *(continued)*

Feature	Description
Improved the automatic configuration and installation process	This enhancement automatically configures the Analysis and Reporting Services settings when SQL Analysis and Reporting Services are detected on the server during installation. In addition, any cubes and reports that can be installed are automatically installed.

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-2 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-2 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-3 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Chapter 2

Installing and configuring IT Analytics Solution

This chapter includes the following topics:

Installing and configuring IT Analytics Solution

From the Symantec Management Console, you can install, configure, and set up your version of IT Analytics Solution.

Table 2-1 Process for installing and configuring IT Analytics Solution

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 Solution. See "Hardware prerequisites" on page 28. See "Software prerequisites" on page 28.
Step 2	Install IT Analytics Solution.	You can use the Symantec Installation Manager to install IT Analytics Solution. See "Installing IT Analytics Solution" on page 30.
Step 3	Configure IT Analytics Solution.	You can specify the names of your Analysis Services server, database, Reporting Services virtual directory, and report folder. See "Configuring IT Analytics Solution" on page 30.
Step 4	(Optional) Add and configure External CMDB connections.	You can add and configure the connections to external CMDBs. See "Adding and configuring external Symantec CMDB connections" on page 33.
Step 5	(Optional) Configure the Symantec Endpoint Protection connections.	You can configure the Symantec Endpoint Protection connections that IT Analytics Symantec Endpoint Protection Pack uses. See "Configuring Symantec Endpoint Protection connections" on page 40.
Step 6	(Optional) Configure the ServiceDesk connections.	You can configure the ServiceDesk connections that IT Analytics ServiceDesk Pack uses. See "Configuring the ServiceDesk connection" on page 43.
Step 7	Add the cubes.	You can choose the cubes that you want to include in your environment. See "Adding cubes" on page 45.

Table 2-1 Process for installing and configuring IT Analytics Solution *(continued)*

Step	Action	Description
Step 8	Add the reports.	You can choose the reports that you want to include in your environment. See "Adding reports" on page 46.
Step 9	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 46.
Step 10	Verify your installation.	You can check to see that your installation was successful and that your version of IT Analytics Solution contains all the necessary items. See "Verifying your installation" on page 47.

Hardware prerequisites

The computer you want to install IT Analytics Solution must meet the specific hardware requirements that are outlined in the Symantec Management Platform Installation Guide.

See "Installing and configuring IT Analytics Solution" on page 26.

Software prerequisites

The computer on which you want to install IT Analytics Solution must meet specific software prerequisites.

See "Installing and configuring IT Analytics Solution" on page 26.

Before you install IT Analytics Solution, the following software must be installed and configured:

- Symantec Management Platform 7.1
- Microsoft SQL Server Analysis Services
  This software is required for the IT Analytics Cube database.
  Supported versions: 2005 SP2 or higher, 2008 SP2 or higher, and 2008 R2.

For more information about proper configuration, see the Microsoft MSDN Web site at the following URL:

http://msdn2.microsoft.com/en-us/library/ms143764.aspx.

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 IT Analytics Reports.

  Supported versions: 2005 SP2 or higher, 2008 SP2 or higher, and 2008 R2.

  For more information about proper configuration, see the Microsoft MSDN Web site at the following URL:

  http://go.microsoft.com/fwlink/?LinkID=91847.

  Symantec recommends that you disable Internet Explorer Enhanced Security on the computer that hosts Microsoft SQL Server 2005 Reporting Services.

  Symantec recommends that you install SQL Server Reporting Services and SQL Server Analysis Services on the same server.

- 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:

  http://www.microsoft.com/downloads/details.aspx?familyid=d09c1d60-a13c-4479-9b91-9e8b9d835cdc&displaylang=en.

- Microsoft Office Web Components 11 (2003)

  Install this software on all computers that access the 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/downloads/details.aspx?familyId=7287252C-402E-4F72-97A5-E0FD290D4B76&displaylang=en.

- Microsoft Report Viewer

  Install this software on all computers that access the console.

  Supported versions: 2008 SP1.

  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.

Installing IT Analytics Solution

You can install IT Analytics Solution from the Symantec Management Console.

See "Installing and configuring IT Analytics Solution" on page 26.

To install IT Analytics Solution

1. Launch the Symantec Installation Manager.
2. Click **Install New Products**.
3. Change the filter from **Suites** to **Solutions**.
4. Scroll down the list, and check **IT Analytics Solution**, **IT Analytics Client Server Management Pack**, **IT Analytics Symantec Endpoint Protection Pack**, and **IT Analytics ServiceDesk Pack**.
5. Click **Review Selected Products**.
6. Click **Next**.
7. Follow the rest of the installation instructions.

Configuring IT Analytics Solution

You can configure IT Analytics Solution to meet the needs of your environment. If ADOMD.NET 9.0 is not installed, then you must install the software prerequisite first.

See "Software prerequisites" on page 28.

See "Installing and configuring IT Analytics Solution" on page 26.

See "Purging resource event data" on page 48.

To configure IT Analytics Solution

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 **General** tab.

4 Under **Analysis Server**, enter the host name of the Microsoft SQL Server Analysis Services.

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

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

5 Click **Verify Connection**, and confirm that the Analysis Server name has been verified and saved.

6 Under **Analysis Server Database**, select an Analysis Server Database.

For a new standard configuration, in the **Create New Database** box, accept the default to create a new Analysis Server Database with the IT Analytics name. If you select an existing database, note that the existing data sources are overwritten with the current Symantec Management Platform database settings.

7 Click **Verify Connection** and confirm that Analysis Server Database has been verified and saved.

8 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, specify the virtual directory in the following format:
`http://servername/ReportServer$InstanceName/` for SQL Server 2005 or
`http://servername/ReportServer_InstanceName/` for SQL Server 2008.

Symantec recommends that you type the host name of the server on which Reporting Services reside. Using `localhost` as a host name restricts the access from the Symantec Management Console to the computer where Reporting Services resides.

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

10 In the **Create new report folder** text box, accept the default to create a new IT Analytics Report Folder.

If you select an existing folder, existing data sources are overwritten with the current Analysis Server Database settings.

11 Under **Authentication Type**, click one of the following options for accessing Reporting Services:

- **Stored Credentials**

It 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.

See "About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes" on page 90.

- **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 90.

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

Configuring the parent or local Symantec CMDB as an external connection

If you installed IT Analytics on a Notification Server computer that is a parent in a hierarchy with replication, you must consider if you want IT Analytics to process data from the parent or local CMDB and downstream CMDBs. To avoid duplication of data and still process the parent or local CMDB, you must configure the parent or local CMDB as an external connection. By configuring the parent or local CMDB as an external connection, you can use the Cube Inclusion functionality. You can also configure which CMDBs should be included to process which sets of cubes.

See "Adding and configuring external Symantec CMDB connections" on page 33.

See "Including or excluding the local Symantec CMDB" on page 38.

To configure the parent or local Symantec CMDB as an external 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** folder.

3 Click **Symantec CMDB**.

4 In the right pane, under **Local Symantec CMDB Connection**, select **Do not include the Symantec CMDB configured for this Symantec Management Platform**.

5 Click **Save Changes**.

6 After the **Updating Dependencies** dialog box is complete, click **Close**.

7 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.

8 In the left pane, expand the **Connections** folder.

9 Click **Symantec CMDB**.

10 Click **Add External Connection**.

If you have already added a connection and want to add another under **External Symantec CMDB Connections**, click **Add**.

See "External Symantec CMDB connection fields" on page 34.

11 In the **Add/Edit CMDB Connection** dialog box, enter the information for each of the connection fields.

12 Click **Create**.

13 After the connection is configured, click **Close**.

Adding and configuring external Symantec CMDB connections

IT Analytics Solution lets you add Symantec CMDB connections so their relevant data can be leveraged for reporting purposes.

You need to complete these steps only if the IT Analytics Client and Server Management Pack is installed.

The IT Analytics Client and Server Management Pack lets you view data from one or more Symantec CMDBs. By default, the local Symantec CMDB on which IT Analytics is installed is used. If the local Symantec CMDB is the desired configuration, then you do not need to carry out this procedure.

If the local Symantec CMDB is part of a hierarchy for inventory replication, you must configure the local CMDB as an external connection.

See "Configuring the parent or local Symantec CMDB as an external connection" on page 32.

External Symantec CMDB connections provide global IT Analytics reporting across multiple CMDBs without the need to replicate large amounts of data. It allows multiple Notification Servers to populate all existing cubes. Notification Server computers can be configured in a hierarchy or standalone.

See "External Symantec CMDB connection fields" on page 34.

See "Editing external Symantec CMDB connections" on page 35.

See "Excluding cubes from external CMDBs cube processing" on page 36.

See "Deleting external Symantec CMDB connections" on page 37.

See "Including or excluding the local Symantec CMDB" on page 38.

See "Updating the Solution Dependencies" on page 39.

To add and configure external Symantec CMDB connections

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folder.
3. Click **Symantec CMDB**.
4. Click **Add External Connection**.

   If you have already added a connection and want to add another under **External Symantec CMDB Connections**, click **Add**.

   See "External Symantec CMDB connection fields" on page 34.
5. In the **Add/Edit CMDB Connection** dialog box, enter the information for each of the connection fields.
6. Click **Create**.
7. After the connection is configured, click **Close**.

External Symantec CMDB connection fields

You can add, edit, and modify Symantec CMDB connections by entering information for the corresponding fields.

See "Adding and configuring external Symantec CMDB connections" on page 33.

See "Editing external Symantec CMDB connections" on page 35.

See "Deleting external Symantec CMDB connections" on page 37.

Table 2-2 Fields for external Symantec CMDB connection

Field	Description
Symantec CMDB Server Name:	The name of the server that hosts the Symantec CMDB.
Symantec CMDB Database Name:	The name of the Symantec CMDB database. The default database name and schema name is Symantec_CMDB.
Symantec CMDB Database Username:	The user name for the Symantec CMDB database.
Symantec CMDB Database Password:	The password for the Symantec CMDB database.
Symantec CMDB Database Password Confirmation:	The confirming password for the Symantec CMDB database.

Editing external Symantec CMDB connections

IT Analytics Solution lets you edit Symantec CMDB connections so that data can be leveraged for reporting purposes.

See "Adding and configuring external Symantec CMDB connections" on page 33.

See "Deleting external Symantec CMDB connections" on page 37.

See "Editing the Report Integration URLs for an external Symantec CMDB" on page 36.

To edit Symantec CMDB connections

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

2 In the left pane, expand the **Connections** folder.

3 Click **Symantec CMDB**.

4 In the right pane, under the **External Symantec CMDB Connections** section, select the server that you want to edit from the drop-down list. The information appears for the server that you selected.

5 Click **Change Credentials**.

6 In the **Add/Edit CMDB Connection** dialog box change the credentials to connect to this Symantec CMDB for any of the following fields:

- Symantec CMDB Database Username

- Symantec CMDB Database Password
- Symantec CMDB Database Password Confirmation

  See "External Symantec CMDB connection fields" on page 34.

7. Click **Save**.
8. After the connection is edited, click **Close**.

Editing the Report Integration URLs for an external Symantec CMDB

The Report Integration URLs are used to specify the appropriate URL to the Resource Manager and Resource Edit screens. A number of reports provide the capability to open a resource in the Resource Manager or Resource Edit pages. If these URL for an external Symantec CMDB connection needs to be changed, it can be done here.

See "Editing external Symantec CMDB connections" on page 35.

See "Editing the Report Integration URLs for the local Symantec CMDB" on page 38.

To edit the Report Integration URLs for an external Symantec CMDB

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folder.
3. Click **Symantec CMDB**.
4. In the right pane, under the **External Symantec CMDB Connections** section, select the external Symantec CMDB connection that you want to change the URLs for.
5. Click **Change Report Integration URLs**.
6. In the **Edit Report Integration URLs** dialog box, make the edits to URLs, and click **Save**.

Excluding cubes from external CMDBs cube processing

When processing cubes, you can select cubes to exclude from external CMDBs cube processing. You can select cubes to exclude from processing to avoid duplication of data or for other purposes. For example, you may have two client-facing Symantec Management Platform servers and a third server that is your Asset repository. You can connect IT Analytics to all three servers. Then, you can only process the inventory cubes for the client-facing servers and the asset cubes for the Asset server.

See “Configuring the parent or local Symantec CMDB as an external connection” on page 32.

See “Installing and configuring IT Analytics Solution” on page 26.

See “Adding cubes” on page 45.

See “Configuring the cube processing tasks” on page 46.

To exclude cubes from external CMDBs cube processing

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folder.
3. Click **Symantec CMDB**.
4. In the right pane, under the **External Symantec CMDB Connections** section, select the CMDB connection from the drop-down list. Select the CMDB that you want to exclude the cubes from its cube processing.
5. Click **Manage Cube Inclusion Settings**.
6. In the **Manage Cube Inclusion Settings** dialog box, select the cubes that you want to exclude the CMDB from processing.
7. Click **Save**

Deleting external Symantec CMDB connections

IT Analytics Solution lets you delete Symantec CMDB connections to remove data from reports.

See “Adding and configuring external Symantec CMDB connections” on page 33.

See “Editing external Symantec CMDB connections” on page 35.

To delete Symantec CMDB connections

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folder.
3. Click **Symantec CMDB**.
4. In the right pane, under **External Symantec CMDB Connections**, select the server that you want to delete from the drop-down list.

5 Click **Delete**.

6 After the **Updating Dependencies** dialog box is complete, click **Close**.

Including or excluding the local Symantec CMDB

If you add an external Symantec CMDB connection, you can select whether you want to include the data in the local Symantec CMDB. Depending on your environment, you may want to include this local CMDB.

See "Adding and configuring external Symantec CMDB connections" on page 33.

See "Editing the Report Integration URLs for an external Symantec CMDB" on page 36.

You can include the local CMDB if you have configured external Symantec CMDBs that are not part of the same hierarchy. However, if the local CMDB is part of hierarchy for inventory replication, you may encounter some duplicate information if you include this local CMDB. To avoid duplication of data and still process the local CMDB, you must configure the local CMDB as an external connection.

See "Configuring the parent or local Symantec CMDB as an external connection" on page 32.

To include or exclude the local CMDB

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

2 In the left pane, expand the **Connections** folder.

3 Click **Symantec CMDB**.

4 In the right pane, under **Local Symantec CMDB Connection**, select to include or exclude the local Symantec CMDB.

5 Click **Save Changes**.

6 After the **Updating Dependencies** dialog box is complete, click **Close**.

Editing the Report Integration URLs for the local Symantec CMDB

The Report Integration URLs are used to specify the appropriate URL to the **Resource Manager** and **Resource Edit** pages. A number of reports provide the capability to open a resource in the **Resource Manager** or **Resource Edit** pages. If the URL needs to be changed for any reason, it can be done here.

See "Including or excluding the local Symantec CMDB" on page 38.

See “Editing the Report Integration URLs for an external Symantec CMDB” on page 36.

To edit the Report Integration URLs for the local Symantec CMDB

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folder.
3. Click **Symantec CMDB**.
4. In the right pane, under the **Local Symantec CMDB Connection** section, click **Change Report Integration URLs**.
5. In the **Edit Report Integration URLs** dialog box, make the edits to URLs, and click **Save**.
6. Click **Close**.

Updating the Solution Dependencies

Each time an external connection to a Symantec CMDB is added or removed, IT Analytics reviews all configured connections. IT Analytics evaluates what solutions are installed that should be queried when cubes are processed. If the set of solutions using a configured connection is changed, updating the dependencies ensures that all relevant solutions are queried from each external CMDB. You ensure that this change is incorporated by updating the solution dependencies.

See “Adding and configuring external Symantec CMDB connections” on page 33.

To update the solution dependencies

1. In the Symantec Management Console, on the **Settings** menu, click **Notification Server > IT Analytics Settings**.
2. In the left pane, expand the **Connections** folder.
3. Click **Symantec CMDB**.
4. In the right pane, under the **Dependencies** section, click **Update Dependencies**.
5. After the **Updating Dependencies** dialog box is complete, click **Close**.

Configuring Symantec Endpoint Protection connections

You need to complete these steps only if the IT Analytics Symantec Endpoint Protection Pack is installed.

Configure these connections before you install the IT Analytics Symantec Endpoint Protection cubes.

See "Installing and configuring IT Analytics Solution" on page 26.

To configure Symantec Endpoint Protection connections

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

   Note that if there is a saved Symantec Endpoint Protection connection, clicking the **New** option provides a new connection screen.

   See "Symantec Endpoint Protection connection fields" on page 40.
5. Click **Apply**.
6. (Optional) Add, edit, and delete Symantec Endpoint Protection connections.

   See "Adding Symantec Endpoint Protection connections" on page 41.

   See "Editing Symantec Endpoint Protection connections" on page 42.

   See "Deleting Symantec Endpoint Protection connections" on page 42.

Symantec Endpoint Protection connection fields

You can add, edit, and modify Symantec Endpoint Protection connections by entering information for the corresponding fields.

See "Adding Symantec Endpoint Protection connections" on page 41.

See "Editing Symantec Endpoint Protection connections" on page 42.

See "Deleting Symantec Endpoint Protection connections" on page 42.

See "Configuring Symantec Endpoint Protection connections" on page 40.

Table 2-3 Fields for Symantec Endpoint Protection connections

Field	Description
SEP Database Server Name:	The name of the server that hosts the Symantec Endpoint Protection Manager database.
SEP Database Name:	The name of the Symantec Endpoint Protection Manager database. The default database name and schema name is SEM5. If you use several Symantec Endpoint Protection Managers in your environment, you might want to change this name.
SEP Database Username:	The user name for the Symantec Endpoint Protection Manager database.
SEP Database Password:	The password for the Symantec Endpoint Protection Manager database.
SEP Database Password Confirmation:	The confirming password for the Symantec Endpoint Protection Manager database.

Adding Symantec Endpoint Protection connections

IT Analytics Solution lets you add Symantec Endpoint Protection connections so their relevant data can be leveraged for reporting purposes.

See “Editing Symantec Endpoint Protection connections” on page 42.

See “Deleting Symantec Endpoint Protection connections” on page 42.

See “Configuring Symantec Endpoint Protection connections” on page 40.

See “Installing and configuring IT Analytics Solution” on page 26.

To add Symantec Endpoint Protection connections

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 Endpoint Protection**.

4. In the right pane, click **New**, and enter the information for each of the connection fields.

   Note that the **New** option is not displayed if you do not have at least one Symantec Endpoint Protection connection saved.

   See "Symantec Endpoint Protection connection fields" on page 40.

5. Click **Apply**.

Editing Symantec Endpoint Protection connections

IT Analytics Solution lets you edit Symantec Endpoint Protection connections so that data can be leveraged for reporting purposes.

See "Adding Symantec Endpoint Protection connections" on page 41.

See "Deleting Symantec Endpoint Protection connections" on page 42.

See "Configuring Symantec Endpoint Protection connections" on page 40.

See "Installing and configuring IT Analytics Solution" on page 26.

To edit Symantec Endpoint Protection connections

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 Endpoint Protection**.

4. In the right pane, select the server that you want to edit from the drop-down list.

   The information appears for the server that you selected.

5. Change the information for any of the following fields:

   - SEP Database Username
   - SEP Database Password
   - SEP Database Password Confirmation

   See "Symantec Endpoint Protection connection fields" on page 40.

6. Click **Apply**.

Deleting Symantec Endpoint Protection connections

IT Analytics Solution lets you delete Symantec Endpoint Protection connections to remove data from reports.

You might have only one Symantec Endpoint Protection connection left and there are IT Analytics Symantec Endpoint Protection cubes installed on your system. In that case, you cannot delete the server until you uninstall the cubes.

See "Adding Symantec Endpoint Protection connections" on page 41.

See "Editing Symantec Endpoint Protection connections" on page 42.

See "Configuring Symantec Endpoint Protection connections" on page 40.

See "Installing and configuring IT Analytics Solution" on page 26.

To delete Symantec Endpoint Protection connections

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 Endpoint Protection**.
4. In the right pane, select the server that you want to delete from the drop-down list.
5. Click **Delete**.

Configuring the ServiceDesk connection

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

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

See "Installing and configuring IT Analytics Solution" on page 26.

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 44.
5. Click **Save**.
6. (Optional) Edit and delete the ServiceDesk connection.

   See "Editing the ServiceDesk connection" on page 44.

   See "Deleting the ServiceDesk connection" on page 45.

ServiceDesk connection fields

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

See “Editing the ServiceDesk connection” on page 44.

See “Deleting the ServiceDesk connection” on page 45.

See “Configuring the ServiceDesk connection” on page 43.

See “Installing and configuring IT Analytics Solution” on page 26.

Table 2-4 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.
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.

Editing the ServiceDesk connection

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

See “Deleting the ServiceDesk connection” on page 45.

See “Configuring the ServiceDesk connection” on page 43.

See “Installing and configuring IT Analytics Solution” on page 26.

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 44.
- 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**.

Deleting the ServiceDesk connection

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

See "Editing the ServiceDesk connection" on page 44.

See "Configuring the ServiceDesk connection" on page 43.

See "Installing and configuring IT Analytics Solution" on page 26.

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**.

Adding cubes

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

See "Installing and configuring IT Analytics Solution" on page 26.

To add cubes

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

2 In the left pane, expand the **Cubes** folders.

3 In the **Cube Setup** window, click the **Available** tab.

4 Select each cube to install.

5 Click **Save Changes**.

6 At the prompt, click **OK** to proceed with the installation.

7 Verify that the cubes were successfully created by clicking the **Installed** tab, and then review the list of cubes.

Adding reports

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

See "Installing and configuring IT Analytics Solution" on page 26.

To add reports

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

2 In the left pane, expand the **Reports** folders.

3 In the **Report Setup** window, click the **Available** tab.

4 Select each report to install.

5 Click **Save Changes**.

6 At the prompt, click **OK** to proceed with the installation.

7 Verify that the reports were successfully installed by clicking the **Installed** tab, and then review the list of reports.

Configuring the cube processing tasks

You can create and assign processing schedules for all installed cubes. Your business needs to dictate how often the cubes should be 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 use 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.

See "Installing and configuring IT Analytics Solution" on page 26.

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 the **Processing** folders.

3 Select the schedule that you want for the default processing tasks, and then click **Enable Schedule**.

4 Check the box for each available cube 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 CMDB. You can monitor its progress by viewing the events in the **Event Viewer** window while the manual processing task executes.

   This task is essential for the solution to function properly because the cubes do not contain any data until the process completes.

Verifying your installation

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

See “Installing and configuring IT Analytics Solution” on page 26.

To verify your installation

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

2 Verify that the correct items appear in your installation.

   The left pane should include the following items:

   - IT Analytics Reports
   - Cubes
     If you experience pop-up dialog boxes while your cubes load, you need to remove the warning messages.
     See “Removing warning messages” on page 66.

Purging resource event data

Certain tasks IT Analytics 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 IT Analytics data is stored for six months or a mix table row count of 1000000.

See "Configuring IT Analytics Solution" on page 30.

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. On the **Purging Maintenance** page, click the **Resource Event Data Purging Settings** tab.
4. On the **Resource Event Data Purging Settings** tab, ensure that the **Configured** option is checked.
5. Under the **Custom** section, click on the hyperlink.
6. In the **Items Selector** dialog box, expand the **Data Classes > Notification Server Events** folder, and check **IT Analytics Configuration** and **IT Analytics Usage**.
7. Click **Save Changes**.
8. (Optional) Under the **Configured** option, specify any other resource event data purge settings.
9. Click **Save Changes**.

Uninstalling IT Analytics

You can uninstall IT Analytics Solution by removing the IT Analytics Packs from Symantec Management Platform and then uninstalling IT Analytics Solution itself.

Table 2-5 Process for uninstalling IT Analytics

Step	Action	Description
Step 1	Remove the IT Analytics Packs from Symantec Management Platform.	You can use Symantec Installation Manager to remove your IT Analytics Packs. See "Removing the IT Analytics Packs" on page 49.
Step 2	Uninstall IT Analytics Solution.	You can use Symantec Installation Manager to safely remove IT Analytics Solution. See "Uninstalling IT Analytics Solution" on page 49.

Removing the IT Analytics Packs

Before you uninstall IT Analytics Solution, you need to remove all of your IT Analytics Packs.

See "Uninstalling IT Analytics" on page 48.

To remove the IT Analytics Packs

1. Launch Symantec Installation Manager.
2. In the **Installed Products** window, scroll down and click **IT Analytics Client and Server Management Pack**, **IT Analytics Symantec Endpoint Protection Pack**, and **IT Analytics ServiceDesk Pack**.
3. Click **Uninstall**.
4. To confirm the uninstall process, click **Yes**.
5. On the **Uninstallation Complete** page, click **Finish**.

Uninstalling IT Analytics Solution

You can use Symantec Installation Manager to uninstall IT Analytics Solution.

See "Uninstalling IT Analytics" on page 48.

To uninstall IT Analytics Solution

1. Launch Symantec Installation Manager.
2. In the **Installed Products** window, scroll down and click **IT Analytics Solution**.

3 Click **Uninstall**

4 To confirm the uninstall process, click **Yes**.

5 On the **Uninstallation Complete** page, click **Finish**.

Hosting Symantec Management Platform and Reporting Services on the same server

You need to perform some additional configuration to host the instance of SQL Server 2005 Reporting Services that IT Analytics Solution uses. The configuration changes let Reporting Services work on the same server as Symantec Management Platform. The IIS script that runs as part of the Symantec Management Platform installation causes the default Reporting Services virtual directories to stop functioning.

To fix this issue, create a separate IIS Web site and application pool for Reporting Services.

Symantec recommends that do not use the default Web site and default application pool for Symantec Management Platform. Also, avoid creating a new Web site and application pool to use with the two virtual directories that SQL Server 2005 Reporting Services requires.

See "About SQL Server Reporting Services" on page 83.

To host Symantec Management Platform and Reporting Services on the same server

1 In the `c:\inetpub` directory, create a new folder to use as the base folder for the new Web site.

2 Assign a descriptive name to the new folder (for example, ReportingServices).

3 On the server that hosts Symantec Management Platform and SQL Reporting Services, launch IIS.

4 In IIS, expand the **servername** node.

5 Right-click the **Web Sites** node, and then click **New** > **Web site**.

6 On the **Web Site Creation Wizard** page, click **Next**.

7 In the **Description** box, type a descriptive name for the new Web site (for example, ReportingServices).

8 Click **Next**.

9 Set the appropriate IP address and port settings.

- In the **IP Addresses** drop-down list, the default is usually **All Unassigned**. However, you can specify that this Web site is configured to a specific IP address. Change this box only if you know the appropriate setting.
- For the TCP port, use a port that is not currently in use by another Web site under IIS. You can check the ports that other Web sites use by clicking **Properties** under the Web site folder. Usually, the default Web site is configured to use port 80. You can also use port 8080, which is a common practice.
- Leave the **Host Header** box blank.

10 Click **Next**.

11 In the path box, browse to the new folder that you created.

Leave **Allow anonymous access to this Web site** checked.

12 Click **Next**.

13 Check the following options:

- **Read**
- **Run scripts**
- **Execute**

14 Click **Finish**.

15 In Windows, click **Start** > **All Programs** > **Microsoft SQL Server 2005** > **Configuration Tools** > **Reporting Services Configuration** to launch SQL Reporting Services.

16 Connect to the local instance.

17 In the left pane, click **Report Server Virtual Directory**.

18 Click **New**.

19 Select the new Web site that you created.

Leave **Virtual Directory** as the default.

20 Click **OK**.

21 In the left pane, select **Report Manager Virtual Directory**.

22 Click **New**.

23 Select the new Web site that you created.

Leave **Virtual Directory** as the default.

24 Click **OK**.

25 In the left frame, click **Web Service Identity**.

26 Ensure that the Report Server and Report Manager drop-down lists specify an application pool that is different than the one that Symantec Management Platform uses.

If you cannot tell if the application pool is different, you can create a new application pool in this window. You can then use that application pool for both drop-down lists.

27 Click **Apply**.

28 Launch the Symantec Management Console.

29 On the **Home** menu, click **IT Analytics** > **Settings** > **Connections**.

30 Under **Reporting Server**, next to the **Report Server Virtual Directory URL** setting, click the edit symbol.

31 Type in the name of the server and the port number in the following format:

```
http://servername:port/ReportServer
```

Servername is the name of the server that is running Reporting Services. *Port* is the port number that you assigned to the new Web site that you created.

32 Next to the **Report Folder Name** setting, click the edit symbol.

Leave IT Analytics as the default.

33 Click **Save Folder Settings**.

34 In the left pane of the Symantec Management Console, click the **Report Setup** task.

35 Click the **Available Reports** tab.

36 Check all of the reports that you want to install.

To install all of the available reports, in the header row of the table, click **Install**.

37 Click **Apply**.

A progress window launches.

38 Once the **Close** symbol is enabled, click it.

39 Ensure that you can access the dashboards and reports.

Chapter 3

Implementing IT Analytics Solution

This chapter includes the following topics:

- Displaying results in a chart
- Displaying results in a table
- Exporting table results
- Removing warning messages
- Creating a table using the Computer cube example
- Managing resources from the built-in cube browser
- About Key Performance Indicators (KPIs)
- Creating Key Performance Indicators (KPIs)
- Setting the status of a KPI (advanced)

Ways to access IT Analytics Solution

You can access IT Analytics Solution in many ways.

See "About IT Analytics Solution" on page 19.

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 55.
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 IT Analytics. See "Viewing a dashboard report" on page 55. See "Viewing a detailed report" on page 56.

Method	Description
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. See “Managing resources from the built-in cube browser” on page 69.
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.

Viewing a cube

You can access IT Analytics Solution in many ways.

See “Ways to access IT Analytics Solution” on page 54.

To view a cube

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

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 IT Analytics reports in detail.

See “Ways to access IT Analytics Solution” on page 54.

See “Viewing a detailed report” on page 56.

See “Creating a new report” on page 56.

See “Adding reports” on page 46.

To view dashboard reports

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

Viewing a detailed report

Reports provide you with access to various IT Analytics data views. They also provide you with click-through capabilities to the Symantec Management Console pages.

See "Ways to access IT Analytics Solution" on page 54.

See "Viewing a dashboard report" on page 55.

See "Creating a new report" on page 56.

See "Adding reports" on page 46.

To view IT Analytics reports

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

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 IT Analytics 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. For more information on using this tool, see http://msdn2.microsoft.com/en-us/library/ms159267.aspx.

See "Viewing a dashboard report" on page 55.

See "Viewing a detailed report" on page 56.

See "Adding reports" on page 46.

To create a report

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.
15. In the Symantec Management Console, click the **IT Analytics** tab.

16 In the left pane, select the folder where you want the new report to appear.

17 Right-click the folder, and then click **New** > **New Report** (or click **New Dashboard** if you designed a dashboard report).

18 Select the new report from the **Report Name** drop-down list.

19 Select the initial functionality for the parameter area: visible or collapsed.

20 Click **Apply** to import the report.

21 In the left pane, select your report and verify that it renders properly.

About cubes

A cube is an interactive view of an IT Analytics Cube. You can use it to dynamically analyze data from within the Symantec Management Console. It uses Microsoft Office Web Components that are embedded within Microsoft Office products or that are freely available to download.

Cubes were developed to let you view, organize, and summarize data into on-demand, personalized reports.

See "Cube prerequisites" on page 58.

See "Cube fields" on page 59.

See "Top cube toolbar functions" on page 60.

See "Cube toolbar functions" on page 60.

See "Charts toolbar functions" on page 61.

See "Saving a cube view" on page 62.

See "Loading a table view" on page 62.

See "Modifying a table view" on page 63.

See "Deleting a view" on page 64.

See "Exporting table results" on page 66.

See "Removing warning messages" on page 66.

See "Creating a table using the Computer cube example" on page 68.

Cube prerequisites

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 58.

Cube fields

The following cube fields are available.

See “About cubes” on page 58.

Table 3-1 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.

Top cube toolbar functions

The following toolbar functions are available in the top toolbar.

See "About cubes" on page 58.

Table 3-2 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.
Display as Table	Displays the data and results as a table.
Display as Chart	Displays the data and results as a chart.

Cube toolbar functions

The following toolbar functions are available in the cube toolbar

See "About cubes" on page 58.

Table 3-3 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.

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

Function	Description
Auto Filter	Enables or disables the auto filter function. IT Analytics Solution 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.
Field List	Displays the available attributes within the cube. Each attribute can be added to the table to shape your results.

Charts toolbar functions

The following toolbar functions are available only for charts.

See "About cubes" on page 58.

Table 3-4 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.

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.

See "About cubes" on page 58.

To save a cube view

1. Configure a table or chart.
2. From the toolbar at the top of the page, click **Save**.
3. In the **Save View** dialog box, choose from the following options:

Save as New View	Saves the current configuration as a new view with the name that you specify.
Save as Existing View	Overwrites a previously saved view with the current configuration.

4. Check **Available to All Users** if this view should be publicly available.

   Otherwise, leave the box unchecked (default).
5. Click **Save**.

Loading a table view

You can load a table view that you previously created.

See "About cubes" on page 58.

To load a table view

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 contains your saved view.

   For example, the Computer cube.
4. From the toolbar at the top of the page, click **Open**.

5 From the drop-down list, select the saved view to load.

6 Click **Open**.

The page refreshes and displays the name of the view under the name of the cube.

Modifying a table view

You can modify a table view that you previously created.

See “About cubes” on page 58.

To modify a table view

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 contains your saved view.

For example, the Computer cube.

4 From the toolbar at the top of the page, click **Open**.

5 From the drop-down list, select the saved view that you want to modify.

6 Click **Open**.

The page refreshes and displays the name of the view under the name of the cube.

7 Modify the configuration as necessary.

8 From the toolbar at the top of the page, click **Save**.

9 In the **Save View** dialog box, choose from the following options:

Save as New View	Saves the current configuration as a new view with the name that you specify.
Save as Existing View	Overwrites a previously saved view with the current configuration.

10 Check **Available to All Users** if this view should be publicly available.

Otherwise, leave the box unchecked (default).

11 Click **Save**.

The page refreshes and displays the name of the view under the name of the cube.

Deleting a view

You can delete a view that you previously created.

See "About cubes" on page 58.

To delete a view

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 contains your saved view.

For example, the Computer cube.

4 From the toolbar at the top of the page, click **Open**.

5 From the drop-down list, select the saved view that you want to delete.

6 Click **Open**.

The page refreshes and displays the name of the view under the name of the cube.

7 From the toolbar at the top of the page, click **Delete**.

8 Click **OK** to confirm the deletion.

9 Click **OK** to confirm that the view has been deleted.

The page refreshes without a named view under the name of the cube.

About displaying cube data results

You can display cube data as either a table or chart. Both tables and charts let you interact with and drag and drop the available fields. 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.

You can position the available fields on the chart or 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. For example, you can check **Altiris Managed** only.

See "About cubes" on page 58.

Table 3-5 Cube data results display options

Display option	Description
Chart	Lets you see a summary of the information in graphical format for easier comparison. See "Displaying results in a chart" on page 65.
Table	Lets you expand and collapse rows and columns to identify specific values. This option is the default view. See "Displaying results in a table" on page 65.

Displaying results in a chart

Charts make it easier to compare data because you can see a summary of the information in graphical format.

See "About cubes" on page 58.

See "About displaying cube data results" on page 64.

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 Computer cube.

4 From the toolbar at the top of the page, click **Display as Chart**.

Displaying results in a table

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.

See "About cubes" on page 58.

See "About displaying cube data results" on page 64.

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 **Cubes** folder.

3 Click the cube that you want to create a table for.

For example, the Computer cube.

4 From the toolbar at the top of the page, click **Display as Table**.

Exporting table results

You can export data from a table 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.

See "About cubes" on page 58.

To export table results

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

2 Expand the **Cubes** folder.

3 Select a cube and open an existing table view.

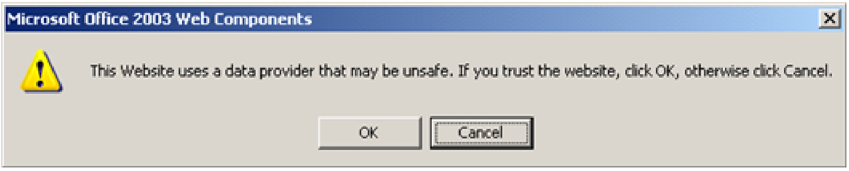
If there is not an existing table view, drag and drop some measures and dimensions to create a table view.

4 On the toolbar, click **Export to Excel**.

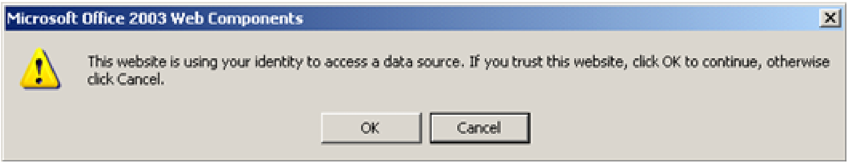
5 Follow the on-screen instructions.

Removing warning messages

While trying to access cubes within IT Analytics Solution, you might encounter the following warning messages:


Microsoft Office 2003 Web Components

This Website uses a data provider that may be unsafe. If you trust the website, click OK, otherwise click Cancel.



Microsoft Office 2003 Web Components

This website is using your identity to access a data source. If you trust this website, click OK to continue, otherwise click Cancel.

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.

See "About cubes" on page 58.

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.

Creating a table using the Computer cube example

You can create a Computer cube table that displays computers by system type, OS name, and system manufacturer in this example.

See "About cubes" on page 58.

To create a Computer cube table

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

   A list of available cubes displays.
3. Choose the Computer 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 Computer cube, expand **Totals**.
6. Click **Computer Count** to select 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. From the field list, click **Computer - OS Name**, and then drag it to the **Row** area.

   This field displays the operating system by name.
8. From the field list, click **Computer - System Manufacturer**, and then drag it to the **Row** area.
9. Because you already have an existing field (**Computer - OS Name**), you have the option of placing 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.

10 From the field list, click **Computer - System Type**, and then drag it to the **Row** area.

This field displays each system type and the total results for the name and the system manufacturer. You can select the drop-down arrow next to each System Type to further define your results.

11 Expand the **OS Name** to view the results by each system manufacturer.

In the totals area, you can view the number of each System by Type, OS Name, and System Manufacturer. Grand total values are also included at the end of each category.

Managing resources from the built-in cube browser

You can manage resources from the built-in cube browser. You can access the right-click menu options for resources from the cube browser. The right-click menu options let you access Resource Manager. They let you assign a computer to an organizational group They also let you perform other actions, such as accessing a computer by Remote Management.

See “Ways to access IT Analytics Solution” on page 54.

The right-click menu option **Display Resource List** displays only for the cubes in the Client and Server Management Pack. The cubes must have the Computer or the Asset dimension present. Resources from external CMDB connections are excluded from the resource list because you cannot manage them by using the tools that are provided. Therefore, the number of computers that are in the resource list may not match the number of resources that are shown in the field that you have selected in the cube browser.

To manage resources from the built-in cube browser

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

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

3 Select a cube to view.

4 Click **Field List**. The **Field List** displays the fields that are available within the cube. You can select the fields that you want to add to the table to shape your results.

In the **Field List** expand **Totals**.

5 Select the measure value that you want to use and drag it into the **Totals** pane of the cube browser

Continue to drag and drop any other fields that you want to add into the cube browser.

6 Right-click a field in the cube browser. The field should be a measure/total field that contains the resources.

7 On the right-click menu, click **Display Resource List**.

The pop-up window lists all of the resources that the host Symantec Management Platform manages.

8 Select one or more resources in the pop-up window, and then right-click a resource. Right-clicking a resource lets you access the right-click menu options. The right-click menu options let you perform any actions that are valid for the selected set of resources.

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.

See “Creating Key Performance Indicators (KPIs)” on page 71.

See “Setting the status of a KPI (advanced)” on page 72.

In IT Analytics Solution, KPIs are created from existing measures. However, not all measures are good candidates for KPI utilization. A measure should be leveraged in a KPI only if it represents a critical success factor to gauge performance. Besides being measurable and performance-oriented, KPIs should be used to track progress against the strategic and typically long-term goals that remain fairly static in nature.

KPIs consist of four critical elements, and IT Analytics Solution offers the flexibility to define each of the following expressions:

- A Value Expression is an MDX expression that represents the primary measurement for this KPI. For example, Computer Count.
- A Goal Expression is an MDX expression that represents the desired target for the measure that is used for the Value Expression.
- A Status Expression is typically used to compare the Value Expression with the Goal Expression. However, it can be any MDX expression that is meaningful for this KPI. This expression is typically a number between 1 (goal has been met) and -1 (goal has not been met).

- A Trend Expression is typically used to represent the current trending over time of the Value Expression as compared with the Goal Expression. However, it can be any MDX expression that is meaningful for this KPI. This expression is typically a number between 1 (increasing or getting better) and -1 (decreasing or getting worse).

The default KPIs included with the IT Analytics Solution are samples and should be reviewed and tailored to each unique environment.

For more information on KPIs in SQL Server Analysis Services, see the Microsoft TechNet Web site at the following URL:

http://technet.microsoft.com/en-us/library/ms166869(SQL.90).aspx.

Creating Key Performance Indicators (KPIs)

IT Analytics Solution 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 70.

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 **Cubes** folder.
3. Click **Patch Management Cube**.
4. Click anywhere inside the cube to display the **Field List**.
5. Click and drag the **Software Update - Severity** field into the **Drop Row Fields Here** section.
6. Click and drag **Vulnerable Computer Count** into the **Drop Totals or Detail Fields Here** section.
7. Click and drag **Applicable Computer Count** into the **Drop Totals or Detail Fields Here** section.
8. Right-click the cell in the cube that represents **Vulnerable Computer Count with Critical Severity** and click **Use as KPI Value**.
9. Right-click the cell in the cube that represents **Applicable Computer Count with Critical Severity** and click **Use as KPI Goal**.

10 In the **New Key Performance Indicator** section, verify that **KPI Value** and **KPI Goal** are defined.

11 Click **Create KPI**.

12 In the resulting pop-up window, in the **KPI Name** box, enter Computers with Critical Vulnerability.

13 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 Solution is configured to use.
- **Cube Name**. This box should already be set to the Patch Management Cube.
- **Associated Measure Group**. This box should already be set to Applicable Patches.
- **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 vulnerable computers to a percentage of all applicable computers. By adding “0.1*” directly before the MDX string, you define your goal as 10% of all applicable 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.

14 Click **Save Changes**.

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

16 In the left pane, open the **Settings** folder.

17 Click **Key Performance Indicators**.

The new KPI should now display in the list with the current value and goal already defined.

Setting the status of a KPI (advanced)

IT Analytics Solution 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.

See “Creating Key Performance Indicators (KPIs)” on page 71.

See "About Key Performance Indicators (KPIs)" on page 70.

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 **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 **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].&[Cri
[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].&[Cr
[Measures].[Applicable Computer Count])
THEN   -1
ELSE   0
END
```

6. For Status Graphic, click **Traffic Light**.
7. Click **Save Changes**.
8. Refresh the list of KPIs.

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

Chapter 4

Granting access to IT Analytics Solution

This chapter includes the following topics:

- About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes
- 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 of the users and groups of users that require access to IT Analytics. For the purpose of this configuration example, this group is called IT Analytics Users.

Users typically use the Symantec Management Console to access IT Analytics Solution. 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 “About IT Analytics Solution” on page 19.

See “Granting access to cubes using the Symantec Management Console” on page 79.

See “Granting access to reports using the Symantec Management Console” on page 84.

See “Granting access to the dashboards, cubes, and reports” on page 87.

See “Symantec Management Platform role-based privileges” on page 88.

About the SQL Server Database Engine

IT Analytics Solution provides the configuration information and the user functionality that is hosted inside Symantec Management Platform. It supports all database versions that Symantec Management Platform 7.1 supports.

You can access the solution-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 Server Analysis Services.

During the configuration of the Analysis Server section of the **Connection** page in the IT Analytics Solution **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. The SQL Server Database Engine that IT Analytics Solution uses stores the IT Analytics Solution configuration settings, events, and cube processing settings. IT Analytics Solution has no other interactions with the SQL Server Database Engine.

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 localhost. 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 19.

See “About SQL Server Analysis Services” on page 78.

See “About SQL Server Reporting Services” on page 83.

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 IT Analytics Solution is already created on the designated Analysis Services instance before the configuration of IT Analytics Solution. 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 user 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. IT Analytics also provides the ability to use the scoping security capabilities of Symantec Managements Platform. Scoping provides a method to limit the devices a particular role may view.

See "How IT Analytics works" on page 19.

See "About the SQL Server Database Engine" on page 77.

See "About SQL Server Reporting Services" on page 83.

See "Filtering role-based cubes (advanced)" on page 89.

See "About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes" on page 90.

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.

See "Adding a user to a default role" on page 79.

See "Modifying role privileges" on page 80.

See "Creating a role" on page 81.

See "Deleting a role" on page 82.

See "Granting access to cubes using SQL Server Management Studio" on page 82.

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.

Adding a user to a default role

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

See "Granting access to cubes using the Symantec Management Console" on page 79.

See “Modifying role privileges” on page 80.

See “Creating a role” on page 81.

See “Deleting a role” on page 82.

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.

Modifying role privileges

You can modify the privileges for each defined role.

See “Granting access to cubes using the Symantec Management Console” on page 79.

See “Adding a user to a default role” on page 79.

See “Creating a role” on page 81.

See “Deleting a role” on page 82.

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 IT Analytics 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**.

Creating a role

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

See “Granting access to cubes using the Symantec Management Console” on page 79.

See “Adding a user to a default role” on page 79.

See “Modifying role privileges” on page 80.

See “Deleting a role” on page 82.

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 **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 **Apply**.

Deleting a role

You can delete any roles that you created.

See "Granting access to cubes using the Symantec Management Console" on page 79.

See "Adding a user to a default role" on page 79.

See "Modifying role privileges" on page 80.

See "Creating a role" on page 81.

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**.

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 79.

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 IT Analytics 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 an IT Analytics Solution 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 IT Analytics Solution 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 IT Analytics Solution 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 19.

See “About the SQL Server Database Engine” on page 77.

See “About SQL Server Analysis Services” on page 78.

See “About configuring the Reporting Services data sources to use Stored Credentials or Windows Integrated Authentication to access the Analysis Services cubes” on page 90.

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.

See “About security” on page 76.

See “Granting access to reports using the Report Manager Web site” on page 86.

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 IT Analytics 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 textbox, enter the role in the native language.
10. Click **Save Changes**.
11. In the **Role Members** dialog box, add members to the role.

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 IT Analytics reports.

See "About security" on page 76.

See "Granting access to reports using the Symantec Management Console" on page 84.

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 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.

See “About security” on page 76.

See “Granting access to cubes using the Symantec Management Console” on page 79.

See “Granting access to cubes using SQL Server Management Studio” on page 82.

See “Granting access to reports using the Symantec Management Console” on page 84.

See “Granting access to reports using the Report Manager Web site” on page 86.

See “Granting access to save and load views and create new reports” on page 88.

To grant access to the IT Analytics features

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 IT Analytics features in the Symantec Management Console. They also have full access to the installed IT Analytics cubes and reports.

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

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 76.

See “Modifying role privileges” on page 80.

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.

See “About security” on page 76.

See “Granting access to the dashboards, cubes, and reports” on page 87.

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.

Filtering role-based cubes (advanced)

SQL Server Analysis Services has a wide range of advanced security opportunities. You can explore these opportunities through the SQL Server Management Studio. One such feature is the ability to filter the data that a role has access to by restricting access to specific members of a dimension.

You can restrict access for the IT Analytics Users role to return the cube data only for computers with a Win32 system type. For this example, you must grant access to the Computer cube for the IT Analytics Users role.

See “About security” on page 76.

See “About SQL Server Analysis Services” on page 78.

To filter a role-based cube

1 In SQL Server Management Studio, in the IT Analytics analysis services database, navigate to the properties for the IT Analytics Users role.

2 In the **Edit Role** dialog box, navigate to the **Dimension Data** page.

3 In the **Dimension** drop-down list, click the **Computer** dimension.

4 Select the **Deselect all members** radio symbol.

5 In the **Attribute Hierarchy** drop-down list, click **Computer - System Type**.

6 Select the dimension members that you want the role to have access to.

In our example, there is a Win32 member. Actual names are specific to each instance of Notification Server.

7 Navigate to the **Advanced** tab of the **Dimension Data** page.

8 Click **Enable Visual Totals**.

This step prevents the role from seeing the aggregate totals that are independent of the configured filtering and restricts aggregations.

9 Click **OK** to save the role configuration.

Users in the configured role now see the results only for the computers that have a Win32 system type across all cubes. This filtering is enforced across all means of accessing the cubes including dashboards, cubes, reports, and third-party applications.

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 IT Analytics Solution" on page 30.

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 IT Analytics Solution.

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 IT Analytics 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 92.

- 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 94.

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 IT Analytics Solution 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 91.

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

When you initially configure IT Analytics Solution, you selected either **Stored Credentials** or **Windows Integrated Authentication** to access Reporting Services.

See "Configuring IT Analytics Solution" on page 30.

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 90.

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 90.

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 91.

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.

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.

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.

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 90.

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 91.

See "About security" on page 76.

See "About SQL Server Analysis Services" on page 78.

See "About SQL Server Reporting Services" on page 83.

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.

   For more information, see the Microsoft knowledge base article *SQL Server 2008 Analysis Services and SQL Server 2005 Analysis Server to use Kerberos authentication* at the following URL:

   http://support.microsoft.com/kb/917409

   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.

Chapter 5

IT Analytics Solution packs

This chapter includes the following topics:

About IT Analytics Solution packs

IT Analytics Solution contains the following packs.

The following packs correspond to common Symantec licensing scenarios and functionality:

- IT Analytics Client and Server Management Pack
  See "About IT Analytics Client and Server Management Pack" on page 99.
- IT Analytics Symantec Endpoint Protection Pack
  See "About IT Analytics Symantec Endpoint Protection Pack" on page 100.
- IT Analytics ServiceDesk Pack
  See "About IT Analytics ServiceDesk Pack" on page 102.

About IT Analytics Client and Server Management Pack

This pack contains all of the core functionality of IT Analytics Solution for the configuration of cubes and reports.

See "About IT Analytics Solution packs" on page 99.

It also contains the cubes and the reports that are associated with the following cubes:

- **Add Remove Programs**
- **Application Metering**
- **Assets**
- **Computers**
- **ESX Servers**
- **Event Console Alerts**
- **IIS Servers**
- **Installed Files**
- **Installed Software**
- **Monitor Metrics**
- **Monitor NT Events**
- **Monitor Processes**
- **Package Distribution Events**
- **Package Server Configuration Events**
- **Package Server Status**
- **Patch Management**
- **Software Delivery Execution Events**
- **Software Delivery Package Events**
- **Software Delivery Status Events**
- **Software License Compliance**
- **Software Purchases**
- **SQL Servers**
- **Tasks**

About IT Analytics Symantec Endpoint Protection Pack

The cubes and reports in this pack use the configuration information of the Symantec Endpoint Protection Manager servers. The configuration information is captured when the SEP cubes are installed from the cube setup page. The information is used as the foundation of the data source views that are used to process the cubes. This functionality lets the Symantec Endpoint Protection cubes read data from the Configuration Management Database, as well as from each configured Symantec Endpoint Protection database. It also allows the data to come together into a single, unified view of all Symantec Endpoint Protection clients, alerts, and scan activity.

Before installing any cubes, ensure that the Symantec Endpoint Protection Server is fully configured. Full configuration is needed for each Symantec Endpoint Protection Manager that you want represented in the IT Analytics Symantec Endpoint Protection cubes.

This pack contains all of the core functionality of IT Analytics Solution for the configuration of cubes and reports.

See “About IT Analytics Solution packs” on page 99.

It also contains the cubes and reports that are associated with the following cubes:

- **SEP Access Rights**
- **SEP Agent Behavior Events**
- **SEP Agent Security Events**
- **SEP Agent System Events**
- **SEP Agent Traffic Events**
- **SEP Alerts**
- **SEP AntiVirus Policies**
- **SEP App and Device Control Policies**
- **SEP Clients**
- **SEP Exception Policies**
- **SEP Firewall Policies**
- **SEP Host Integrity Events**
- **SEP Host Integrity Policies**
- **SEP Insight Detections**
- **SEP Intrusion Prevention Policies**
- **SEP LiveUpdate Policies**
- **SEP Policies**
- **SEP Scans**

- **SEP Server Admin Events**
- **SEP Server System Events**
- **SEP SONAR Detections**

About IT Analytics ServiceDesk Pack

The cubes and reports in this pack use the configuration information of the ServiceDesk servers. The configuration information is captured when the ServiceDesk cubes are installed from the cube setup page. The information is used as the foundation of the data source views that are used to process the cubes. This functionality lets the ServiceDesk cubes read data from the ServiceDesk databases.

Before installing any cubes, ensure the ServiceDesk server is fully configured for the ServiceDesk instance that you want represented in the IT Analytics ServiceDesk cubes.

This pack contains all of the core functionality of IT Analytics Solution for configuration of cubes and reports. The pack also contains all of the cubes and reports that are associated with the following licensed cubes:

- **ServiceDesk Incidents**
- **ServiceDesk Problems**
- **ServiceDesk Changes**

See “About IT Analytics Solution packs” on page 99.

Appendix A

Cube reference

This appendix includes the following topics:

- Software Delivery Execution Events Cube
- Software Delivery Package Events Cube
- Software Delivery Status Events Cube
- Software License Compliance Cube
- Software Purchases Cube
- SQL Servers Cube
- SEP Access Rights Cube
- SEP Agent Behavior Events Cube
- SEP Agent Security Events Cube
- SEP Agent System Events Cube
- SEP Agent Traffic Events Cube
- SEP Alerts Cube
- SEP AntiVirus Policies Cube
- SEP App and Device Control Policies Cube
- SEP Clients Cube
- SEP Exception Policies Cube
- SEP Firewall Policies Cube
- SEP Host Integrity Events Cube
- SEP Host Integrity Policies Cube
- SEP Insight Detections Cube
- SEP Intrusion Prevention Policies Cube
- SEP LiveUpdate Policies Cube
- SEP Policies Cube
- SEP Scans Cube
- SEP Server Admin Events Cube
- SEP Server System Events Cube
- SEP SONAR Events Cube

- Tasks Cube

Application Metering Cube

`Application Metering Cube` – Contains data that is primarily associated with Altiris™ Inventory Solution from Symantec™. It represents a historical view of application execution.

Dimensions

- **Computer**
- **Date**
- **File**
- **Filter**
- **Software Component**
- **Organizational Group**
- **Software Product**
- **User**

Measures

`Computer Count`

The distinct number of computers.

`Denial Count`

The number of times that an application was denied execution.

`File Count`

The total number of files that matched the given criteria. If an application is in multiple locations on the same computer, this number can be larger than the Computer Count.

`Run Count`

The number of times that the application was executed.

`Total Run Time`

The amount of time that the application was running.

Key Performance Indicators

`Application Denials This Month`

The number of applications that were denied in the current month.

`Computers Metered This Month`

The number of computers that were metered in the current month.

Assets Cube

`Assets Cube` – Contains the information that is primarily associated with Asset Management Solution. It provides details about the ownership, status, location, and the type of asset that is intended to be used within the organization.

Dimensions

- **Asset**
- **Asset Status**
- **Asset Type**
- **Cost Center**
- **Department**
- **Location**
- **Organizational Group**
- **User**

Measures

`Asset Count`

The number of distinct assets of all types that are in the CMDB.

Key Performance Indicators

`Percent of Assets with Assigned Owners`

Percent of the assets that have an assigned owner.

`Percent of Assets with Assigned Cost Center`

Percent of the assets that have an assigned Cost Center.

`Percent of Assets with Assigned Location`

Percent of the assets that have an assigned Location.

Computers Cube

`Computers Cube` – Contains data that is primarily associated with Altiris™ Inventory Solution from Symantec™. It represents a current view of the information that the hardware and operating system scans that are stored in Symantec Management Platform collect.

Dimensions

- **Computer**
- **Created Date**
- **Filter**
- **Last Basic Inventory Date**
- **Logical Disk**
- **Organizational Group**
- **Processor**

Measures

`Computer Count`

The distinct count of computers.

`Logical Disk Free Space GB`

The sum of the available space on logical disks. The results are in Gigabytes.

`Logical Disk Count`

The count of logical disks. This number might be more than one per computer.

`Logical Disk Size GB`

The sum of the size of logical disks. The results are in Gigabytes.

`Physical Memory Capacity GB`

The sum of the physical memory capacity of the installed memory devices. The results are in Gigabytes.

`Physical Memory Device Count`

The count of physical memory devices that are installed. This number might be more than one per computer.

`Physical Memory Array Max Capacity GB`

The maximum capacity of memory that the physical memory arrays for a device support. This number is equal to or greater than the actual installed memory capacity that is represented in the **Physical Memory Capacity** measure. The results are in Gigabytes.

`Physical Memory Array Max Device Count`

The maximum number of devices that the physical memory arrays for a device support. This number is equal to or greater than the actual installed memory device count that is represented in the **Physical Memory Device Count** measure.

`Processor Speed GHz`

The maximum speed of a processor for a device or set of devices. The results are in gigahertz.

`Processor Count`

The count of processors for a device or set of devices.

Key Performance Indicators

`Percent of Computers Reporting Basic Inventory in Last 30 Days`

The percentage of the computers that have reported basic inventory in the last 30 days.

`New Computers in Last 30 Days`

The number of new computers in the last 30 days.

ESX Servers Cube

`ESX Servers Cube` – Contains the data about the virtual machines that are hosted on ESX Servers.

Dimensions

- **Computer**
- **Organizational Group**
- **Storage Volume**
- **Virtual Machine**

Measures

`Host Count`

The number of machines that host one or more virtual machines.

`Storage Volume Count`

The number of storage volumes.

`Virtual Machine Count`

The number of virtual machines by the selected criteria.

Event Console Alerts Cube

`Event Console Alerts Cube` – Contains the information about the alerts that are available within the Event Console. It represents a historical view of alerts and provides the ability to search for recurring issues or clients with problems.

Dimensions

- **Computer**
- **Date**
- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**
- **Filter**
- **Organizational Group**
- **Time**

Measures

`Action Count`

The number of actions that were launched.

`Alert Count`

The number of alerts that were triggered.

`Computer Count`

The distinct number of computers.

Key Performance Indicators

`Computers with Critical Alerts in Last 30 Days`

The number of computers with critical alerts in the last 30 days.

`Avg Alerts per Computer per Day in Last 30 Days`

The average number of alerts per computer per day in the last 30 days.

IIS Servers Cube

`IIS Servers Cube` – Contains the information about the configuration and settings of servers that host IIS.

Dimensions

- **Computer**
- **FTP Site**
- **Organizational Group**
- **Server**
- **Virtual Directory**
- **Web Site**

Measures

`FTP Site Count`

The distinct number of FTP sites.

`Server Count`

The number of identified servers.

`Virtual Directory Count`

The number of virtual directories.

`Web Site Count`

The number of individual Web sites that were found.

Installed Files Cube

`Installed Files Cube` – Contains data that is primarily associated with Altiris™ Inventory Solution from Symantec™. It represents a current view of the information that the Software Inventory that is stored in Symantec Management Platform collects.

Dimensions

- **Computer**
- **File**
- **File Modified Date**
- **Filter**
- **Organizational Group**
- **Software Component**
- **Software Product**

Measures

`Computer Count`

The distinct number of computers.

`File Count`

The total number of files that matched the given criteria. If a software component is in multiple locations on the same computer, this number can be larger than the Computer Count.

Installed Software Cube

`Installed Software Cube` – Contains data that is primarily associated with the Software Management Framework. It represents a current view of the information that is collected from the managed computers and stored in Symantec Management Platform.

Dimensions

- **Add Remove Programs**
- **Computer**
- **Filter**
- **Organizational Group**
- **Software Component**
- **Software Product**

Measures

`Computer Count`

The distinct number of computers.

`Instance Count`

The total number of times that a software component matched the given criteria. If a software component is in multiple locations on the same computer, this number can be larger than the Computer Count.

Monitor Metrics Cube

`Monitor Metrics Cube` – Contains the historical information regarding alerts, metrics, rules, and the tasks that Monitor Solution captures. Monitor Solution sets up the rules that can trigger alerts and the tasks that are based on a collected set of metrics. This cube provides insight into how these items work together to resolve issues on monitored clients.

Dimensions

- **Computer**
- **Date**
- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**
- **Event Console Monitor Rule**
- **Filter**
- **Monitor Metric**
- **Monitor Metric Detail Level**
- **Monitor Metric Instance**
- **Monitor Metric Source**
- **Monitor Task**
- **Organizational Group**
- **Task Server**
- **Time**

Measures

`Action Count`

The number of actions that were launched.

This measure group is not valid with the following dimensions:

- **Event Console Monitor Rule**
- **Monitor Metric**

- **Monitor Metric Detail Level**
- **Monitor Metric Instance**
- **Monitor Metric Source**
- **Monitor Task**
- **Task Server**

`Alert Count`

The number of alerts that were triggered.

This measure group is not valid with the following dimensions:

- **Event Console Alert Action Audit Type**
- **Monitor Metric**
- **Monitor Metric Detail Level**
- **Monitor Metric Instance**
- **Monitor Metric Source**
- **Monitor Task**
- **Task Server**

`Computer Count`

The distinct number of computers.

This measure group is not valid with the following dimensions:

- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**
- **Event Console Monitor Rule**
- **Monitor Task**
- **Task Server**

`Duration`

The amount of time (in seconds) that the given value was in effect for.

This measure group is not valid with the following dimensions:

- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**

- **Event Console Alert Severity**
- **Event Console Monitor Rule**
- **Monitor Task**
- **Task Server**

`Max`

The maximum value that was recorded for the given metric.

This measure group is not valid with the following dimensions:

- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**
- **Event Console Monitor Rule**
- **Monitor Task**
- **Task Server**

`Metric Count`

The number of metrics that were recorded.

This measure group is not valid with the following dimensions:

- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**
- **Event Console Monitor Rule**
- **Monitor Task**
- **Task Server**

`Min`

The minimum value that was recorded for the given metric.

This measure group is not valid with the following dimensions:

- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**

- **Event Console Monitor Rule**
- **Monitor Task**
- **Task Server**

`Task Count`

The number of tasks that were launched.

This measure group is not valid with the following dimensions:

- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**
- **Monitor Metric**
- **Monitor Metric Detail Level**
- **Monitor Metric Instance**
- **Monitor Metric Source**

`Avg`

The average value that was recorded for the given metric.

This measure group is not valid with the following dimensions:

- **Event Console Alert**
- **Event Console Alert Action Audit Type**
- **Event Console Alert Category**
- **Event Console Alert Severity**
- **Event Console Monitor Rule**
- **Monitor Task**
- **Task Server**

Key Performance Indicators

`Avg Percent Processor Time in Last 30 Days`

Average percent processor time in the last 30 days.

`Avg Percent Bandwidth Utilization in Last 30 Days`

Average percent bandwidth utilization in the last 30 days.

`Avg Percent Bandwidth Utilization in Last 30 Days`

Average percent disk time in the last 30 days.

`Avg Percent Memory Available in Last 30 Days`

Average percent memory available in the last 30 days.

Monitor NT Events Cube

`Monitor NT Events Cube` – Contains the Windows NT event log data that Monitor Solution captures. It represents a historical view of the Windows NT event log of all monitored client computers.

Dimensions

- **Category**
- **Computer**
- **Date**
- **Description**
- **Event ID**
- **Filter**
- **Log File**
- **Message DLL**
- **Organizational Group**
- **Rule Triggered**
- **Source**
- **Time**
- **Type**
- **User**

Measures

`Computer Count`

The distinct number of computers.

`Event Count`

The number of events.

Key Performance Indicators

`Computers with Error Events in Last 30 Days`

The number of computers with error events in the last 30 days.

`Avg Events per Computer per Day in Last 30 Days`

Average events per computer per day in the last 30 days.

Monitored Processes Cube

`Monitored Processes Cube` – Contains the Windows process data that Monitor Solution captures. It represents a historical view of the process data from all monitored client computers, including processor and virtual memory utilization.

Dimensions

- **Computer**
- **Date**
- **Filter**
- **Monitor Process Name**
- **Monitor Process Owner**
- **Organizational Group**
- **Time**

Measures

`Max Process CPU Percent Usage`

The maximum recorded percent of CPU utilization.

`Max Process CPU Time`

The maximum CPU time that was used for the given dimension.

`Max Process Handle Count`

The maximum handle count for the given dimension.

`Max Process Thread Count`

The maximum number of process threads.

`Max Process Virtual Memory Size`

The maximum virtual memory size that was consumed (in KB) for the given dimension.

`Max Process Working Set Size`

The maximum working set size (in KB) for the given dimension.

`Min Process CPU Percent Usage`

The minimum recorded percent of CPU utilization.

`Min Process CPU Time`

The minimum CPU time that was used for the given dimension.

`Min Process Handle Count`

The minimum handle count for the given dimension.

`Min Process Thread Count`

The minimum number of process threads.

`Min Process Virtual Memory Size`

The minimum virtual memory size for the given dimension.

`Min Process Working Set Size`

The minimum working set size for the given dimension.

`Process Count`

The count of processes.

`Process CPU Percent Usage`

The percent usage of a CPU for a given process.

`Avg Process CPU Percent Usage`

The average CPU percent utilization for the given dimension.

`Avg Process CPU Time`

The average process CPU time for the given dimension.

`Avg Process Handle Count`

The average process handle count for the given dimension.

`Avg Process Thread Count`

The average process thread count for the given dimension.

`Avg Process Virtual Memory Size`

The average process virtual memory size for the given dimension.

`Avg Process Working Set Size`

The average process working set size for the given dimension.

Package Distribution Events Cube

`Package Distribution Events Cube` – Contains the information regarding the actual distribution of packages to package servers. This information is valuable to verify that packages are properly transferred to the appropriate package server in a timely basis. It also provides details on the status of each transfer and the ability to view distribution events over time.

Dimensions

- **Organizational Group**
- **Package**
- **Package Distribution Event Date** (alias for Date Dimension)
- **Package Distribution Event Status**
- **Package Distribution Event Time** (alias for Time Dimension)
- **Package Server**

Measures

`Package Servers`

The number of package servers that host a package.

`Package Distribution Events`

The number of distribution events that were sent from the package server to Symantec Management Platform during package replication.

Package Server Configuration Events Cube

`Package Server Configuration Events Cube` – Contains the information regarding the configuration requests that the package servers generate. Package servers receive instructions from Symantec Management Platform using these configuration requests, and the requests are scheduled to occur at regular intervals. The information in this cube lets you verify the availability of each package server. It also lets you identify periods of time during which a package server did not communicate with Symantec Management Platform.

Dimensions

- **Organizational Group**
- **Package Server**
- **Configuration Request Date** (alias for Date Dimension)
- **Configuration Request Time** (alias for Time Dimension)

Measures

`Configuration Requests`

The number of configuration requests that were sent between the package servers and Symantec Management Platform. This measure can be used to determine package server availability.

`Package Servers`

The number of package servers on which matching events occurred.

Package Server Status Cube

`Package Server Status Cube` – Represents the current state of the package server infrastructure. This information includes the measures and dimensions that provide clarity into the associations between package servers and packages. It also includes the status of each package on each package server.

Dimensions

- **Organizational Group**
- **Package Server**
- **Package**
- **Package Status**

Measures

`Disk Space Used Bytes GB`

The amount of disk space that is used to host the package.

`Package Servers`

The number of package servers.

Key Performance Indicators

`Package Servers with Invalid Packages`

The number of package servers currently hosting invalid packages.

Patch Management Cube

`Patch Management Cube` – Contains data that is primarily associated with Patch Management Solution. It represents the current state of the Patch Management Inventory scan information for Symantec Management Platform.

Dimensions

- **Computer**
- **Filter**
- **Organizational Group**
- **Software Update**
- **Software Update Release Date**

Measures

`Applicable Computer Count`

The number of computers that meet the requirements for a patch by the given criteria.

`Applicable Patch Count`

The number of patches that match the given criteria.

`Installed Computer Count`

The number of computers that have patches installed that match the given criteria.

`Installed Patch Count`

The number of patches that are installed that match the given criteria.

`Vulnerability Count`

The number of patches that are required for the given criteria.

`Vulnerable Computer Count`

The number of computers that require a patch to match the given criteria.

Key Performance Indicators

`Computers Requiring Critical Patches`

The number of computers that require a critical patch.

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

- **Assigned to User**
- **Change**
- **Contact Type**
- **Date Closed**
- **Date Ended**
- **Date Implemented**
- **Date Opened**
- **Date Scheduled**
- **Date Started**
- **Impact**
- **Location**
- **Organizational Group**
- **Priority**
- **Reference**
- **Source**
- **Status**
- **Time Closed**
- **Time Ended**
- **Time Implemented**
- **Time Needed**
- **Time Opened**
- **Time Scheduled**
- **Time Started**
- **Type**

- **Urgency**
- **User**

Measures

`Change Count`

The number of changes.

`Failed Changes`

The number of changes that failed.

`Rejected Changes`

The number of changes that were rejected.

`Unplanned Changes`

The number of changes that were unplanned.

`Change Assignment Count`

The number of assigned users.

`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 Resolve`

The number of days it takes to resolve the change.

`Avg Hours to Resolve`

The number of hours it takes to resolve the change.

`Avg Minutes to Resolve`

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 User**
- **Category**
- **Close Code**
- **Contact Type**
- **Created by User**
- **Date Closed**
- **Date Modified**
- **Date Opened**
- **Impact**
- **Incident**
- **Last Modified by User**
- **Location**
- **Priority**
- **Reference**
- **Resolved by User**
- **Source**
- **Status**
- **Time Closed**
- **Time Modified**
- **Time Opened**
- **Type**
- **Urgency**
- **User**

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 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 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 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.

`Avg Survey Score`

The average survey score. This measure is valid for all incidents that have a status of Resolved or Closed.

`Entered Thru Self Service Count`

The number of incidents that were entered through self service.

`Escalated Count`

The number of incidents that were escalated.

`Escalated More Than Once Count`

The number of incidents that were escalated more than once.

`Escalated Once Count`

The number of incidents that were escalated one time.

`Escalated Zero Count`

The number of incidents that were not escalated.

`Exceeded SLA Count`

The number of incidents that exceeded the defined SLA.

`Exceeded Warn Count`

The number of incidents that exceeded the Warn time that the SLA defines.

`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 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.

`Incident Assignment Count`

The number of users and groups that are assigned to an incident. An incident can have more than one person assigned to it. This measure is useful for determining the number of users that are assigned to a given incident.

`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**
- **Contact Type**
- **Date Closed**
- **Date Due**
- **Date Implemented**
- **Date Opened**
- **Date Resolved**
- **Impact**
- **Location**
- **Priority**
- **Problem**
- **Reference**
- **Source**
- **Status**
- **Time Closed**
- **Time Due**
- **Time Implemented**
- **Time Opened**
- **Time Resolved**
- **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 Resolve`

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

`Avg Hours Spent`

The average number of hours spent.

`Avg Hours To Resolve`

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

`Avg Minutes Spent`

The average number of minutes spent.

`Avg Minutes To Resolve`

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

`Avg Percent Complete`

The average percentage that is complete.

`Exceeded SLA Count`

The number of problems that exceeded the defined SLA.

`Exceeded Warn Count`

The number of problems that exceeded the Warn time that the SLA defines.

`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.

Software Delivery Execution Events Cube

`Software Delivery Execution Events Cube` – Contains the information regarding the execution of the programs that are associated with Software Delivery Advertisements on Symantec managed computers. This information is valuable to ensure that advertisements are running as expected. It also helps to easily identify areas of concern based on event status and trending of when execution events have occurred over time.

Dimensions

- **Advertisement** (alias for Software Delivery Advertisement)
- **Event Status** (alias for Software Delivery Execution Event Status)
- **Command Line** (alias for Software Delivery Execution Event Command Line)
- **Computer**
- **Event Date** (alias for Date Dimension)
- **Event Time** (alias for Time Dimension)
- **Filter**
- **Organizational Group**
- **Package**

Measures

`Avg Duration In Seconds`

The average number of seconds that it took to complete execution.

`Events`

The number of events that were sent from the Symantec Management Agent to Symantec Management Platform.

`Computer Count`

The distinct number of computers.

Key Performance Indicators

`Unsuccessful Software Execution Events in Last 30 Days.`

The number of unsuccessful software execution events in the last 30 days.

`Computers with Unsuccessful Software Execution Events in Last 30 Days`

The number of computers with unsuccessful software execution events in the last 30 days.

`Successful Software Execution Events in Last 30 Days`

The number of successful software execution events in the last 30 days.

Software Delivery Package Events Cube

`Software Delivery Package Events Cube` – Contains the information regarding the download of packages to Symantec managed computers. This information includes the method location and the source location for each download. It also includes status information and the date and time of each package download. The information in this cube is valuable to determine where client computers download the packages from. By reviewing this information, you can ensure that the behavior is consistent with expectations. You can also easily spot trends in package downloads over time or quickly identify issues with the software delivery process.

Dimensions

- **Computer**
- **Download Method** (alias for Package Download Method)
- **Download Source** (alias for Package Download Source)
- **Download URL** (alias for Package Download URL)
- **Event Date** (alias for Date Dimension)
- **Event End Status** (alias for Software Delivery Package Event Status)
- **Event Start Status** (alias for Software Delivery Package Event Status)
- **Event Time** (alias for Event Time)
- **Filter**
- **Organizational Group**
- **Package**

Measures

`Avg Bytes Transferred`

The average number of bytes that were transferred between the package source and the Symantec Management Agent.

`Avg Duration In Seconds`

The average duration in seconds for the Symantec Management Agent to download packages.

`Computer Count`

The distinct number of computers.

`Events`

The number of events that were sent during the download of packages.

`Total Bytes Transferred`

The total number of bytes that were transferred during the download of packages.

Key Performance Indicators

`Computers with Unsuccessful Software Downloads in Last 30 Days`

The number of computers that have had unsuccessful software downloads in the last 30 days.

`Unsuccessful Downloads in Last 30 days`

The number of unsuccessful downloads in the last 30 days.

Software Delivery Status Events Cube

`Software Delivery Status Events Cube` – Contains the information about the status of Advertisements as they relate to Symantec managed computers. This information is valuable to verify that client computers receive Advertisements as expected.

Dimensions

- **Advertisement** (alias for Software Delivery Advertisement)
- **Computer**
- **Event Date** (alias for Date Dimension)
- **Event Status** (alias for Software Delivery Status Event Status)
- **Event Time** (alias for Time Dimension)
- **Event Type** (alias for Software Delivery Status Event Type)
- **Filter**
- **Organizational Group**
- **Package**

Measures

`Events`

The number of events that the Symantec Management Agents sent.

`Computer Count`

The distinct number of computers.

Software License Compliance Cube

`Software License Compliance Cube` – Contains and relates contract data from Asset Management Inventory and Application Metering Solutions. Software purchase and inventory data is associated with licenses using automated search rules.

Dimensions

- **Asset**
- **Cost Center**
- **Department**
- **Evaluation Date**
- **Location**
- **Organizational Group**
- **Software License**
- **Software Product**

Measures

`Installed`

The number of installed copies of a particular software application.

`In Use`

The usage count for the software from Application Metering.

`Owned`

The total number of all software purchases that match the software license.

`Peak Inventoried Install Count`

The largest number of installs that were recorded for a given period. For example, a license for a given Month period shows a count of 20. The count of 20 means that during that month, 20 was the largest number of installs that were recorded.

`Period Closing Inventoried Install Count`

The number of installs that were recorded at the closing of a given period. For example, the count may show as many as 20 installs for a given period. At the end of that period, if only 10 were installed, this count would then show 10.

`Metered Usage Count`

Count of machines using given software.

`Borrowed License Count`

Number of licenses borrowed.

`Donated License Count`

Number of licenses donated.

`Non-Inventoried Install Count`

Number of non-inventoried licenses.

`Purchased License Count`

Number of licenses purchased.

`Total Install Count`

This is the Period Closing Inventoried Install Count + Non Inventoried Install Count.

`Total License Count`

This is the Purchased License Count - Donated License Count + Borrowed License Count.

`Compliance`

Number of licenses available for use, and is calculated as Total License Count - Total Install Count.

Key Performance Indicators

`Software Licenses Out of Compliance`

The number of software licenses currently out of compliance.

Software Purchases Cube

`Software Purchases Cube` – Contains contract data from Asset Management Solution. This cube provides data regarding all software purchase records within the CMDB and allows the data to be associated with organizational units and software licenses.

Dimensions

- **Cost Center**
- **Date**
- **Department**
- **Location**
- **Software License**
- **Software Purchase**
- **User**

Measures

`Purchase Quantity`

The total number of all purchases for a particular software application.

Key Performance Indicators

`Software Purchases Added in Last 90 Days`

The number of software purchases that have been added in the last 90 days.

SQL Servers Cube

`SQL Servers Cube` – Contains the data regarding the operating SQL servers in the environment.

Dimensions

- **Computer**
- **Organizational Group**
- **SQL Cluster**
- **SQL Cluster Resource**
- **SQL Database**
- **SQL Database Creation Date**
- **SQL Database System**
- **SQL Storage Area**
- **SQL User**

Measures

`Cluster Resource Count`

The number of cluster resources.

`Cluster Count`

The number of clusters.

`Database System Count`

The number of database systems.

`Database Count`

The number of databases.

`Storage Area Count`

The number of storage areas.

`User Count`

The number of SQL users.

Key Performance Indicators

`SQL Server Databases Created in Last 30 Days`

The number of SQL server databases that have been created in the last 30 days.

SEP Access Rights Cube

`SEP Access Rights Cube` – Provides the data about the rights a given user has at the group or the computer level. This cube is useful in understanding the rights users have access to specific groups and computers. It is also useful in understanding the level of access each user has (Read, Full, or None).

Dimensions

- **Administrator Count**
- **Computer Rights**
- **Group Rights**

Measures

`Administrator Count`

The number of administrators.

`Computer Rights`

The number of rights that are assigned to computers. For a given user, a computer can have one of three rights: Read, Full, or No Access.

`Group Rights`

The number of rights that a group has.

SEP Agent Behavior Events Cube

`SEP Agent Behavior Events Cube` – Contains the information about the Agent Behavior Events that the computers with the Symantec Endpoint Protection client generated. Information specific to this cube includes the total number of events, how many computers generated events, and details of those behavior events.

Dimensions

- **Agent Behavior Event**
- **Domain**
- **Site**
- **Server**
- **Group**
- **Computer**
- **Event Date**

Measures

`Event Count`

The number of events.

`Computer Count`

The number of computers.

SEP Agent Security Events Cube

`SEP Agent Security Events Cube` – Contains the information about the Agent Security Events that the computers with the Symantec Endpoint Protection client generated. Information specific to this cube includes the total number of events, how many computers generated events, and details of those security events.

Dimensions

- **Agent Security Event**
- **Domain**
- **Site**
- **Server**
- **Group**
- **Computer**
- **Client**
- **Event Date**
- **IPS Detection Event**

Measures

`Event Count`

The number of events.

`Computer Count`

The number of computers.

Key Performance Indicators

`Number of IPS Detections in Last 30 Days`

The number of IPS detection events in the last 30 days.

SEP Agent System Events Cube

`SEP Agent System Events Cube` – Contains the information about the Agent System Events that the computers with the Symantec Endpoint Protection client generated. Information specific to this cube includes the total number of events, how many computers generated events, and details of those system events.

Dimensions

- **Agent System Event**
- **Domain**
- **Site**
- **Server**
- **Group**
- **Computer**
- **Event Date**

Measures

`Event Count`

The number of events.

`Computer Count`

The number of computers.

SEP Agent Traffic Events Cube

`SEP Agent Traffic Events Cube` – Contains the information about the Agent Traffic Events that the computers with the Symantec Endpoint Protection client generated. Information specific to this cube includes the total number of events, how many computers generated events, and details of those traffic events.

Dimensions

- **Agent Traffic Event**
- **Domain**
- **Site**
- **Server**
- **Group**
- **Computer**
- **Event Date**

Measures

`Event Count`

The number of events.

`Computer Count`

The number of computers.

SEP Alerts Cube

`SEP Alerts Cube` – Contains the information about the alerts that the computers with the Symantec Endpoint Protection client generated. The information that is specific to this cube includes: total number of alerts, how many computers generated alerts, actions taken, categorization, and details of the viruses and risks that caused the alerts to be generated.

Dimensions

- **Alert**
- **Alert Date**
- **Computer**
- **Domain**
- **Group**
- **Server**
- **Site**
- **Virus**

Measures

`Alerts`

The number of alerts that match the given criteria.

`Computers`

The number of computers that match the given criteria.

`Viruses`

The number of viruses that match the given criteria.

`Still Infected`

The number of systems that are still infected that match the given criteria.

`Blocked`

The number of viruses that were blocked that match the given criteria.

`Cleaned`

The number of viruses that were cleaned that match the given criteria.

`Deleted`

The number of viruses that were deleted that match the given criteria.

`Quarantined`

The number of viruses that were quarantined that match the given criteria.

`Suspicious`

The number of suspicious viruses that were detected that match the given criteria.

Key Performance Indicators

`Percent of Virus Infections Cleaned`

The percentage of virus infections that have been cleaned in the last 30 days.

`Number of Alerts in Last 30 Days`

The number of alerts in the last 30 days.

SEP AntiVirus Policies Cube

`SEP AntiVirus Policies Cube` – Contains the information that provides insight into the AntiVirus policies, which can be applied to groups and/or machines.

Dimensions

- **Computer**
- **Client**
- **AntiVirus Policy**
- **Domain**
- **Group**
- **Last Checkin Date**
- **Location**
- **Server**
- **Site**
- **Virus Definition**
- **Download Advisor**
- **Global Scan Options**
- **Mac Auto Protect**
- **Mac Miscellaneous**
- **Sonar Settings**
- **Windows Auto Protect**
- **Windows Miscellaneous**
- **Mac Admin Defined Scans**
- **Mac Admin Defined Common**
- **Windows Admin Defined Scans**
- **Windows Admin Defined Advanced**

Measures

`Computer Count`

The number of computers.

`Group Count`

The number of groups.

SEP App and Device Control Policies Cube

`SEP App and Device Control Policies Cube` – Contains the information that provides insight into the Application and Device Control policies which can be applied to groups and/or machines.

Dimensions

- **Client**
- **Computer**
- **Domain**
- **Group**
- **Last Checkin Date**
- **Location**
- **Server**
- **Site**
- **Virus Definition**
- **Blocked Device**
- **Excluded Device**
- **Application and Device Control Policy**
- **Application and Device Control Rule**

Measures

`Computer Count`

The number of computers.

`Group Count`

The number of groups.

SEP Clients Cube

`SEP Clients Cube` – Contains the information about computers with the Symantec Endpoint Protection client. Information unique to this cube includes virus definition information and client settings. It also contains several important date elements that are meaningful when you manage the deployment and maintenance of Symantec Endpoint Protection clients.

Dimensions

- **Client**
- **Computer**
- **Creation Date**
- **Domain**
- **Group**
- **Intrusion Prevention Signature**
- **Last Checkin Date**
- **Last Scan Date**
- **Last Virus Date**
- **Server**
- **Site**
- **Virus Definition**

Measures

`Client Count`

The number of Symantec Endpoint Protection clients that match the given criteria.

Key Performance Indicators

`Percent of Clients with Virus Infection`

The percentage of clients with a virus infection in the last 30 days.

`Percent of Clients with Scan Completed in Last 30 Days`

The percentage of the clients that have completed a scan in the last 30 days.

SEP Exception Policies Cube

`SEP Exception Policies Cube` – Contains the information that provides insight into the Exception policies which can be applied to groups and/or machines.

Dimensions

- **Computer**
- **Location**
- **Client**
- **Last Checkin Date**
- **Server**
- **Domain**
- **Group**
- **Virus Definition**
- **Site**
- **Client Restrictions**
- **Exception Item**
- **Exception Policy**

Measures

`Computer Count`

The number of computers.

`Group Count`

The number of groups.

SEP Firewall Policies Cube

`SEP Firewall Policies Cube` – Contains the information that provides insight into the Firewall policies which can be applied to groups and/or machines.

Dimensions

- **Client**
- **Computer**
- **Domain**
- **Firewall Policy**
- **Group**
- **Last Checkin Date**
- **Location**
- **Server**
- **Site**
- **Virus Definition**
- **Firewall Policy Rule**
- **Security Settings**

Measures

`Computer Count`

The number of computers.

`Group Count`

The number of groups.

`Rule Count`

The number of firewall rules.

SEP Host Integrity Events Cube

`SEP Host Integrity Events Cube` – Contains the information about the Host Integrity Events that the computers with the Symantec Endpoint Protection client generated. The information that is specific to this cube includes: total number of Host Integrity events and the breakdown of pass vs. failure of those events, total number of checks and the breakdown of pass vs. failure for those checks, how many computers generated events, and details of the events.

Dimensions

- **Client**
- **Computer**
- **Domain**
- **Event Date**
- **Group**
- **Server**
- **Site**
- **Host Integrity Check**
- **Host Integrity Event**

Measures

`Checks Failed`

The number of Host Integrity checks that failed.

`Checks Passed`

The number of groups.

`Host Integrity Check Count`

Total number of Host Integrity checks.

`Passed Count`

The number of Host Integrity policies passed.

`Failed Count`

The number of Host Integrity policies failed.

`Event Count`

The number of Host Integrity events.

`Computer Count`

The number of computers.

Key Performance Indicators

`Percent of Host Integrity Checks Failed in Last 30 Days`

The number of Host Integrity checks that failed in the last 30 days.

SEP Host Integrity Policies Cube

`SEP Host Integrity Policies Cube` – Contains the information that provides insight into the Host Integrity policies which can be applied to groups and/or machines.

Dimensions

- **Client**
- **Computer**
- **Domain**
- **Group**
- **Last Checkin Date**
- **Location**
- **Server**
- **Site**
- **Virus Definition**
- **Host Integrity Policy**
- **Advanced**
- **Requirement**

Measures

`Computer Count`

The number of computers that are subject to the policies.

`Group Count`

The number of groups.

SEP Insight Detections Cube

`SEP Insight Detections Cube` – Contains the information about the Insight Detections that the computers with the Symantec Endpoint Protection client generated. The information that is specific to this cube includes: total number of detections, how many computers generated detections, the number of risks detected, and details of the detections and risks that caused the event to be generated.

Dimensions

- **Alert**
- **Alert Date**
- **Computer**
- **Domain**
- **Group**
- **Insight Detection**
- **Location**
- **Server**
- **Site**
- **Virus**

Measures

`Computer Count`

The number of computers that are subject to the policies.

`Detection Count`

The number of detections.

`Risk Count`

The number of risks.

Key Performance Indicators

`Number of Insight Detections in Last 30 Days`

The number of Insight detections in the last 30 days.

`Percent of Insight Detections Permitted by User in Last 30 Days`

The number of Insight Detections that were permitted by users in the last 30 days.

SEP Intrusion Prevention Policies Cube

`SEP Intrusion Prevention Policies Cube` – Contains the information that provides insight into the Intrusion Prevention policies which can be applied to groups and/or machines.

Dimensions

- **Client**
- **Computer**
- **Domain**
- **Group**
- **Last Checkin Date**
- **Location**
- **Server**
- **Site**
- **Virus Definition**
- **Intrusion Prevention Policy**

Measures

`Computer Count`

The number of computers that are subject to the policies.

`Group Count`

The number of groups.

SEP LiveUpdate Policies Cube

`SEP LiveUpdate Policies Cube` – Contains the information that provides insight into the LiveUpdate policies which can be applied to groups and/or machines.

Dimensions

- **Client**
- **Computer**
- **Domain**
- **Group**
- **Last Checkin Date**
- **Location**
- **Server**
- **Site**
- **Virus Definition**
- **LiveUpdate Policy**
- **Mac Advanced**
- **Mac Schedule**
- **Mac Server Settings**
- **Proxy Settings**
- **Windows Advanced**
- **Windows Schedule**
- **Windows Server Settings**

Measures

`Computer Count`

The number of computers that are subject to the policies.

`Group Count`

The number of groups.

SEP Policies Cube

`SEP Policies Cube` – Contains the information that provides insight into the various Symantec Endpoint Protection policies which can be applied to groups and/or machines.

Dimensions

- **Computer**
- **Virus Definition**
- **Domain**
- **Group**
- **Server**
- **Site**
- **Client**
- **Last Checkin Date**
- **Policy**
- **Location**

Measures

`Computer Count`

The number of computers that are subject to the policies.

`Group Count`

The number of groups.

SEP Scans Cube

`SEP Scans Cube` – Contains the information about the actual scans that were performed on computers with the Symantec Endpoint Protection client. The information that is specific to this cube includes: total number of scans performed, how many computers were scanned, how many infections and threats the scans detected, total number of files scanned, the files that were omitted from the scans, and the duration of the scans.

Dimensions

- **Client**
- **Computer**
- **Domain**
- **Group**
- **Scan Start Date**
- **Server**
- **Site**
- **Status**

Measures

`Computers`

The total number of computers that were scanned that match the given criteria.

`Duration`

The total duration to complete a scan that matched the given criteria.

`Infected`

The total number of infections that were detected that matched the given criteria.

`Omitted`

The total number of files that were omitted from the scans that matched the given criteria.

`Scans`

The total number of scans that were performed that matched the given criteria.

`Threats`

The total number of threats that were detected that matched the given criteria.

`Total Files`

The total number of files that were scanned that matched the given criteria.

Key Performance Indicators

`Percent of Scans Cancelled in Last 30 Days`

The percentage of the scans that have been canceled in the last 30 days.

SEP Server Admin Events Cube

`SEP Server Admin Events Cube` – Contains the information about the Server Admin Events that the Symantec Endpoint Protection Managers generated. Information specific to this cube includes the total number of events and details of those events.

Dimensions

- **Server Admin Event**
- **Domain**
- **Site**
- **Server**
- **Event Date**

Measures

`Event Count`

The number of events.

SEP Server System Events Cube

`SEP Server System Events Cube` – Contains the information about the Server System Events that the Symantec Endpoint Protection Managers generated. Information specific to this cube includes the total number of events and details of those events.

Dimensions

- **Server System Event**
- **Domain**
- **Site**
- **Server**
- **Event Date**

Measures

`Event Count`

The number of events.

SEP SONAR Events Cube

`SEP SONAR Events Cube` – Contains the information about the SONAR Detections that the computers with the Symantec Endpoint Protection client generated. The information that is specific to this cube includes: total number of detections, how many computers generated detections, the number of risks detected, and details of the detections and risks that caused the event to be generated.

Dimensions

- **Alert**
- **Alert Date**
- **Computer**
- **Domain**
- **Group**
- **Server**
- **Site**
- **SONAR Detection**
- **Virus**

Measures

`Detection Count`

The number of detections.

`Risk Count`

The number of risks.

`Computer Count`

The number of computers.

Key Performance Indicators

`Number of High Sensitivity SONAR Detections in Last 30 Days`

The number of SONAR detections in the last 30 days that have a high sensitivity.

`Percent of SONAR Risks Confirmed in Last 30 Days`

The number of SONAR Detections in the last 30 days where the detection type is Confirmed Risk.

Tasks Cube

`Tasks Cube` – Contains the historical information regarding the tasks that Symantec Management Platform, site servers, or managed client computers performed.

Dimensions

- **Computer**
- **Event Date**
- **Event Time**
- **Filter**
- **Organizational Group**
- **Parent Task**
- **Task**
- **Task End Date**
- **Task End Time**
- **Task Server**
- **Task Start Date**
- **Task Start Time**

Measures

`Computer Count`

The distinct number of computers.

`Task Count`

The distinct number of tasks.

Key Performance Indicators

`Percent of Task Successful in Last 30 Days`

Percent of successful tasks in the last 30 days.

`Avg Tasks per Computer in Last 30 Days`

The average tasks per computer in the last 30 days.

Dashboard reference

This appendix includes the following topics:

- Symantec Management Agent Dashboard
- Asset Control Dashboard
- Computer Inventory Dashboard
- Event Console Alerts Dashboard
- IT Analytics Usage Dashboard
- Monitor Alerts Dashboard
- Patch Management Dashboard
- ServiceDesk Change Trend Dashboard
- ServiceDesk Incident Trend Dashboard
- ServiceDesk Problem Trend Dashboard
- Software Compliance Dashboard
- Software Delivery Dashboard
- Software Installs Dashboard
- Symantec Endpoint Protection Client Dashboard
- Symantec Endpoint Protection Host Integrity Event Dashboard
- Symantec Endpoint Protection Insight Detection Dashboard
- Symantec Endpoint Protection IPS Detection Event Dashboard
- Symantec Endpoint Protection Risk Dashboard

- Symantec Endpoint Protection SONAR Detection Dashboard
- Vista Readiness Dashboard
- Windows 7 Readiness Dashboard

Symantec Management Agent Dashboard

Displays a graphical representation of basic inventory age, a count of received solution inventory and received application metering summary information for all Symantec Management Agents.

Asset Control Dashboard

Displays a graphical representation of computers by asset status and in-stock assets by type.

It also contains the pie charts that represent the ratios of assets with and without their assigned owners, locations, cost centers, and departments.

Computer Inventory Dashboard

Displays a graphical representation of the operating system, manufacturer, and domain breakdown of computers. It also includes the top five operating systems.

Event Console Alerts Dashboard

Displays a graphical representation of Event Console Alerts by category and severity level. It also includes the top event console messages.

IT Analytics Usage Dashboard

Provides a high-level summary of IT Analytics usage over time. It also includes the top users, top cubes, and top reports.

Monitor Alerts Dashboard

Displays a graphical representation of Monitor Alerts by category and severity level. It also includes the most active rules that generated alerts.

Patch Management Dashboard

Displays a graphical representation of patch risk level and vulnerable computers by severity.

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 resolve, 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 resolve
- 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 hours since modified, average hours to resolve, and average survey score.

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**, **category**, **impact**, **priority**, **urgency**, 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 resolve, 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 resolve
- 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**.

Software Compliance Dashboard

Provides a high-level overview of the software compliance in an organization. It contains a chart that displays the current breakdown of compliance, as well as a trend that shows the overall compliance over time.

Software Delivery Dashboard

Provides a high-level overview of the top software advertisements by execution status.

This report filters by **data range**, **filter**, and **organizational group**.

Software Installs Dashboard

Provides a breakdown of the top five software titles, top Microsoft Office editions, and top five Adobe installations.

This report filters by **filter** and **organizational group**.

Symantec Endpoint Protection Client Dashboard

Displays a graphical representation of the current Symantec Endpoint Protection clients that are in the environment. Specific charts also include the following information:

- Client version, virus definition version
- Intrusion prevention signatures
- The number of days since clients last connected to the Endpoint Protection Manager

Symantec Endpoint Protection Host Integrity Event Dashboard

Displays a graphical representation of the Top five Host Integrity rules that have had failed checks. It also contains the Host Integrity checks broken down by Rule Type and Location.

Symantec Endpoint Protection Insight Detection Dashboard

Displays a graphical representation of the following information:

- Top five detections that users allowed
- Top five detections by broken down by the reason for the detection
- Top download detections by user
- The top download detections by web domain

Symantec Endpoint Protection IPS Detection Event Dashboard

Displays a graphical representation that includes the following information:

- Top five IPS detection events by application name
- Top five IPS detection events by group
- Top five IPS detection events by location
- Top five IPS detection events by user

Symantec Endpoint Protection Risk Dashboard

Displays a graphical representation of the threat types and specific virus names. It also contains the remediation actions that the Symantec Endpoint Protection clients have taken over a period of time.

Symantec Endpoint Protection SONAR Detection Dashboard

Displays a graphical representation of the top applications that SONAR detected, the top detections by type, and the top download detections by sensitivity.

Vista Readiness Dashboard

Displays a graphical representation of memory, disk space, and processor readiness. It also includes a readiness summary and a requirement segmentation summary breakdown of all computers that are based on minimum requirements for Microsoft Vista.

Windows 7 Readiness Dashboard

Displays a graphical representation of memory, disk space, and processor readiness. It also includes a readiness summary and a requirement segmentation summary breakdown of all computers that are based on minimum requirements for Microsoft Windows 7.

Appendix C

Report reference

This appendix includes the following topics:

- Computers by Operating System report
- Computers by System Type report
- Event Console Alert Details report
- Event Console Alerts Trend report
- Host Integrity Event Details report
- Insight Detection Details report
- Installed Files by File Name report
- Installed Files Search report
- Intrusion Prevention Detection Details report
- Intrusion Prevention Detection Trend report
- Intrusion Prevention Signature Details report
- IT Analytics Configuration Events report
- IT Analytics Usage Events report
- Microsoft Server Applications report
- Microsoft Software Installs report
- Monitor Alert Details report
- Monitor Metrics CPU Utilization Trend report
- Monitor Metrics Disk Utilization Trend report
- Monitor Metrics Network Utilization Trend report
- Monitor Metrics Trend report
- Monitored Processes CPU Utilization Trend report
- Package Download Event Summary report
- Package Server Availability - Monthly report
- Package Server Availability - Daily report
- Patch Management Bulletin Summary report
- Patch Management Details report
- Patch Vulnerability report

- Patch Vulnerability Search report
- Scan Trend report
- Servers by Type and Version report
- ServiceDesk Change Search report
- ServiceDesk Changes by Assigned to User report
- ServiceDesk Changes by Impact report
- ServiceDesk Changes by Priority report
- ServiceDesk Changes by Status report
- ServiceDesk Changes by Type report
- ServiceDesk Changes by Urgency report
- ServiceDesk Incident Search report
- ServiceDesk Incidents by Assigned to User report
- ServiceDesk Incidents by Category report
- ServiceDesk Incidents by Impact report
- ServiceDesk Incidents by Priority report
- ServiceDesk Incidents by Status report
- ServiceDesk Incidents by Type report
- ServiceDesk Incidents by Urgency report
- ServiceDesk Problem Search report
- ServiceDesk Problems by Assigned to User report
- ServiceDesk Problems by Category report
- ServiceDesk Problems by Impact report
- ServiceDesk Problems by Priority report
- ServiceDesk Problems by Status report
- ServiceDesk Problems by Urgency report
- Software Delivery Search report
- Software License Compliance by Cost Center report

- Software License Compliance by Department report
- Software License Compliance by Location report
- Software License Trend report
- SONAR Detection Details report
- Top 10 Applications Consuming CPU report
- Top 10 Applications Consuming Memory report
- Top 10 Users Consuming CPU report
- Virus Alert Details report
- Virus Alert Trend report
- Virus Definition Distribution Details report
- Vista Readiness Details report
- Windows 7 Readiness Details report

Add Remove Programs by Name report

Displays the publisher and the program name of all of the programs that the Software Management Framework detected. The Software Management Framework detects the programs as they are defined in the Add Remove Programs registry. It also includes a count of computers where each item was detected.

This report lets users define a publisher and a program name to filter the results with.

Add Remove Programs Search report

Displays the publisher, program name, and computer name for each distinct program and computer that the Software Management Framework detected. The Software Management Framework detects the programs in the Add Remove Programs registry.

This report lets users define a publisher and a program name to filter the results with.

Advertisement Execution Event Summary report

Contains the information from the Software Delivery Execution Event Cube. It includes a graphical trend of advertisement execution events over time.

This report also includes a summary of the number of events, computers, packages, average duration in seconds per advertisement, and event status.

Alert and Task Details report

Displays an hourly summary of tasks that are related to Monitor Alerts and Monitor Solution for the specified computer.

Application Metering by File Name report

Displays a file name with a breakdown by year, quarter, and month. It also includes a computer count and run count, as detected by Application Metering Solution.

This report lets users define a file name and product name to filter the results with.

Application Metering Search report

Displays the file name, product name, computer name, and run count for each file that Application Metering Solution detected.

The report lets users define a month and a year date range, file name, and product name to filter the results with.

Asset Search report

Displays the asset name, serial number, system number, asset type, asset status, cost center, department, location, manufacturer, model, and owner.

The report lets users filter the results by any of these fields.

Assets by Asset Type report

Displays the asset type, along with counts of each asset status.

The report lets users filter the results by asset type, asset status, department, cost center, and location.

Assets by Cost Center report

Displays the asset type by cost center, along with counts of each asset status.

The report lets users filter the results by asset type, asset status, department, cost center, and location.

Assets by Department report

Displays the asset type by department, along with counts of each asset status.

The report lets users filter the results by asset type, asset status, department, cost center, and location.

Assets by Location report

Displays the asset type by location, along with counts of each asset status.

The report lets users filter the results by asset type, asset status, department, cost center, and location.

Assets by Model report

Displays the asset models by manufacturer, along with counts of each asset status.

The report lets users filter the results by asset type, asset status, department, cost center, and location.

Client Version Details report

Displays the details of the Symantec Endpoint Protection client versions that are in the environment.

Computer Search report

Displays a summary of computer hardware and OS inventory as detected by Inventory Solution.

The report allows users to filter the results by computer name, manufacturer, and model.

Computers by CPU report

Displays a count of computers by CPU type, speed, and count.

Computers by Domain report

Displays a count of computers by domain.

Computers by Manufacturer report

Displays a count of computers by manufacturer and model.

Computers by Memory report

Displays a count of computers by total physical memory in megabytes.

Computers by Operating System report

Displays a count of computers by OS name and version.

Computers by System Type report

Displays a count of computers by system type (platform).

Event Console Alert Details report

Displays a summary of Event Console Alerts.

Event Console Alerts Trend report

Displays a count of critical, warning, major, informational, normal, undetermined, and by value alerts over time. These counts are displayed in table format along with a graphical trend of alerts for a designated period of time.

Host Integrity Event Details report

Displays the details of the Host Integrity events. Symantec Endpoint Protection clients generate these events over a designated period of time.

Insight Detection Details report

Displays the details of Insight detections. Symantec Endpoint Protection clients generate these detections over a designated period of time.

Installed Files by File Name report

Displays the file name, product name, and manufacturer. It also includes a count of computers where software exists as detected by Software Management Framework.

The report lets users filter the results by manufacturer, product name, and file name.

Installed Files Search report

Displays the manufacturer, product name, file name, product version, and computer name as detected by Software Management Framework.

The report lets users filter the results by manufacturer, product name, and file name.

Intrusion Prevention Detection Details report

Displays the details of IPS detection events. Symantec Endpoint Protection clients generate these events over a designated period of time.

Intrusion Prevention Detection Trend report

Displays a count of IPS detection events over time in a table form. It includes a graphical trend of IPS detection events for a designated period of time.

Intrusion Prevention Signature Details report

Displays the details of the intrusion prevention signatures for the Symantec Endpoint Protection clients.

IT Analytics Configuration Events report

Provides a historical view of the events that occurred during the configuration of IT Analytics Solution.

The report lets the user filter the results by month, day, year, event type, event target, and event descriptions.

IT Analytics Usage Events report

Provides a historical view of the report and cube utilization from IT Analytics Solution.

The report lets users filter the results by a month, day, year, action, source, patch, and user.

Microsoft Server Applications report

Displays the number of computers that have Microsoft server applications.

Microsoft Software Installs report

Displays the number of systems that host common Microsoft software.

Monitor Alert Details report

Displays a summary of Monitor Alerts.

Monitor Metrics CPU Utilization Trend report

Displays a graphical representation of the utilization of each individual processor over time for the monitored client computer. This report includes a table that details the CPU utilization metrics for each processor.

Monitor Metrics Disk Utilization Trend report

Displays a graphical representation of disk utilization over time for a monitored client computer. This report includes a table that details the disk utilization metrics.

Monitor Metrics Network Utilization Trend report

Displays a graphical representation of network utilization over time for a monitored client computer. This report includes a table that details the network utilization metrics.

Monitor Metrics Trend report

Displays a graphical representation of Monitor Alerts and Tasks.

Monitored Processes CPU Utilization Trend report

Displays a graphical representation of the utilization of the CPU over time for the monitored client. This report includes a table that details the CPU utilization metrics for the CPU.

Package Download Event Summary report

Displays the information that is contained in the Software Delivery Package Event cube. This summary includes a graphical trend of package download events by download method (HTTP or UNC).

This report includes a summary of the number of events, computers, packages, disk space used, and download duration per download source and package.

Package Server Availability - Monthly report

Displays the information that is contained in the **Package Server Configuration Event** cube. The report displays the percentage of time that the package servers communicate with Symantec Management Platform. The time is measured by comparing the expected number of configuration requests from a package server to the actual number of configuration requests that the package server performs over time.

The report contains a parameter to designate the expected configuration request interval from the package server plug-in settings that should be used for the calculation. The results are presented in a graphical form. Bars represent the actual configuration requests per month in green. The difference between the expected requests and the actual requests are in red.

This report also contains summary information by month and day in table form. It contains the ability to drill down to see the data further broken down by days within any given month.

Package Server Availability - Daily report

Displays the information that is contained in the **Package Server Configuration Event** cube. The report displays the percentage of time that the package servers communicate with Symantec Management Platform. The time is measured by comparing the expected number of configuration requests from a package server to the actual number of configuration requests that the package server performs over time.

The report contains a parameter to designate the expected configuration request interval from the package server plug-in settings that should be used for the calculation. The results are presented in a graphical form. Bars represent the actual configuration requests per day in green. The difference between the expected requests and the actual requests are in red.

This report also contains summary information by day in table form.

Patch Management Bulletin Summary report

Displays the applicable, installed, and vulnerable computer counts by bulletin.

Patch Management Details report

Displays a summary of computer hardware and OS inventory as detected by Inventory Solution. It contains the parameters that let you on patch risk level and vulnerable computers by severity.

Patch Vulnerability report

Displays the bulletins by severity with a count of applicable, installed, and vulnerable computers as detected by Patch Management Solution.

The report lets users filter the results by severity and bulletin name.

Patch Vulnerability Search report

Displays a summary of the vulnerable computers for each bulletin that Patch Management Solution discovered. It also includes the computer hardware and OS inventory as detected by Inventory Solution.

The report lets users filters the results by severity, bulletin name, and patch status.

Scan Trend report

Displays a count of computers, scans, threats, and the total files that were scanned over time in a table form. It also includes a graphical trend of computers, scans, and threats for a designated period of time.

Servers by Type and Version report

Displays a count of the computers that are running a server OS, and displays these computers by OS title and version.

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 assignee.

ServiceDesk Changes by Assigned to User report

Displays a count of changes by worker 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 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 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 assignee.

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 assignee.

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 assignee.

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 assignee.

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, category, impact, priority, urgency, creator, 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, category, impact, priority, urgency, creator, and assignee.

ServiceDesk Incidents by Category 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, category, impact, priority, urgency, creator, 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, category, impact, priority, urgency, creator, 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, category, impact, priority, urgency, creator, 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, category, impact, priority, urgency, creator, 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, category, impact, priority, urgency, creator, 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, category, impact, priority, urgency, creator, 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, 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, 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, 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, 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, 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, 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, and assignee.

Software Delivery Search report

Displays a summary of computers that have executed the Software Delivery Solution Advertisement. It contains the hardware and OS inventory as detected by Inventory Solution. The report requires users to select an advertisement.

The report lets users filter the results by a month and a year date range.

The source information for this report is the **Software Delivery - Standard** cube. The cube contains the information that is derived from the summary data that is stored in inventory classes and not from the original events.

Software License Compliance by Cost Center report

Displays the license name by cost center. It also contains a count of installed, used, owned, and compliance status.

The report lets users filter the results by license name, month and year, cost center, department, and location.

Software License Compliance by Department report

Displays the license name by department. It also contains a count of installed, used, owned, and compliance status.

The report lets users filter the results by license name, month and year, cost center, department, and location.

Software License Compliance by Location report

Displays the license name by location. It also contains a count of installed, used, owned, and compliance status.

The report lets users filter the results by license name, month and year, cost center, department, and location.

Software License Trend report

Displays by year, quarter, and month a count of installed, used, and owned licenses and their compliance status. It also displays a graphical trend representation of the licenses that are owned, installed, and used. The report requires users to select a license name.

The report lets users filter the results by cost center, department, and location.

SONAR Detection Details report

Displays the details of SONAR detections. Symantec Endpoint Protection clients generate these detections over a designated period of time.

Top 10 Applications Consuming CPU report

Displays a graphical representation of the top Windows processes that are consuming the greatest amount of CPU for a given monitored client computer. This report includes a table that details the hourly maximum and minimum CPU utilization percentage.

Top 10 Applications Consuming Memory report

Displays a graphical representation of the top Windows processes that use the greatest amount of virtual memory for a given monitored client computer. This report includes a table that details the hourly virtual memory utilization.

Top 10 Users Consuming CPU report

Displays a graphical representation of the top owners of Windows processes that are consuming the greatest amount of CPU for a given monitored client computer. This report includes a table that details the hourly maximum and minimum CPU utilization percentage.

Virus Alert Details report

Displays the details of alerts. Symantec Endpoint Protection clients generate these alerts over a designated period of time.

Virus Alert Trend report

Displays a count of blocked, cleaned, quarantined, deleted, suspicious, and still infected alerts over time in a table form. It includes a graphical trend of virus alerts for a designated period of time.

Virus Definition Distribution Details report

Displays the details of virus definition distribution for the Symantec Endpoint Protection clients.

Vista Readiness Details report

Displays a summary of computer hardware and OS inventory as detected by Inventory Solution. It contains the parameters that let you filter the results that are based on the minimum requirements for Microsoft Vista.

The report lets users filter the results by computer name, manufacturer, and model.

Windows 7 Readiness Details report

Displays a summary of computer hardware and OS inventory as detected by Inventory Solution. This report contains the parameters that let you filter the results that are based on the minimum requirements for Microsoft Windows 7.

This report lets you filter the results by computer name, manufacturer, and model.

Appendix D

Dimension Attribute reference

This appendix includes the following topics:

- Add Remove Programs
- Asset
- Asset Status
- Asset Type
- Computer
- Cost Center
- Created Date
- Date
- Department
- EP Access Right
- EP Administrator
- EP Agent Behavior Event
- EP Agent Security Event
- EP Agent System Event
- EP Agent Traffic Event
- EP Alert

- EP Alert Date
- EP AntiVirus Policy Download Advisor
- EP AntiVirus Policy Global Scan Options
- EP AntiVirus Policy Mac Admin Defined Common
- EP AntiVirus Policy Mac Admin Defined Scans
- EP AntiVirus Policy Mac Auto Protect
- EP AntiVirus Policy Mac Miscellaneous
- EP AntiVirus Policy Sonar Settings
- EP AntiVirus Policy Windows Admin Defined Advanced
- EP AntiVirus Policy Windows Admin Defined Scans
- EP AntiVirus Policy Windows Auto Protect
- EP AntiVirus Policy Windows Miscellaneous
- EP AntiVirus Policy
- EP Application and Device Control Policy
- EP Application and Device Control Rule
- EP Blocked Device
- EP Client
- EP Computer
- EP Creation Date
- EP Domain
- EP Event Date
- EP Exception Client Restriction
- EP Exception Item Restriction
- EP Exception Policy
- EP Excluded Device
- EP Firewall Policy Rule
- EP Firewall Policy Security Settings

- EP Firewall Policy
- EP Group
- EP Host Integrity Check
- EP Host Integrity Event
- EP Host Integrity Policy Advanced
- EP Host Integrity Policy Requirement
- EP Host Integrity Policy
- EP Insight Detection
- EP Intrusion Prevention Policy
- EP Intrusion Prevention Signature
- EP IPS Detection Event
- EP Last Checkin Date
- EP Last Scan Date
- EP Last Virus Date
- EP Live Update Policy Mac Advanced
- EP Live Update Policy Mac Schedule
- EP Live Update Policy Mac Server Settings
- EP Live Update Policy Proxy Settings
- EP Live Update Policy Windows Advanced
- EP Live Update Policy Windows Schedule
- EP Live Update Policy Windows Server Settings
- EP Live Update Policy
- EP Location
- EP Policy
- EP Scan Client User
- EP Scan Start Date
- EP Scan Status

- EP Server Admin Event
- EP Server System Event
- EP Server
- EP Site
- EP SONAR Detection
- EP Virus
- EP Virus Definition
- ESX Storage Volume
- ESX Virtual Machine
- Event Console Alert
- Event Console Alert Action Audit Type
- Event Console Alert Category
- Event Console Alert Severity
- Event Console Monitor Rule
- File
- File Modified Date
- Filter
- IIS FTP Site
- IIS Server
- IIS Virtual Directory
- IIS Web Site
- Last Basic Inventory Date
- Location
- Logical Disk
- Monitor Metric
- Monitor Metric Detail Level
- Monitor Metric Instance

- Monitor Metric Source
- Monitor NT Event Category
- Monitor NT Event Description
- Monitor NT Event ID
- Monitor NT Event Log File
- Monitor NT Event Message DLL
- Monitor NT Event Rule Triggered
- Monitor NT Event Source
- Monitor NT Event Type
- Monitor NT Event User
- Monitor Process Name
- Monitor Process Owner
- Monitor Task
- Organizational Group
- Package
- Package Distribution Event Status
- Package Download Method
- Package Download Source
- Package Download URL
- Package Server
- Package Status
- Parent Task
- Processor
- ServiceDesk Affected User
- ServiceDesk Assigned to User
- ServiceDesk Change
- ServiceDesk Change Impact

- ServiceDesk Change Location
- ServiceDesk Change Priority
- ServiceDesk Change Source
- ServiceDesk Change Status
- ServiceDesk Change Type
- ServiceDesk Change Urgency
- ServiceDesk Contact Type
- ServiceDesk Created by User
- ServiceDesk Date Closed
- ServiceDesk Date Due
- ServiceDesk Date Ended
- ServiceDesk Date Implemented
- ServiceDesk Date Modified
- ServiceDesk Date Needed
- ServiceDesk Date Opened
- ServiceDesk Date Resolved
- ServiceDesk Date Reviewed
- ServiceDesk Date Scheduled
- ServiceDesk Date Started
- ServiceDesk Incident
- ServiceDesk Incident Category
- ServiceDesk Incident Close Code
- ServiceDesk Incident Impact
- ServiceDesk Incident Location
- ServiceDesk Incident Priority
- ServiceDesk Incident Source
- ServiceDesk Incident Status

- ServiceDesk Incident Type
- ServiceDesk Incident Urgency
- ServiceDesk Last Modified by User
- ServiceDesk Problem
- ServiceDesk Problem Category
- ServiceDesk Problem Impact
- ServiceDesk Problem Location
- ServiceDesk Problem Priority
- ServiceDesk Problem Source
- ServiceDesk Problem Status
- ServiceDesk Problem Urgency
- ServiceDesk Reference
- ServiceDesk Resolved by User
- ServiceDesk Time Closed
- ServiceDesk Time Due
- ServiceDesk Time Ended
- ServiceDesk Time Implemented
- ServiceDesk Time Modified
- ServiceDesk Time Needed
- ServiceDesk Time Opened
- ServiceDesk Time Resolved
- ServiceDesk Time Reviewed
- ServiceDesk Time Scheduled
- ServiceDesk Time Started
- ServiceDesk User
- Software Component
- Software Delivery Advertisement

- Software Delivery Execution Event Command Line
- Software Delivery Execution Event Status
- Software Delivery Package Event Status
- Software Delivery Status Event Status
- Software Delivery Status Event Type
- Software License
- Software Product
- Software Purchase
- Software Update
- Software Update Release Date
- SQL Cluster
- SQL Cluster Resource
- SQL Database
- SQL Database Creation Date
- SQL Database System
- SQL Storage Area
- SQL User
- Task
- Task Server
- Time
- User

Add Remove Programs

Add Remove Programs contains the following dimension attributes:

- **Add Remove Programs - Display Name**
- **Add Remove Programs - Hidden**

Asset

Asset contains the following dimension attributes:

- **Asset - Asset Tag**
- **Asset - Barcode**
- **Asset - Manufacturer**
- **Asset - Model**
- **Asset - Name**
- **Asset - Resource Guide**
- **Asset - Serial Number**
- **Asset - Server**

Asset Status

Asset Status contains the following dimension attributes:

- **Asset - Status**

Asset Type

Asset Type contains the following dimension attributes:

- **Asset - Type**

Computer

Computer contains the following dimension attributes:

- **Computer - Symantec Managed**
- **Computer - Discovery Method**
- **Computer - Domain**
- **Computer - IP Address**
- **Computer - Last Logon User**
- **Computer - MAC Address**
- **Computer - Manufacturer**
- **Computer - Model**

- **Computer - Name**
- **Computer - OS Name**
- **Computer - OS Type**
- **Computer - OS Version**
- **Computer - OS Revision**
- **Computer - Primary User**
- **Computer - Resource Guide**
- **Computer - Serial Number**
- **Computer - Server**
- **Computer - System Type**

Cost Center

Cost Center contains the following dimension attributes:

- **Cost Center - Code**
- **Cost Center - Hierarchy Path**
- **Cost Center - Name**

Created Date

Created Date contains the following dimension attributes:

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

Date

Date contains the following dimension attributes:

- **Date**
- **Day of Week**

- **Month**
- **Quarter**
- **Year**

Department

Department contains the following dimension attributes:

- **Department - Hierarchy Level**
- **Department - Hierarchy Path**
- **Department - Name**

EP Access Right

EP Access Right contains the following dimension attributes:

- **Access Right - Type**

EP Administrator

EP Administrator contains the following dimension attributes:

- **Administrator - Account Name**
- **Administrator - Authentication Method**
- **Administrator - Domain**
- **Administrator - Full Name**
- **Administrator - Status**
- **Administrator - Type**
- **Administrator - User Name**

EP Agent Behavior Event

EP Agent Behavior Event contains the following dimension attributes:

- **Agent Behavior Event - Action**
- **Agent Behavior Event - Alert**
- **Agent Behavior Event - Caller Process**

- **Agent Behavior Event - Caller Return Address**
- **Agent Behavior Event - Caller Return Module**
- **Agent Behavior Event - Description**
- **Agent Behavior Event - Domain**
- **Agent Behavior Event - Encoded API**
- **Agent Behavior Event - Hardware Key**
- **Agent Behavior Event - Host Name**
- **Agent Behavior Event - ID**
- **Agent Behavior Event - Parameter**
- **Agent Behavior Event - Repetition**
- **Agent Behavior Event - Rule**
- **Agent Behavior Event - Send SNMP Trap**
- **Agent Behavior Event - Severity**
- **Agent Behavior Event - Test Mode**
- **Agent Behavior Event - User**
- **Agent Behavior Event - USN**
- **Agent Behavior Event - VAPI**

EP Agent Security Event

EP Agent Security Event contains the following dimension attributes:

- **Agent Security Event - Alert**
- **Agent Security Event - App Name**
- **Agent Security Event - Description**
- **Agent Security Event - Domain**
- **Agent Security Event - Hack Type**
- **Agent Security Event - Hardware Key**
- **Agent Security Event - Host Name**
- **Agent Security Event - ID**
- **Agent Security Event - Local Host IP**

- **Agent Security Event - Local Host MAC**
- **Agent Security Event - Location**
- **Agent Security Event - Network Protocol**
- **Agent Security Event - Remote Host IP**
- **Agent Security Event - Remote Host MAC**
- **Agent Security Event - Remote Host Name**
- **Agent Security Event - Repetition**
- **Agent Security Event - Send SNMP Trap**
- **Agent Security Event - Severity**
- **Agent Security Event - Traffic Direction**
- **Agent Security Event - Type**
- **Agent Security Event - User**

EP Agent System Event

EP Agent System Event contains the following dimension attributes:

- **Agent System Event - Category**
- **Agent System Event - Description**
- **Agent System Event - Hardware Key**
- **Agent System Event - Host Name**
- **Agent System Event - ID**
- **Agent System Event - Send SNMP Trap**
- **Agent System Event - Severity**
- **Agent System Event - Source**
- **Agent System Event - Type**

EP Agent Traffic Event

EP Agent Traffic Event contains the following dimension attributes:

- **Agent Traffic Event - Alert**
- **Agent Traffic Event - App Name**

- **Agent Traffic Event - Blocked**
- **Agent Traffic Event - Domain**
- **Agent Traffic Event - Hardware Key**
- **Agent Traffic Event - ID**
- **Agent Traffic Event - Local Host IP**
- **Agent Traffic Event - Local Host MAC**
- **Agent Traffic Event - Local Port**
- **Agent Traffic Event - Location**
- **Agent Traffic Event - Network Protocol**
- **Agent Traffic Event - Remote Host IP**
- **Agent Traffic Event - Remote Host MAC**
- **Agent Traffic Event - Remote Host Name**
- **Agent Traffic Event - Remote Port**
- **Agent Traffic Event - Repetition**
- **Agent Traffic Event - Rule**
- **Agent Traffic Event - Send SNMP Trap**
- **Agent Traffic Event - Severity**
- **Agent Traffic Event - Traffic Direction**
- **Agent Traffic Event - User**

EP Alert

EP Alert contains the following dimension attributes:

- **Alert - Actual Action**
- **Alert - File Path**
- **Alert - Requested Action**
- **Alert - Secondary Action**
- **Alert - Source**
- **Alert - User Name**
- **Alert - Virus Type**

EP Alert Date

EP Alert Date contains the following dimension attributes:

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

EP AntiVirus Policy Download Advisor

EP AntiVirus Policy Download Advisor contains the following dimension attributes:

- **Download Advisor - Enabled**
- **Download Advisor - Enabled Lock**
- **Download Advisor - First Seen Days Threshold**
- **Download Advisor - First Seen Days Threshold Enabled**
- **Download Advisor - Prevalence Threshold**
- **Download Advisor - Prevalence Threshold Enabled**
- **Download Advisor - Threshold**
- **Download Advisor - Threshold Lock**
- **Download Advisor - Trust Intranet**
- **Download Advisor - Trust Intranet Lock**

EP AntiVirus Policy Global Scan Options

EP AntiVirus Policy Global Scan Options contains the following dimension attributes:

- **Global Scan Options – Bloodhound Enabled**
- **Global Scan Options – Bloodhound Enabled Lock**
- **Global Scan Options – Bloodhound Level**
- **Global Scan Options – Scanless Enabled**

- **Global Scan Options – Scanless Enabled Lock**
- **Global Scan Options – Scanless For**

EP AntiVirus Policy Mac Admin Defined Common

EP AntiVirus Policy Mac Admin Defined Common contains the following dimension attributes:

- **Mac Admin Defined Common – Allow Scan Can Cancel**
- **Mac Admin Defined Common – Allow Scan Can Snooze**
- **Mac Admin Defined Common – Auto Repair Infected Files**
- **Mac Admin Defined Common – Quarantine unrepairable Files**
- **Mac Admin Defined Common – Scan Inside Compressed Files**
- **Mac Admin Defined Common – Scan Results Display**

EP AntiVirus Policy Mac Admin Defined Scans

EP AntiVirus Policy Mac Admin Defined Scans contains the following dimension attributes:

- **Mac Admin Defined Scans – Description**
- **Mac Admin Defined Scans – Enabled**
- **Mac Admin Defined Scans – Scan Name**

EP AntiVirus Policy Mac Auto Protect

EP AntiVirus Policy Mac Auto Protect contains the following dimension attributes:

- **Mac Auto Protect – Allow Can Cancel**
- **Mac Auto Protect – Allow Can Snooze**
- **Mac Auto Protect – Auto Repair Infected Files**
- **Mac Auto Protect – Disk Type All**
- **Mac Auto Protect – Disk Type All Others**
- **Mac Auto Protect – Disk Type Audio Video**
- **Mac Auto Protect – Disk Type Data Disk**

- **Mac Auto Protect – Disk Type IPOD**
- **Mac Auto Protect – Enable Auto Protect**
- **Mac Auto Protect – Enable Auto Protect Lock**
- **Mac Auto Protect – Mount Disk Scan Options Enabled**
- **Mac Auto Protect – Quarantine Unrepairable Files**
- **Mac Auto Protect – Scan Compressed Files**
- **Mac Auto Protect – Scan Files In Folder**
- **Mac Auto Protect – Scan Option**

EP AntiVirus Policy Mac Miscellaneous

EP AntiVirus Policy Mac Miscellaneous contains the following dimension attributes:

- **Mac Miscellaneous – Display Outdated Message**
- **Mac Miscellaneous – Warn After Days**

EP AntiVirus Policy Sonar Settings

EP AntiVirus Policy Sonar Settingscontains the following dimension attributes:

- **Sonar Settings - Display Alert**
- **Sonar Settings - Display Alert Lock**
- **Sonar Settings - DNS Change Action**
- **Sonar Settings - DNS Change Locked**
- **Sonar Settings - Enabled**
- **Sonar Settings - Enabled Lock**
- **Sonar Settings - High Risk**
- **Sonar Settings - High Risk Lock**
- **Sonar Settings - Host File Change Action**
- **Sonar Settings - Host File Change Locked**
- **Sonar Settings - Low Risk**
- **Sonar Settings - Low Risk Lock**
- **Sonar Settings - Prompt Stop Service**

- **Sonar Settings - Prompt Stop Service Lock**
- **Sonar Settings - Prompt Terminate Process**
- **Sonar Settings - Prompt Terminate Process Lock**
- **Sonar Settings - SB High Risk**
- **Sonar Settings - SB High Risk Lock**
- **Sonar Settings - SB Low Risk**
- **Sonar Settings - SB Low Risk Lock**
- **Sonar Settings - System Changes Enabled**
- **Truscan - Can For Keyloggers**
- **Truscan - Incremental Scan Interval**
- **Truscan - Lock Incremental Scan Interval**
- **Truscan - Lock Scan New Processes**
- **Truscan - Lock Use Default Scan Frequency**
- **Truscan - Scan For Trojans And Worms**
- **Truscan - Scan New Processes**
- **Truscan - Use Default Scan Frequency**

EP AntiVirus Policy Windows Admin Defined Advanced

EP AntiVirus Policy Windows Admin Defined Advanced contains the following dimension attributes:

- **Windows Admin Defined Advanced - Allow Pause Or Delay Scan**
- **Windows Admin Defined Advanced - Allow Scan Without User Log On**
- **Windows Admin Defined Advanced - Allow User Modify Startup Scans**
- **Windows Admin Defined Advanced - Allow User Stop Scan**
- **Windows Admin Defined Advanced - Close Window When Done**
- **Windows Admin Defined Advanced - Delay Scan When On Batteries**
- **Windows Admin Defined Advanced - Progress Display Option**
- **Windows Admin Defined Advanced - Run Scan On Login**
- **Windows Admin Defined Advanced - Run Scan When New Defs Arrive**
- **Windows Admin Defined Advanced - Threat Submission Process**

EP AntiVirus Policy Windows Admin Defined Scans

EP AntiVirus Policy Windows Admin Defined Scans contains the following dimension attributes:

- **Windows Admin Defined Scans – Description**
- **Windows Admin Defined Scans - Enabled**
- **Windows Admin Defined Scans – Scan Name**

EP AntiVirus Policy Windows Auto Protect

EP AntiVirus Policy Windows Auto Protect contains the following dimension attributes:

- **Windows Auto Protect - Back Up File Before Repair**
- **Windows Auto Protect - Enable Floppy Drive**
- **Windows Auto Protect - Enable Network Drive**
- **Windows Auto Protect - File System Auto Protect**
- **Windows Auto Protect - Internet Email Auto Protect**
- **Windows Auto Protect - Lock Back Up File Before Repair**
- **Windows Auto Protect - Lock Block Security Risk Install**
- **Windows Auto Protect - Lock Enable Floppy Drive**
- **Windows Auto Protect - Lock Enable Network Drive**
- **Windows Auto Protect - Lock File System Auto Protect**
- **Windows Auto Protect - Lock File Types**
- **Windows Auto Protect - Lock Macro Virus First Action**
- **Windows Auto Protect - Lock Macro Virus Second Action**
- **Windows Auto Protect - Lock Non Macro Virus First Action**
- **Windows Auto Protect - Lock Non Macro Virus Second Action**
- **Windows Auto Protect - Lock Scan Security Risks**
- **Windows Auto Protect - Lock Security Risks First Action**
- **Windows Auto Protect - Lock Security Risks Second Action**
- **Windows Auto Protect - Lock Stop Services Automatically**
- **Windows Auto Protect - Lock Terminate Processes Automatically**

- **Windows Auto Protect - Lotus Notes Auto Protect**
- **Windows Auto Protect - Macro Virus First Action**
- **Windows Auto Protect - Macro Virus Second Action**
- **Windows Auto Protect - Microsoft Outlook Auto Protect**
- **Windows Auto Protect - Non Macro Virus First Action**
- **Windows Auto Protect - Non Macro Virus Second Action**
- **Windows Auto Protect - Scan All Files**
- **Windows Auto Protect - Scan Security Risks**
- **Windows Auto Protect - Security Risks First Action**
- **Windows Auto Protect - Security Risks Second Action**
- **Windows Auto Protect - Stop Services Automatically**
- **Windows Auto Protect - Terminate Processes Automatically**

EP AntiVirus Policy Windows Miscellaneous

AntiVirus Policy Windows Miscellaneous contains the following dimension attributes:

- **Windows Miscellaneous – Disable AV Alerts In Windows Security Center**
- **Windows Miscellaneous – Display Windows Security center Msg When Defs Are Outdated**
- **Windows Miscellaneous – Windows Security Center Disabled**

EP AntiVirus Policy

EP AntiVirus Policy contains the following dimension attributes:

- **AntiVirus Policy - Description**
- **AntiVirus Policy - Enabled**
- **AntiVirus Policy - Name**

EP Application and Device Control Policy

EP Application and Device Control Policy contains the following dimension attributes:

- **Application and Device Control Policy - Description**
- **Application and Device Control Policy - Enabled**
- **Application and Device Control Policy - Name**

EP Application and Device Control Rule

EP Application and Device Control Rule contains the following dimension attributes:

- **Rule - Name**

EP Blocked Device

EP Blocked Device contains the following dimension attributes:

- **Blocked Device – Name**

EP Client

EP Client contains the following dimension attributes:

- **Client - Client Type**
- **Client - Client Version**
- **Client - Client Version Status**
- **Client - Antivirus Engine Status**
- **Client - Auto-Protect Status**
- **Client - Firewall Status**
- **Client - Free Disk**
- **Client - Free Memory**
- **Client - Host Integrity Status**
- **Client - Infected**
- **Client - Major Version**
- **Client - Minor Version**
- **Client - Online Status**
- **Client - Profile Serial Number**

- **Client - Profile Version**
- **Client - Reboot Required**
- **Client - Tamper Protection Status**
- **Client - Time Zone**

EP Computer

EP Computer contains the following dimension attributes:

- **Computer - BIOS Version**
- **Computer - Computer Name**
- **Computer - Current Login Domain**
- **Computer - Current Login Server**
- **Computer - DHCP Server**
- **Computer - Disk Drive**
- **Computer - Disk Total**
- **Computer - DNS Server**
- **Computer - Domain**
- **Computer - IP Address**
- **Computer - Memory Total**
- **Computer - Operating System**
- **Computer - OS Language**
- **Computer - Processor Clock Speed**
- **Computer - Processor Count**
- **Computer - Processor Type**
- **Computer - Service Pack**
- **Computer - TPM Device**
- **Computer - WINS Server**

EP Creation Date

EP Creation Date contains the following dimension attributes:

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

EP Domain

EP Domain contains the following dimension attributes:

- **Domain**

EP Event Date

EP Event Date contains the following dimension attributes:

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

EP Exception Client Restriction

EP Exception Client Restriction contains the following dimension attributes:

- **Client Restriction - Add Application Exceptions**
- **Client Restriction - Add Extension Exceptions**
- **Client Restriction - Add File Exceptions**
- **Client Restriction - Add Folder Exceptions**
- **Client Restriction - Add Known Risk Exceptions**
- **Client Restriction - Add Security Risk Exceptions**
- **Client Restriction - Add SONAR Exceptions**
- **Client Restriction - Add Trusted Web Domain Exceptions**

EP Exception Item Restriction

EP Exception Item Restriction contains the following dimension attributes:

- **Exception Item - Action**
- **Exception Item - Platform**
- **Exception Item - Type**
- **Exception Item - Value**

EP Exception Policy

EP Exception Policy contains the following dimension attributes:

- **Exception Policy - Description**
- **Exception Policy - Enabled**
- **Exception Policy - Name**

EP Excluded Device

EP Excluded Device contains the following dimension attributes:

- **Excluded Device - Name**

EP Firewall Policy Rule

EP Firewall Policy Rule contains the following dimension attributes:

- **Rule - Enabled**
- **Rule - Name**

EP Firewall Policy Security Settings

EP Firewall Policy Security Settings contains the following dimension attributes:

- **Security Settings - Anti MAC Spooling**
- **Security Settings - Disable Windows Firewall**
- **Security Settings - Net BIOS Protection**
- **Security Settings - OS Fingerprint Masquerading**
- **Security Settings - Reverse DNS**

- **Security Settings - Smart DO-IP**
- **Security Settings - Smart DNS**
- **Security Settings - Smart WINS**
- **Security Settings - Stealth Mode Browsing**
- **Security Settings - TCP Resequencing**
- **Security Settings - Token Ring Traffic**

EP Firewall Policy

EP Firewall Policy contains the following dimension attributes:

- **Firewall Policy - Description**
- **Firewall Policy - Enabled**
- **Firewall Policy - Name**

EP Group

EP Group contains the following dimension attributes:

- **Group**

EP Host Integrity Check

EP Host Integrity Check contains the following dimension attributes:

- **Host Integrity Check - Action**
- **Host Integrity Check - Criteria**
- **Host Integrity Check - Description**
- **Host Integrity Check - Result**
- **Host Integrity Check - Rule Name**
- **Host Integrity Check - Rule Type**
- **Host Integrity Check - Target**

EP Host Integrity Event

EP Host Integrity Event contains the following dimension attributes:

- **Host Integrity Event - Description**
- **Host Integrity Event - ID**
- **Host Integrity Event - Location**
- **Host Integrity Event - Severity**
- **Host Integrity Event - Type**
- **Host Integrity Event - User**

EP Host Integrity Policy Advanced

EP Host Integrity Policy Advanced contains the following dimension attributes:

- **Advanced - Allow User to Cancel Remediation Max**
- **Advanced - Allow User to Cancel Remediation Max Number Of Times**
- **Advanced - Allow User to Cancel Remediation Min**
- *Advanced - Check HI Every*
- **Advanced - Continue Check Alter Fail**
- **Advanced - Display Notification When HI Check Fails**
- **Advanced - Display Notification When HI Check Fails Additional Text**
- **Advanced - Display Notification When HI Check Passes Alter Fail**
- **Advanced - Display Notification When HI Check Passes Alter Fail Additional Text**
- **Advanced - Keep Results For**
- **Advanced - Notification On Snooze Additional Text**
- **Advanced - Show Verbose Host Integrity Logging**
- **Advanced - User Must Log On Before Apps And HI Notifications Appear**

EP Host Integrity Policy Requirement

EP Host Integrity Policy Requirement contains the following dimension attributes:

- **Requirement - Enabled**
- **Requirement - Name**
- **Requirement - When HI Checks Run**

EP Host Integrity Policy

EP Host Integrity Policy contains the following dimension attributes:

- **Host Integrity Policy - Description**
- **Host Integrity Policy - Enabled**
- **Host Integrity Policy - Name**

EP Insight Detection

EP Insight Detection contains the following dimension attributes:

- **Insight Detection - Application**
- **Insight Detection - Application Version**
- **Insight Detection - Company**
- **Insight Detection - Detection Reason**
- **Insight Detection - Domain**
- **Insight Detection - File Path**
- **Insight Detection - Risk**
- **Insight Detection - Sensitivity**
- **Insight Detection - URL**
- **Insight Detection - User**
- **Insight Detection - Whitelist Reason**

EP Intrusion Prevention Policy

EP Intrusion Prevention Policy contains the following dimension attributes:

- **IDS Policy - Active Response Block IP**
- **IDS Policy - Denial Of Service Protection**
- **IDS Policy - Enabled**
- **IDS Policy - Exceptions Exist**
- **IDS Policy - Intrusion Prevention**
- **IDS Policy - Name**
- **IDS Policy - Port Scan Detection**

EP Intrusion Prevention Signature

EP Intrusion Prevention Signature contains the following dimension attributes:

- **Intrusion Prevention Signature - Pattern Date**
- **Intrusion Prevention Signature - Revision**
- **Intrusion Prevention Signature - Sequence Number**
- **Intrusion Prevention Signature - Version**

EP IPS Detection Event

EP IPS Detection Event contains the following dimension attributes:

- **IPS Detection - Application Name**
- **IPS Detection - Name**
- **IPS Detection - SID**

EP Last Checkin Date

EP Last Checkin Date contains the following dimension attributes:

- **Last Checkin Date - Date**
- **Last Checkin Date - Day of Week**
- **Last Checkin Date - Month**
- **Last Checkin Date - Quarter**
- **Last Checkin Date - Year**

EP Last Scan Date

EP Last Scan Date contains the following dimension attributes:

- **Last Scan Date - Date**
- **Last Scan Date - Day of Week**
- **Last Scan Date - Month**
- **Last Scan Date - Quarter**
- **Last Scan Date - Year**

EP Last Virus Date

EP Last Virus Date contains the following dimension attributes:

- **Last Virus Date - Date**
- **Last Virus Date - Day of Week**
- **Last Virus Date - Month**
- **Last Virus Date - Quarter**
- **Last Virus Date - Year**

EP Live Update Policy Mac Advanced

EP Live Update Policy Mac Advanced contains the following dimension attributes:

- **Mac Settings – Download SEP Updates Using LU Server**

EP Live Update Policy Mac Schedule

EP Live Update Policy Mac Schedule contains the following dimension attributes:

- **Mac Settings - Download Updates Day**
- **Mac Settings - Download Updates Frequency**
- **Mac Settings - Download Updates Frequency Interval**
- **Mac Settings - Download Updates Start Time**
- **Mac Settings - Randomization Enabled**
- **Mac Settings - Randomization Time**
- **Mac Settings - Retry Window**
- **Mac Settings - Retry Window Enabled**

EP Live Update Policy Mac Server Settings

EP Live Update Policy Mac Server Settings contains the following dimension attributes:

- **Mac Settings - Live Update Server Type**

EP Live Update Policy Proxy Settings

EP Live Update Policy Proxy Settings contains the following dimension attributes:

- **Proxy Settings - Ftp Proxy**
- **Proxy Settings - Ftp Proxy Mode**
- **Proxy Settings - Ftp Proxy Mode Lock**
- **Proxy Settings - Ftp Proxy Port**
- **Proxy Settings - Http Proxy**
- **Proxy Settings - Http Proxy Https Port**
- **Proxy Settings - Http Proxy Mode**
- **Proxy Settings - Http Proxy Mode Lock**
- **Proxy Settings - Http Proxy Port**
- **Proxy Settings - Http Proxy Require Authentication**
- **Proxy Settings - Http Proxy User Name**

EP Live Update Policy Windows Advanced

EP Live Update Policy Windows Advanced contains the following dimension attributes:

- **Windows Settings - Download Updated by LiveUpdate Enabled**
- **Windows Settings - Manual LiveUpdate Enabled**
- **Windows Settings - Modify LiveUpdate Schedule Enabled**
- **Windows Settings - Require Http Headers Enabled**

EP Live Update Policy Windows Schedule

EP Live Update Policy Windows Schedule contains the following dimension attributes:

- **Windows Settings - Download Updates Day**
- **Windows Settings - Download Updates Interval**
- **Windows Settings - Download Updates Frequency**
- **Windows Settings - Download Updates Start Time**

- **Windows Settings - Enable LiveUpdate Scheduling**
- **Windows Settings - Idle Detection Enabled**
- **Windows Settings - Randomization Enabled**
- **Windows Settings - Randomization Time**
- **Windows Settings - Retry Window**
- **Windows Settings - Retry Window Enabled**

EP Live Update Policy Windows Server Settings

EP Live Update Policy Windows Server Settings contains the following dimension attributes:

- **Windows Settings - 3rd Party Server**
- **Windows Settings - Group Update Client Throttling**
- **Windows Settings - Group Update Delete Unused Contents Days**
- **Windows Settings - Group Update Host**
- **Windows Settings - Group Update Max Disk Cache Allowed**
- **Windows Settings - Group Update Max Simul Client Down Loads**
- **Windows Settings - Group Update Port**
- **Windows Settings - Live Update Server Type**
- **Windows Settings - Use Group Update Provider**
- **Windows Settings - Use Live Update Server**
- **Windows Settings - Use Management Server**

EP Live Update Policy

EP Live Update Policy contains the following dimension attributes:

- **Live Update Policy - Description**
- **Live Update Policy - Enabled**
- **Live Update Policy - Name**

EP Location

EP Location contains the following dimension attributes:

- **Location - Description**
- **Location - Name**

EP Policy

EP Policy contains the following dimension attributes:

- **Policy - Description**
- **Policy - Enabled**
- **Policy - Name**
- **Policy - Type**

EP Scan Client User

EP Scan Client User contains the following dimension attributes:

- **Scan - Client User**

EP Scan Start Date

EP Scan Start Date contains the following dimension attributes:

- **Scan Start Date - Date**
- **Scan Start Date - Day of Week**
- **Scan Start Date - Month**
- **Scan Start Date - Quarter**
- **Scan Start Date - Year**

EP Scan Status

EP Scan Status contains the following dimension attributes:

- **Scan - Status**

EP Server Admin Event

EP Server Admin Event contains the following dimension attributes:

- **Server Admin Event - Administrator Name**
- **Server Admin Event - Description**
- **Server Admin Event - Error Code**
- **Server Admin Event - ID**
- **Server Admin Event - Message ID**
- **Server Admin Event - Severity**
- **Server Admin Event - Stack Trace**
- **Server Admin Event - Type**

EP Server System Event

EP Server System Event contains the following dimension attributes:

- **Server System Event - Description**
- **Server System Event - Error Code**
- **Server System Event - ID**
- **Server System Event - Message ID**
- **Server System Event - Severity**
- **Server System Event - Stack Trace**

EP Server

EP Server contains the following dimension attributes:

- **Server**

EP Site

EP Site contains the following dimension attributes:

- **Site**

EP SONAR Detection

EP SONAR Detection contains the following dimension attributes:

- **SONAR Detection - Application Name**
- **SONAR Detection - Application Version**
- **SONAR Detection - Company**
- **SONAR Detection - File Path**
- **SONAR Detection - Risk**
- **SONAR Detection - Score**
- **SONAR Detection - Sensitivity**
- **SONAR Detection - Type**
- **SONAR Detection - User**
- **SONAR Detection - Whitelist Reason**

EP Virus

EP Virus contains the following dimension attributes:

- **Virus - Date Discovered**
- **Virus - Name**
- **Virus - Risk Category**
- **Virus - Threat Location**
- **Virus - Threat Type**

EP Virus Definition

EP Virus Definition contains the following dimension attributes:

- **Virus Definition - Content Status**
- **Virus Definition - Content Type**
- **Virus Definition - Date**
- **Virus Definition - Revision**
- **Virus Definition - Sequence Number**
- **Virus Definition - Version**

ESX Storage Volume

ESX Storage Volume contains the following dimension attributes:

- **ESX Storage Volume - File System Version**
- **ESX Storage Volume - Free Size GB**
- **ESX Storage Volume - Instance ID**
- **ESX Storage Volume - Total Size GB**
- **ESX Storage Volume - Volume Name**

ESX Virtual Machine

ESX Virtual Machine contains the following dimension attributes:

- **ESX Virtual Machine - Automatic Shutdown Action**
- **ESX Virtual Machine - Automatic Shutdown Delay**
- **ESX Virtual Machine - Automatic Startup Action**
- **ESX Virtual Machine - Automatic Startup Delay**
- **ESX Virtual Machine - CPS Assigned**
- **ESX Virtual Machine - Disk Used GB**
- **ESX Virtual Machine - Instance ID**
- **ESX Virtual Machine - Max Disk Size GB**
- **ESX Virtual Machine - Memory Allocated GB**
- **ESX Virtual Machine - Name**
- **ESX Virtual Machine - State**
- **ESX Virtual Machine - Virtual System Type**

Event Console Alert

Event Console Alert contains the following dimension attributes:

- **Event Console Alert - Alert ID**
- **Event Console Alert - Hostname**
- **Event Console Alert - Message**

Event Console Alert Action Audit Type

Event Console Alert Action Audit Type contains the following dimension attributes:

- **Event Console Alert Action Audit Type - Action Type Description**
- **Event Console Alert Action Audit Type - Action Type Name**

Event Console Alert Category

Event Console Alert Category contains the following dimension attributes:

- **Event Console Alert Category - Name**

Event Console Alert Severity

Event Console Alert Severity contains the following dimension attributes:

- **Event Console Alert Severity - Severity Level**
- **Event Console Alert Severity - Severity Name**

Event Console Monitor Rule

Event Console Monitor Rule contains the following dimension attributes:

- **Event Console Monitor Rule - Category Name**
- **Event Console Monitor Rule - Monitor Pack Name**
- **Event Console Monitor Rule - Rule Name**

File

File contains the following dimension attributes:

- **File - Name**

File Modified Date

File Modified Date contains the following dimension attributes:

- **Filed Modified Date - Date**
- **Filed Modified Date - Day of the Week**

- **File Modified Date - Month**
- **Filed Modified Date - Quarter**
- **File Modified Date - Year**

Filter

Filter contains the following dimension attributes:

- **Filter - Name**

IIS FTP Site

IIS FTP Site contains the following dimension attributes:

- **IIS FTP Site - Name**
- **IIS FTP Site - Path**
- **IIS FTP Site - Rights**

IIS Server

IIS Server contains the following dimension attributes:

- **IIS Server - Application Server Console Installed**
- **IIS Server - ASP Dot Net Installed**
- **IIS Server - ASP Installed**
- **IIS Server - BITS Service**
- **IIS Server - COM Plus Service**
- **IIS Server - Instance ID**
- **IIS Server - Internet Data Connector Installed**
- **IIS Server - Message Queue Service**
- **IIS Server - Network DTC Installed**
- **IIS Server - NNTP Service**
- **IIS Server - Remote Admin Installed**
- **IIS Server - Remote Desktop Web Connection Installed**
- **IIS Server - Service**

- **IIS Server - SMTP Service**
- **IIS Server - Version**
- **IIS Server - WWW Service**

IIS Virtual Directory

IIS Virtual Directory contains the following dimension attributes:

- **IIS Virtual Directory - Access Read Enabled**
- **IIS Virtual Directory - Access Write Enabled**
- **IIS Virtual Directory - Anonymous Authentication Enabled**
- **IIS Virtual Directory - Application Name**
- **IIS Virtual Directory - Application Pool**
- **IIS Virtual Directory - Basic Authentication Enabled**
- **IIS Virtual Directory - Content Expiration Enabled**
- **IIS Virtual Directory - Content Expiration Setting**
- **IIS Virtual Directory - Content Location**
- **IIS Virtual Directory - Content Location Path**
- **IIS Virtual Directory - Default Document Name**
- **IIS Virtual Directory - Default Document Enabled**
- **IIS Virtual Directory - Digest Authentication Enabled**
- **IIS Virtual Directory - Directory Browsing Enabled**
- **IIS Virtual Directory - Dot Net Passport Authentication Enabled**
- **IIS Virtual Directory - Element Name**
- **IIS Virtual Directory - Execute Permission**
- **IIS Virtual Directory - Integrated Windows Authentication Enabled**
- **IIS Virtual Directory - Log Enabled**
- **IIS Virtual Directory - Name**
- **IIS Virtual Directory - Script Source Access Enabled**
- **IIS Virtual Directory - Session State Enabled**
- **IIS Virtual Directory - Session Timeout**

- **IIS Virtual Directory - SSL Access Enabled**

IIS Web Site

IIS Web Site contains the following dimension attributes:

- **IIS Web Site - Access Read Enabled**
- **IIS Web Site - Access Write Enabled**
- **IIS Web Site - Anonymous Authentication Enabled**
- **IIS Web Site - Application Name**
- **IIS Web Site - Application Pool**
- **IIS Web Site - Bandwidth Throttling Enabled**
- **IIS Web Site - Bandwidth Throttling Limit**
- **IIS Web Site - Basic Authentication Enabled**
- **IIS Web Site - Buffering Enabled**
- **IIS Web Site - Certificate Enabled**
- **IIS Web Site - Connection Limit**
- **IIS Web Site - Content Expiration Enabled**
- **IIS Web Site - Content Expiration Setting**
- **IIS Web Site - Content Location**
- **IIS Web Site - Default Document Name**
- **IIS Web Site - Default Document Enabled**
- **IIS Web Site - Digest Authentication Enabled**
- **IIS Web Site - Directory Browsing Enabled**
- **IIS Web Site - Dot Net Passport Authentication Enabled**
- **IIS Web Site - Enforce Process Throttling**
- **IIS Web Site - Execute Permission**
- **IIS Web Site - Instance ID**
- **IIS Web Site - Integrated Windows Authentication Enabled**
- **IIS Web Site - Log Enabled**
- **IIS Web Site - Max CPU Use Percentage**

- **IIS Web Site - Name**
- **IIS Web Site - Parents Path Enabled**
- **IIS Web Site - Process Throttling Enabled**
- **IIS Web Site - Script Source Access Enabled**
- **IIS Web Site - Session State Enabled**

Last Basic Inventory Date

Last Basic Inventory Date contains the following dimension attributes:

- **Last Basic Inventory Date - Date**
- **Last Basic Inventory Date - Day of Week**
- **Last Basic Inventory Date - Month**
- **Last Basic Inventory Date - Quarter**
- **Last Basic Inventory Date - Year**

Location

Location contains the following dimension attributes:

- **Location - Address**
- **Location - City**
- **Location - Country**
- **Location - Name**
- **Location - State**
- **Location - Zip**

Logical Disk

Logical Disk contains the following dimension attributes:

- **Logical Disk - Description**
- **Logical Disk - File System**
- **Logical Disk - Name**

Monitor Metric

Monitor Metric contains the following dimension attributes:

- **Monitor Metric - Metric Name**

Monitor Metric Detail Level

Monitor Metric Detail Level contains the following dimension attributes:

- **Monitor Metric Detail Level**

Monitor Metric Instance

Monitor Metric Instance contains the following dimension attributes:

- **Monitor Metric Instance - Instance Key**
- **Monitor Metric Instance - Instance Name**

Monitor Metric Source

Monitor Metric Source contains the following dimension attributes:

- **Monitor Metric Source - Source Name**

Monitor NT Event Category

Monitor NT Event Category contains the following dimension attributes:

- **Monitor NT Event - Category**

Monitor NT Event Description

Monitor NT Event Description contains the following dimension attributes:

- **Monitor NT Event - Description**

Monitor NT Event ID

Monitor NT Event ID contains the following dimension attributes:

- **Monitor NT Event - ID**

Monitor NT Event Log File

Monitor NT Event Log File contains the following dimension attributes:

- **Monitor NT Event - Log File**

Monitor NT Event Message DLL

Monitor NT Event Message DLL contains the following dimension attributes:

- **Monitor NT Event - Message DLL**

Monitor NT Event Rule Triggered

Monitor NT Event Rule Triggered contains the following dimension attributes:

- **Monitor NT Event - Rule Triggered**

Monitor NT Event Source

Monitor NT Event Source contains the following dimension attributes:

- **Monitor NT Event - Source**

Monitor NT Event Type

Monitor NT Event Type contains the following dimension attributes:

- **Monitor NT Event - Type**

Monitor NT Event User

Monitor NT Event User contains the following dimension attributes:

- **Monitor NT Event - User**

Monitor Process Name

Monitor Process Name contains the following dimension attributes:

- **Monitor Process Name - Name**

Monitor Process Owner

Monitor Process Owner contains the following dimension attributes:

- **Monitor Process Owner - Name**

Monitor Task

Monitor Task contains the following dimension attributes:

- **Monitor Task - Task Name**

Organizational Group

Organizational Group contains the following dimension attributes:

- **Organizational Group - Name**

Package

Package contains the following dimension attributes:

- **Package Name**

Package Distribution Event Status

Package Distribution Event Status contains the following dimension attributes:

- **Package Distribution Event Status**

Package Download Method

Package Download Method contains the following dimension attributes:

- **Package Download Method**

Package Download Source

Package Download Source contains the following dimension attributes:

- **Package Download Source Name**
- **Package Download Source Type**

Package Download URL

Package Download URL contains the following dimension attributes:

- **Package Download URL**

Package Server

Package Server contains the following dimension attributes:

- **Package Server Name**
- **Package Server Type**

Package Status

Package Status contains the following dimension attributes:

- **Package Status**

Parent Task

Parent Task contains the following dimension attributes:

- **Parent Task - Instance Type**
- **Parent Task - Name**

Processor

Processor contains the following dimension attributes:

- **Processor - Description**
- **Processor - Manufacturer**
- **Processor - Model**
- **Processor - Number of Processors**
- **Processor - Speed GHz**

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 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 Change

ServiceDesk Change contains the following dimension attributes:

- **Change - Business Unit Impacted**
- **Change - Completed**
- **Change - Contractual Obligation**
- **Change - Customer Impacted**
- **Change - ID**
- **Change - Implement On Release**
- **Change - Open For Voting**
- **Change - Title**
- **Change - Unplanned**
- **Change - URL**
- **Change - Verification Required**
- **Change - Verified**

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 - Source**

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 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 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 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 Incident

ServiceDesk Incident contains the following dimension attributes:

- **Incident - Entered Thru Self Service**
- **Incident - Escalated**
- **Incident - Escalated More Than Once**
- **Incident - Escalated Once**
- **Incident - Exceeded SLA**
- **Incident - Exceeded Warn**
- **Incident - ID**
- **Incident - Name**
- **Incident - URL**
- **Incident - Resolved On First Attempt**
- **Incident - Survey Present**

ServiceDesk Incident Category

ServiceDesk Incident Category contains the following dimension attributes:

- **Incident - Category**

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 Source

ServiceDesk Incident Source contains the following dimension attributes:

- **Incident - Source**

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 Problem

ServiceDesk Problem contains the following dimension attributes:

- **Problem - Action To Date**
- **Problem - Exceeded SLA**
- **Problem - Exceeded Warn**
- **Problem - ID**
- **Problem - Next Step**
- **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 Reference

ServiceDesk Reference contains the following dimension attributes:

- **Reference - Description**

- **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 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 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**

Software Component

Software Component contains the following dimension attributes:

- **Software Component - Company Name**
- **Software Component - Name**

- **Software Component - Software Product Name**
- **Software Component - Software Type Name**
- **Software Component - Type Name**
- **Software Component - Version**

Software Delivery Advertisement

Software Delivery Advertisement contains the following dimension attributes:

- **Advertisement Name**

Software Delivery Execution Event Command Line

Software Delivery Execution Event Command Line contains the following dimension attributes:

- **Command Line**

Software Delivery Execution Event Status

Software Delivery Execution Event Status contains the following dimension attributes:

- **Event Status**

Software Delivery Package Event Status

Software Delivery Package Event Status contains the following dimension attributes:

- **Event Status**

Software Delivery Status Event Status

Software Delivery Status Event Status contains the following dimension attributes:

- **Event Status**

Software Delivery Status Event Type

Software Delivery Status Event Type contains the following dimension attributes:

- **Event Type**

Software License

Software License contains the following dimension attributes:

- **Software License - Name**

Software Product

Software Product contains the following dimension attributes:

- **Software Product - Name**

Software Purchase

Software Purchase contains the following dimension attributes:

- **Software Purchase - Description**
- **Software Purchase - Name**

Software Update

Software Update contains the following dimension attributes:

- **Software Update - Custom Severity**
- **Software Update - File Name**
- **Software Update - Provider**
- **Software Update - Reference**
- **Software Update - Severity**
- **Software Update - Bulletin Enabled**
- **Software Update - Reboot Required**

Software Update Release Date

Software Update Release Date contains the following dimension attributes:

- **Software Update Release Date - Date**
- **Software Update Release Date - Day of Week**
- **Software Update Release Date - Month**
- **Software Update Release Date - Quarter**

SQL Cluster

SQL Cluster contains the following dimension attributes:

- **SQL Cluster - Cluster Name**
- **SQL Cluster - IP Address**
- **SQL Cluster - Max Number of Nodes**
- **SQL Cluster - Total Number of Nodes**

SQL Cluster Resource

SQL Cluster Resource contains the following dimension attributes:

- **SQL Cluster Resource - Instance Name**
- **SQL Cluster Resource - IP Address**
- **SQL Cluster Resource - Owner Node**
- **SQL Cluster Resource - SQL Server Resource Name**
- **SQL Cluster Resource - Virtual Server Name**

SQL Database

SQL Database contains the following dimension attributes:

- **SQL Database - Automatically Grow File**
- **SQL Database - Data File Growth Mode**
- **SQL Database - Data File Growth Size MB**
- **SQL Database - DB Owner**
- **SQL Database - Instance Name**

- **SQL Database - Language**
- **SQL Database - Log File Path**
- **SQL Database - Log File Size MB**
- **SQL Database - Name**
- **SQL Database - Number of Users**
- **SQL Database - Size Allocated MB**
- **SQL Database - Space Available MB**

SQL Database Creation Date

SQL Database Creation Date contains the following dimension attributes:

- **Database Creation Date - Date**
- **Database Creation Date - Day of Week**
- **Database Creation Date - Month**
- **Database Creation Date - Quarter**
- **Database Creation Date - Year**

SQL Database System

SQL Database System contains the following dimension attributes:

- **SQL Database System - Current License In Use**
- **SQL Database System - License Code**
- **SQL Database System - License Type**
- **SQL Database System - Name**
- **SQL Database System - Number of License**
- **SQL Database System - Path**
- **SQL Database System - Processors**
- **SQL Database System - Service**
- **SQL Database System - Threads Allocated**
- **SQL Database System - Vendor**
- **SQL Database System - Version**

SQL Storage Area

SQL Storage Area contains the following dimension attributes:

- **SQL Storage Area - File System Size GB**
- **SQL Storage Area - File System Type**
- **SQL Storage Area - Name**

SQL User

SQL User contains the following dimension attributes:

- **SQL User - Name**

Task

Task contains the following dimension attributes:

- **Task - Name**
- **Task - Return Code**
- **Task - Success**

Task Server

Task Server contains the following dimension attributes:

- **Task Server - Name**

Time

Time contains the following dimension attributes:

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

User

User contains the following dimension attributes:

- **User - City**
- **User - Company**
- **User - Country**
- **User - Display Name**
- **User - Domain**
- **User - Email**
- **User - Given Name**
- **User - Job Title**
- **User - Office Location**
- **User - State**
- **User - Street Address**
- **User - Surname**
- **User - User Name**
- **User - Zip**

Index